Navigating the Future of Mobile Services

Report to American Technology Council & Federal CIO Council

October 2017

MSCT
Mobile Services Category Team

ATARC
Advanced Technology Academic Research Center

NAVIGATING THE FUTURE OF MOBILE SERVICES

On behalf of the Advanced Technology Academic Research Center and the Mobile Services Category Team, we are proud to release *Navigating the Future of Mobile Services*, a compilation of 12 mobile documents from the MSCT and the ATARC Mobile Working Group.

This collaborative effort between government and private industry includes more than 160 people representing 75 agencies, bureaus and companies.

On August 4, 2016, the Office of Management and Budget established the MSCT to develop and implement a government-wide strategic plan to increase efficiency and drive savings related to acquiring government mobile services.

In the year since the release of OMB Memo M-16-20, the MSCT and the ATARC Mobile Working Group have met regularly and the 11 project teams have combined to produce the 12 mobile deliverables you will read over the next 235 pages.

The result is a vast collection of mobile documentation that will serve as a tremendous resource for government agencies.

Thank you to everyone who contributed to *Navigating the Future of Mobile Services*. Without your knowledge, insight and support, this publication would not be possible.

Sincerely,

Jon Johnson
Mobile Services Category Team

Tom Suder
Advanced Technology Academic Research Center

ATARC MOBILE WORKING GROUP LEADERSHIP TEAM

Government Chair: Jon Johnson, GSA; **Government Vice Chairs:** Walter Bigelow, ATF; Yvonne Cole, DoD/VA IPO; Bobby Duffy, DHS; Cecilia Phan, DoD

Industry Chair: Lori Victor Feller, IBM; **Industry Vice Chairs:** Johnny Overcast, Samsung; Kathleen Urbine, DMI; Pattabhi Nunna, Booz Allen Hamilton

ATARC Chair: Tom Suder; **ATARC Vice Chair:** Tim Harvey; **MITRE Chair:** Pat Benito; **Analyst Chair:** Rick Holgate, Gartner

Mobile Identity Management Project Team – Government Vice Chair: Shoaib Ibrahim, Treasury; **Industry Chair:** David Coley, Intercede; **Industry Vice Chair:** Wendy Fairfield, SurePassID; **MITRE Chair:** Mark Russell

Mobile Customer Experience Project Team – Government Chair: Jacob Parcell, GSA; Mike Pulsifer, DOL; **Industry Chair:** Brian Lacey, Mobomo; **Industry Vice Chair:** Jesse O'Gorman, Parallel6; Reena Vij, IBM

Mobile Emerging Technologies Project Team – Government Chair: Lon Gowen, USAID; **Government Vice Chairs:** Justin Herman, GSA; Rick Jones, GSA; Vincent Sritapan, DHS S&T; **Industry Chair:** Bill Moore, Zimperium; **Industry Vice Chair:** Matt Dosmann, Cog Systems; **MITRE Chair:** Marie Collins

Mobile Security Ecosystem Project Team – Government Chair: Chris Miller, DHS ICE; **Government Vice Chair:** DJ Kachman, VA; **Industry Chair:** Rich Balsewich, Samsung; **Industry Vice Chairs:** Gary Bradt, Zimperium; Matthew Landa, Secusmart; **MITRE Chairs:** Marie Collins; Mike Peck

MDM/MAM/EMM Project Team – Government Chair: Bobby Duffy, DHS; **Government Vice Chairs:** Joshua Franklin, NIST; Brandon Iske, DISA; **Industry Chair:** Molly Brais, BlackBerry; **Industry Vice Chair:** Sean Frazier, MobileIron

Network of Things/Internet of Things Project Team – Government Chair: Eric Simmon, NIST; Government Vice Chair: Marc Wine, VA; **Industry Chair:** Jim Haughwout, Savi Technology; **Industry Vice Chairs:** Craig Ano, Samsung; Rich Greene, Verizon; **MITRE Chair:** Nancy Ross

Mobile Roadmap Project Team – Government Chair: Rob Palmer, DHS; **Government Vice Chairs:** Kristia Hayes, DOT; Travis Larkin, U.S. Navy; Rick Walsh, U.S. Army; **Industry Vice Chairs:** Chris Gorman, Efiia; John DiTomasso, Apple Federal; **MITRE Chair:** Pat Benito, MITRE

Mobile Application Vetting Project Team – Government Chair: Vincent Sritapan, DHS S&T; **Government Vice Chairs:** Bob Clemons, NIAP; Art Mosley, DHS; **Industry Chair:** Tim LeMaster, Director, Lookout; **Industry Vice Chair:** Tom Karygiannis, Kryptowire; Stephen Ryan, Proofpoint; **MITRE Chair:** Carlton Northern

Mobile Backend-as-a-Service (MBaaS) Project Team – Government Chair: Jon Johnson, GSA; **Government Vice Chair;** Debra Zink, FAA; **Industry Chair:** Steve Brady, Shadow-Soft; **Industry Vice Chair:** Heath Marell, ATSG Corporation; **MITRE Chairs:** Matt Pollack; Jeff Stein

Mobile Device-as-a-Service (DaaS) Project Team – Government Chair: Jon Johnson, GSA; **Industry Chair:** Jeff Ait, MobileIron; **Industry Vice Chair:** Erika Peace, DMI; **MITRE Chair:** Andy Pyles

Mobile Strategic Sourcing Project Team – GSA Chair: Susan DiGiacomo; **NASA SEWP Chair:** Betsy Sirk; **NIH NITAAC Chair:** Robert Hedetniemi; **Government Vice Chairs:** Vernelle Archer, USDA; Greg Hixson, GSA; **MITRE Chair:** Diane Hanf

Navigating the Future of Mobile Services

Table of Contents

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Mobile Application Vetting

Working Group Document

1 Introduction

The Federal Government increasingly relies on commercial and custom-built mobile applications (apps) to conduct business and to deliver government information and services to the public. The mobile apps can be developed by trusted in-house developers, by contractors, or third parties having no previous relationship with the agencies using the mobile apps. Well-intentioned developers can make programming errors that can expose both user and enterprise sensitive information. Moreover, while federal agencies have access to source code for internally-developed apps, they must submit third party apps through a software assurance vetting process without access to source code.

Mobile applications increase productivity by providing users real-time information sharing and 'anytime anywhere' access to perform enterprise or mission-specific tasks and communicate with the public. As with traditional desktop and enterprise applications, mobile apps can contain malware or have security vulnerabilities that could be exploited by attackers to gain access to sensitive government information and resources. Unlike desktop applications, precise location information, contact details, sensor data, photos, and messages can be exposed through mobile apps, and personal information collected by these apps can be sold to marketers or advertising agencies. Additional threats include ransomware and malware that surreptitiously records the user with the device's camera or microphone. As mobile applications rely on cloud services to store enterprise data, mobile apps that do not use secure programming practices can expose the cloud infrastructure to new risks.

The sheer number of available apps (millions), the frequently unknown provenance of app developers, and the frequent use of third-party libraries in apps, requires a software assurance process tailored for mobile apps. App vetting is part of the software assurance process that occurs after app development: it evaluates mobile apps against a set of security requirements to identify weaknesses, vulnerabilities, poor programming practices, improper use of cryptographic functions, insecure authentication to cloud services, and malicious or privacy invasive behaviors. Its objective is to provide federal agencies with a level of assurance that commercial and custom-developed mobile apps used to conduct government business will not compromise federal systems or information, operate as described, do not request more permissions than needed, and do not expose information that could harm the privacy, security, or safety of employees or the public.

This document provides guidance and recommendations for vetting the security of mobile apps based on standards and agency best practices. It is intended for federal departments and agencies (D/A) currently performing or considering app vetting, and is aimed broadly at federal government executives, information technology middle managers, software assurance analysts, software developers, and program managers. The guidance applies to vetting both in-house custom-developed apps and apps obtained from commercial app stores (e.g., Google Play Store, Apple App Store, BlackBerry World, Amazon).

1.1 Definitions and Assumptions

App Vetting: A sequence of activities that aims to determine if an app conforms to security and privacy regulations (e.g., Federal Information Security Modernization Act [FISMA], National Information Assurance Partnership [NIAP], Health Insurance Portability and Accountability Act [HIPAA], Payment Card Industry [PCI]) and to organization-specific requirements and policies. The app vetting process follows development of a custom app or identification of a commercial app to be used for government business and prior to the app's installation on a mobile device or publication of a custom app to a federal, community, or commercial app store.

Software Assurance: Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

Assumptions:

- App vetting is conducted, at minimum, on any apps that access or store government Controlled Unclassified Information (CUI), connect to government systems that contain CUI, or collect Personally Identifiable Information (PII) from employees or the public for Government use.
- Apps used by government employees for official business will be installed on devices that meet the D/A's security requirements and security policies, should be managed by an enterprise mobility management (EMM) system, and are segregated by the enterprise management system from any personal use apps (e.g., weather, news) the D/A may allow on the phone.

1.2 Comparison of Mobile and Desktop Platforms

Mobile devices are a relatively recent addition to the Federal Government's computing platforms, and some organizations manage them like the feature phones from which they evolved rather than as the powerful computers they are. Most agencies, however, are grappling with the difficulty of securing the devices, which requires a different approach than endpoint security for laptops and desktops. Government-furnished desktops are secured with endpoint protection tools that include configuration management, anti-virus, firewall, and intrusion detection/prevention software. Mobile devices must rely on an EMM/ mobile device management (MDM) to control and configure the security features of the device. The security architecture of mobile operating systems employs application isolation capabilities that differ from desktop operating systems. The isolation controls allowed interactions between apps and between each app and the operating system, and permissions allowed must be approved by the user. This is more akin to the browser sandbox model than to the desktop application model. Inherently, mobile apps are not trusted by design of the mobile security architecture and there are safeguards in place to prevent unintended use.

Compared to desktop applications, which are typically developed, tested, and maintained by a small number of known software vendors, mobile apps may be developed by unknown entities that are attracted by the potential to sell apps to a market of billions of users. Such developers may have little experience building secure software, and they do not have the resources or motivation to conduct extensive testing. Further, users install new apps, and update and remove mobile apps more frequently than desktop and web applications. Although commercial apps are

vetted by native app stores for malware and other common application issues, the app store's criteria are not equivalent to a Federal agency's security requirements (e.g., cryptography).

The small size and portability of mobile devices is possibly the most significant difference between mobile devices and desktops. This increases the likelihood of loss or theft, potentially allowing a bad actor to access information on the device. Additionally, mobile devices may connect to many different networks (cellular, Wi-Fi, Bluetooth, Near Field Communication), leaving them vulnerable to attacks from unknown networks, such as a malicious wireless network or unwitting installation of malicious network profiles on the device. Such attacks could expose sensitive information to an attacker and apps need to be designed with integrity and confidentiality controls to protect sensitive data against attacks and data leakage.

1.3 References

- National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) *Mobile Threat Catalogue*
- NIST Special Publication (SP) 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
- Department of Homeland Security (DHS), *Study on Mobile Device Security*
- Open Web Application Security Project (OWASP) Top 10 Mobile Risks

2 Best Practice Recommendations

To help mitigate the risks associated with mobile malware and mobile app vulnerabilities, organizations should develop security policy regarding mobile apps including: security and privacy requirements; the process for requesting, developing, approving, updating, and retiring apps; and processes for checking and enforcing compliance with the requirements. To ensure that apps conform to the requirements, organizations should develop, communicate, and implement an app vetting process and acceptance criteria. App vetting comprises two main activities: app testing and app approval/rejection. App testing examines an app for software weaknesses, vulnerabilities, and unwanted behaviors to generate vulnerability reports and risk assessments. App approval/rejection involves evaluating the reports and risk assessments, along with additional organization-specific criteria, to determine the app's conformance with the security requirements and the organization's risk tolerance, and ultimately approving or rejecting the app for deployment.

Mobile app vetting is assumed to require fewer resources than system security authorization, commensurate with the scale, scope and sensitivity of the data accessed or processed by the app. The process needs to be streamlined and automated to the greatest extent feasible to meet user and business demands and avert 'shadow IT' – users ignoring the rules regarding app installation because of a perceived burdensome process that negatively impacts the ability to do their job. Identifying relevant mobile app software assurance standards and agency-specific acceptance criteria can help automate the mobile app vetting process. Automation is also important given the short update cycle of mobile apps, potentially introducing new vulnerabilities or malicious behavior with each version.

2.1 Security Requirements Definition

D/As need a level of assurance that mobile apps used to conduct government business or deliver government services meet the D/A's minimum security requirements for protection of federal information and any backend systems and data accessed by the apps, and the safety and privacy of users. To provide software assurance for apps, organizations should develop security requirements that specify, for example, how data used by an app should be secured, the environment in which an app will be deployed, the acceptable level of risk for an app, and explicit pass/fail criteria. Security requirements are tested during the app testing activity, and provide a basis for technical evaluation and risk determination by Authorization Officials for app approval/rejection.

As a baseline, organizations should adopt mobile app security requirements developed by government and open standards organizations. Sources include: 1) National Information Assurance Partnership (NIAP) Requirements for Vetting Mobile Apps, which provides a consistent baseline set of security requirements developed in partnership with the National Security Agency, NIST, and industry for organizations vetting mobile apps outside NIAP's formal Common Criteria process; 2) NIST SP 800-163, *Vetting the Security of Mobile Applications*, which describes a set of general requirements for any app and examples of organization-specific requirements, and 3) OWASP Mobile Security Project's Top 10 Mobile Risks and Top 10 Mobile Controls. The cross-agency Mobile Technology Tiger Team (MTTT) developed vetting criteria for mobile apps, which were incorporated into the NIAP Requirements for Vetting Mobile Apps and are recommended as the baseline security requirements for use across the government. At a high level, these baseline security requirements include:

- Limit permissions to access platform resources
- Identify and protect sensitive data
- Implement cryptographic protocols correctly
- Protect credentials
- Protect data in transit and at rest
- Employ strong authentication, session management, and authorization
- Secure app access to backend services and servers
- Secure use of third-party libraries, services and APIs
- Secure app installation and update
- Collect consent for use of user data

In addition to these baseline security requirements, D/As need to define their criteria for making an app approval/rejection determination consistent with their risk tolerance. While testing for conformance to general requirements can be automated, evaluation against organization-specific criteria involves human analysis to consider:

- Intended users and environment of use
- Criticality of app to enterprise business/mission
- User (and device) authentication and authorization requirements
- Backend systems and data accessed by app
- App provenance (identity and reputation of app developer)
- Protections afforded against possible app vulnerabilities by enterprise mobile security technologies (e.g., EMM/MDM, Virtual Private Network [VPN], full device encryption)

2.2 App Security Testing

Various use cases for enterprise vetting of mobile apps exist, including in-house developed apps for enterprise use, in-house developed apps for public distribution, commercially developed apps for enterprise use, and commercially developed apps for personal use on enterprise devices. Each of these app types carries different risks.

Mobile app vetting can be performed manually or with tools and/or services that provide automated or semi-automated management of app security testing and app approval or rejection. Manual app vetting generally involves a time and labor-intensive effort, resulting in high costs and delays in approving apps for use. Additionally, mobile app developers often operate on a rapid development cycle, and manual vetting approaches cannot keep up with the rapid release cycle for new app versions. Automated mobile app vetting technologies can be adopted throughout the Software Development Lifecycle for in-house developed apps, while third-party mobile app binaries can be vetted for each new version release.

Specialized software and tools are required to test, validate, and verify mobile apps against baseline security requirements. Numerous vendors now provide automated app vetting tools (sometimes also called app threat intelligence or threat protection services) that run static and/or dynamic analysis tests on apps to detect security vulnerabilities and malicious or privacy-violating behaviors. Tools that perform both static and dynamic analysis are recommended. Static analysis techniques examine the code without running the app, these techniques provide insights into the properties of the app and can detect many vulnerabilities, while dynamic analysis techniques reveal app behaviors that only occur at runtime. Automated tools should provide evidence for security tests that are flagged as failures as well as evidence for security tests that are reported as passing the test.

These tools may be provided as cloud-based services or as on-premises solutions. Many of the tools regularly crawl commercial app stores, automatically analyzing new app versions using the vendors' evolving knowledge of mobile threats and making the analysis results available. Some can perform reputational analysis of apps and their developers based on intelligence information gathered from sources such as app stores and participating mobile devices. They may also provide the ability to directly submit in-house custom-developed apps for analysis. Leveraging these commercial offerings enables enterprises to streamline app vetting, decreasing the cost and time associated with analysis while potentially improving security by staying up-to-date with emerging threats and app versions.

Mobile app testing may include searches for both potentially exploitable vulnerabilities and for potentially malicious or privacy-violating behaviors. Each organization must determine its acceptable level of risk when deciding on the necessary scope of security analysis. However, when conducting the app testing, it is worth considering both the organization that developed the app (in-house vs. external) as well as the planned use of the app (whether it will be used for enterprise purposes or not). In all cases, enterprises should also consider the security features provided by the mobile platform (operating system and other underlying on-device technologies) as well as enterprise and broader ecosystem capabilities.

Apps developed in-house are less likely to contain intentionally malicious or privacy-violating functionality than externally-sourced apps. Security testing of these apps can therefore focus primarily on searching for vulnerabilities. However, some level of risk of malicious or privacy violating behavior may still exist: for example, third-party software libraries included in the app

may include privacy-violating behaviors to enable targeted advertising that are not known to the app developer. Similarly, if the organization outsourced all or part of development, it may not be aware of the full behavior of the app, yet might still be held responsible for the app's behavior.

It is important to note that no known analysis tool can perform an exhaustive search for all possible vulnerabilities, maliciousness, or privacy-violating behavior. Enterprises should follow secure software development practices when developing apps in-house and ensure they understand and mitigate any potential implications of using third-party libraries or outsourced software development. It is important to use objective criteria, such as the NIAP and NIST requirements, when evaluating the capabilities of mobile application vetting tools.

Personal use apps allowed by the organization are not intended to process enterprise data. Testing of these apps can primarily focus on searching for malicious or privacy-violating functionality, with a search for security vulnerabilities being less critical to the organization because mobile device app sandboxes generally isolate the impact that exploitation of a single app would have on other apps on the device. However, some risk still exists that an attacker could use a vulnerable app as a vector to exploit the mobile device itself and gain access to enterprise data. Additionally, government users would likely want to know about the potential impact on their personal data of any vulnerabilities in personal apps. A mitigation strategy for this risk is to only allow users to download apps from official app stores, and disallow apps from unknown third-party app sources. Agencies that permit personal use applications should provide training to make the user aware of the threats and ensure the device is configured via an enterprise management system to segregate personal use apps from government apps and data. Department of Defense (DoD) Security Technical Implementation Guides (STIGs) provide configuration guidance to ensure this separation is enforced on mobile devices.

Table 1 summarizes the recommended primary focus areas for app vetting based on app developer and planned use of app.

Table 1. Primary App Vetting Focus Areas

	Malicious Functionality	Security Vulnerabilities
In-house enterprise use app	Less critical, but may still be necessary	Primary focus
In-house developed app for public distribution	Less critical, but may still be necessary	Primary focus
Commercial enterprise use app	Both should be examined	Both should be examined
Commercial personal use app	Primary focus	Less critical, but may still be necessary

When selecting an app vetting tool or set of tools there are requirements that should be met, outlined in a MITRE report, Analyzing the Effectiveness of App Vetting Tools in the Enterprise. These criteria map to many of the baseline security requirements in version 1.2 of the NIAP Requirements for Vetting Mobile Apps (not all NIAP requirements can be automated). This includes use of NIAP's sample XML Schema (similar to the MTTT's Mobile App Security Vetting Reciprocity Report), which describes useful app vetting results to report based on the NIAP requirements. In addition to the NIAP requirements, MITRE suggests additional criteria to cover broader app vetting tool capabilities (e.g., reputation analysis), threats against the app

vetting tool itself, and other vulnerabilities or malicious behavior commonly observed in apps but not directly addressed by NIAP. The testing tool criteria listed in Table 2 do not represent an exhaustive list of every potential vulnerability or malicious behavior in apps. Rather, they cover many common app issues to enable a baseline evaluation of vetting tool capabilities. Organizations may add criteria based on their specific needs and risks, and test the tools with a set of selected apps.

Table 2. App Vetting Test Tool Criteria

Test Tool Criteria	Tool Requirements Coverage
Types of applications supported by the app vetting solution	A. Supported platforms: e.g., Android, iOS, Windows B. App source code required or not required C. What types of application code can be assessed? For example, on Android, can only the Java code be assessed, or can native code also be assessed? Are cross-platform app development frameworks supported (e.g., Apache Cordova)?
Ability to assess general risks associated with an app [could be skipped for in-house developed apps]	A. Ability to assess the reputation of the app and its developer. B. Are there indications that the app is repackaged/counterfeit?
Ability to detect potentially exploitable security vulnerabilities	A. Ability to identify failure to invoke an appropriate random number generator where needed. B. Ability to identify insecurely storing private keys, passwords, or related secret values. C. Ability to report data stored by the app, including whether the data is stored securely (e.g., in an appropriate storage location and with appropriate file permissions). D. Ability to report whether network communications use secure protocols (e.g., Hypertext Transfer Protocol Secure [HTTPS] vs. HTTP) and any related security issues such as improper HTTPS/Transport Layer Security (TLS) certificate validation or hostname checking. E. Ability to identify default credentials found within the app. F. Ability to identify mapping of memory at explicit locations. G. Ability to identify mapping of memory as both writable and executable. H. Ability to determine whether the app successfully runs on the latest version of the operating system (and hence is likely compatible with its security architecture).
Ability to detect potentially exploitable security vulnerabilities *(continued)*	I. Ability to determine whether the app places executable code in locations where the code can be modified. J. Ability to identify code compiled without stack-based buffer overflow protection enabled. K. Ability to identify third-party libraries included in the app. L. Ability to identify other common cryptographic implementation issues. M. Ability to identify inter-process communication issues.

Test Tool Criteria	Tool Requirements Coverage
Ability to detect potentially malicious or privacy-violating behaviors	A. Ability to report hardware resources accessed by the app. Report permissions requested by the app and/or actual operations performed. B. Ability to report sensitive information repositories accessed by the app. Report permissions requested by the app and/or actual operations performed. C. Ability to report all network communication performed by the app. D. Ability to determine whether the application attempts to update executable code after installation. E. Ability to ensure the app only uses supported platform application programming interfaces (APIs). F. Ability to determine whether the application code has been obfuscated or otherwise deliberately implemented in a way that makes security analysis more difficult. G. Ability to identify known malicious code (e.g., operating system exploits) within the application. H. [Android only] Ability to identify attempts by the application to obtain device administrator access. I. [iOS Only] Ability to identify Uniform Resource Locator (URL) scheme hijacking issues, where the app registers URL schemes that belong to other apps to hijack communications intended for that other app.
Security of the app vetting tool itself	A. Ability to resist attempts by malicious apps to determine that they are running in an analysis environment. B. [Cloud-based vetting solutions used by multiple tenants] Ability to refresh the environment after each app is analyzed so that sensitive data is not exposed to other apps under analysis. C. Ability to resist persistent exploitation of the analysis environment by a malicious app.
Reporting capabilities	A. Ability to list output formats supported, e.g., JSON, XML, other machine-consumable data format, XLS, PDF, etc. B. Ability to provide evidence (e.g., network packet captures, system call traces, screenshots) that analysts can use to clarify or confirm reported information about apps. C. Ability to integrate with EMM/MDM systems.

After selecting test tools and setting up the test environment or service to implement an app testing capability, the organization's mobile app administrator submits apps for testing. The mobile app testing team scans the app with the testing tools/service. The app testing tool/service generates a report that documents the security findings, provides supporting pass/fail evidence and summary results of security testing, and assigns a risk score to the app.

2.3 App Approval/Rejection

One of the issues related to app security test reports is the need for an expert human analyst to interpret the tool results and normalize risk ratings output by different tools: some may assess the risk as low, moderate, high, while others may use ratings of pass, warning, or fail. To address this issue, NIST recommends that organizations identify tools that leverage vulnerability reporting and risk assessment standards. Agency analysts can provide input to the mobile app

vetting tools to provide agency-specific risk scores that reflect the risk tolerance of the specific agency.

The analyst evaluates these results in the context of the environment and intended use of the application; the sensitivity of the data processed; the D/A's security policy and the presence of mitigating controls; assigns an overall risk rating (e.g., low, moderate, high, blacklist); and documents the findings in a report that includes a recommendation for approval or rejection of the app. In some cases, when there are clear pass/fail criteria that can be mapped to an enterprise security/privacy policy, the analyst's job (and associated cost) can be reduced by automating the reject decision. The report is provided to the Authorizing Official, who reviews the report and recommendation and makes a final risk-based approval/rejection decision based on the outcome of the testing, analyst recommendation, and the determination of the business owner about whether the residual risk is acceptable given the mission requirements and any other mitigating factors. The decision is communicated to the Mobile Administrator responsible for management of mobile apps, and the report and final determination decision are stored in an organization-defined repository.

2.4 References

- NIAP Requirements for Vetting Mobile Apps from the *Protection Profile for Application Software*
- NIST Special Publication 800-163, *Vetting the Security of Mobile Applications*
- OWASP Top 10 Mobile Controls and Top 10 Mobile Risks
- Defense Information Systems Agency (DISA) STIGs for Mobile Devices
- XML Schema for NIAP's Requirements for Vetting Mobile Apps
- *Analyzing the Effectiveness of App Vetting Tools in the Enterprise*

3 Implementation Guidance

An essential first step when implementing a mobile app vetting process is for the D/A to define its mobile app security policy, including what apps can/cannot be installed on government-furnished devices, restrictions on downloading apps from third-party app stores, which apps must be tested by the organization prior to installation, policy regarding automated app updates and testing of app updates, and requirements regarding device ownership and device management. It is critical that the organization clearly communicate the app policy and process to users, and explain the process for requesting and approval of apps, including timelines. Organizations may also need to consider re-testing apps after mobile OS upgrades, which may impact app security and/or functionality.

Additionally, standardized guidance and requirements throughout larger D/As can foster reciprocity and lead to the sharing of vetting results, reducing duplicative efforts and costs.

3.1 Security Requirements Definition

Based on the defined security policy, the organization performs a risk analysis to understand and document potential security risks from mobile apps and identify mitigating controls, e.g., a device's encrypted file system or the use of EMM/MDM solutions. Using the sources cited in the Best Practices section, the organization adopts a standard set of baseline requirements and defines its enterprise- or community-specific security requirements, considering the sensitivity of

data generated or accessed by the app, the type of users and how the app will be used, who owns and manages the device and whether the app will access back-end systems or data. If back-end systems will be accessed by the app, test requirements should include testing server-side controls such as access control, session management, and logging.

For apps developed in-house, implementing app security testing only at the end of the development effort leads to increased costs and lengthened timelines. It is strongly recommended that security test tools be used to identify potential vulnerabilities or weaknesses during development when they can still be addressed by the developers.

3.2 App Security Evaluation

Two models exist for structuring a mobile app vetting process: the enterprise model and the developer model. In the enterprise model, the D/A acquires the in-house resources (budget, human analysts, tools, testing environment) and/or external services to conduct the app security testing. If the D/A uses and external service, the D/A may have to negotiate with the external vetting service concerning the cost of analysis per app, the number of concurrent evaluations that can be executed, and who retains ownership of the analysis at the end of the contract period

In the developer model, app developers bear the cost for the security evaluation of their apps. Unlike the enterprise model, this allows the developer to interact more directly with the app vetting service. However, the D/A must still make qualifying statements describing which vetting services meet their criteria for evaluation. This is the model for the formal NIAP validation process for apps that implement security functionality as part of National Security Systems. The Association of Public Communications Officials (APCO) International is also adopting this model for evaluation of for apps intended for the public safety community.

Regardless of the app testing model, there are certain factors that must be considered when planning an app security evaluation strategy. First and foremost is the verbosity and content of the app analysis provided by any testing tool or external vetting services. Typically, app vetting services can produce more technical output than may be desired by the D/A when negotiating the pass/fail and/or rating criteria of an app based on their client's security requirements. D/A must be prepared to clearly define these requirements to the vetting service, especially if it is an external service that is informing the no/no-go decision for an app. Second, it should be noted that if a D/A uses a cloud service for app security testing and analysis, and uploads government custom-developed apps and government data to the cloud service, that service must be FedRAMP certified. Finally, it must be clearly understood that the D/A Authorizing Official for the mobile system to which the app is being deployed is responsible for making the risk-based app deployment decision.

3.3 Deployment and Maintenance

After testing an app and approving it for release, the mobile app must be managed throughout its lifecycle: app deployment, patching, updates, prohibition, and removal.

3.3.1 Deployment

Deployment refers to provisioning of mobile apps to a mobile device. Mobile device users are accustomed to installing apps directly from public app stores onto their phones when they want them. They bring this expectation into the work environment and therefore expect that same direct install for government-furnished devices.

Large government D/As, on the other hand, have traditionally approved software *before* installation on users' desktop computers, so it is a significant change to allow users to directly install apps on mobile devices. If an organization wants to manage mobile apps in a similar manner, they need to consider a different approach that integrates the configuration and policy enforcement capabilities of EMMs/MDMs with mobile app vetting. Provisioning and management of mobile apps may vary based on mobile OS architecture and capabilities.

Continuous monitoring of mobile devices (discussed in the following section), could assist in vetting apps after installation of a new app or when an app has been automatically updated on the mobile device. Vetting an app after installation can add risk because apps can run on the device for a period before being identified as vulnerable or malicious.

3.3.2 Patching and Updates

Popular mobile apps on Android Google Play Store and Apple's App Store are generally updated many times per year for new functionality, bug fixes, and security. This leads to mobile device users needing to implement those updates quickly or risk not having the latest functionality, having a broken app, or having an app without the most up to date security patches.

With most devices containing dozens or more apps, most users will get many updates pushed to their devices every week. Often, the user is unaware of these updates because they are automatically managed by the app store.

Even though many app updates contain security improvements, some app updates can introduce new vulnerabilities or malicious code. Ideally, an organization could scan every app update using the same level of testing and analysis as a brand-new app. However, that will delay the user's ability to access the new versions and any security updates included in those new versions. The following list of organizational activities needed to support scanning of every update illustrates how burdensome this process can be:

- Implement a mechanism to prevent users from automatically getting updates. This likely requires a backend system and front end (i.e. mobile device) configuration. This may require turning off the ability for the device to get to the Google Play or iTunes stores in favor of having the devices limited to accessing only the organization's MDM provided store or other internally maintained app store for acquiring apps.
- Track all apps across all devices in the organization, possibly totaling in the thousands of apps for a mid-sized organization, and track when any new update is available for any used app.
- Analyze each app after every update.
- Decide to permit or deny use of the app.
- If the app is permitted, implement configurations to allow the update to be released to the device.
- Alert the device of the new update.

To avoid this, many organizations are taking the approach of implementing continuous monitoring (CM) on devices. CM is the process and technology used for detecting organizational compliance and risk posture. Using CM allows organizations to be aware of apps installed on devices, the networks that devices connect to, OSs running on the devices, and other security-related information. When CM detects a security issue, it can alert the security administrator and MDM, which can be configured to enforce automatic remediation actions, such as wiping the

device, disabling access to a vulnerable app, or quarantining the device to restrict access to backend systems.

3.3.3 Prohibition and Removal

While there are obvious benefits of implementing CM, there are risks when leveraging CM for app vetting. For an app to be vetted for a device using CM, the app or update must first be installed on the device. To mitigate this risk, there are two main system configurations that can be implemented:

1. The system can be configured to prohibit new apps and updates that are not on an approved list from being installed. However, educating users to reference an approved list before installing a new app or update can be difficult. This adds complexity for the user and requires substantial administration to ensure users are not installing unapproved apps.
2. Allow users to install apps from the native app stores, or an approved internal app store, and perform a deep analysis of each app installed on devices across the organization. If an insecure app is found, that app can be blacklisted and removed from devices by the MDM.

With all IT systems, people will try to avoid any security process or system that is too complex. With mobile devices, this is often accomplished by simply using their personal device, at which point the organization loses significant security insights into app and data security, thereby impacting the ability to protect users and government systems. While access to internal networks and advanced enterprise apps that require enrollment in the EMM system can be restricted, other work related data can still be accessed from personal devices, such as from mobile apps leveraging many Software-as-a-Service (SaaS) applications.

3.3.4 Importance of MDM to App Vetting

An MDM is often a critical piece of the app vetting process, whether to prevent access to public app stores, provide an internal app store, manage update of apps on devices, whitelist and blacklist apps, or to remediate or remove apps from devices.

3.4 Reciprocity

Committee on National Security Instruction (CNSSI) 4009 defines reciprocity as: “Mutual agreement among participating organizations to accept each other’s security assessments in order to reuse information system resources and/or to accept each other’s assessed security posture in order to share information.” Reciprocity is the process of sharing results across app vetting teams to reduce re-work in app vetting; it implies that vetting processes and results performed at one agency will be available for reuse by another agency. Reciprocity occurs when a D/A’s app vetting process leverages results from another D/A that has previously performed app vetting on the same app. It enables the receiving D/A to reuse the app testing results when making their own risk determination on deployment of the app.

To share the security testing results with other D/As, the testing agency captures the results of app security testing against the baseline security requirements (e.g., NIAP) in a standardized reciprocity report format, with the intention to make the information available for use by other agencies.

Given the different potential uses any individual app may have and different mobile architectures between different agencies, sharing risk decisions (approval/rejection determination) is not

recommended. The alternative developed by the Federal Chief Information Officers Council Mobile Technology Tiger Team is to make findings from tests conducted by one federal agency available to other federal agencies. The sharing of this data would allow agencies to access the findings from other agencies and make their own risk-based determinations using a common set of security criteria, without having to repeat tests already conducted by other agencies. In this process, the agency Authorizing Official retains responsibility for the risk management decision. This type of sharing relies heavily on establishing a standard set of vetting requirements between different D/As (i.e., NIAP).

Sharing of security test results for reciprocity can be difficult to accomplish, mainly due to licensing restrictions of security analysis products. Licensing often limits the results that can be shared across organizations or organizational units (for large organizations). Even taking the results of security analysis and ingesting those results into other standard formats or templates can be considered a breach of the license agreement and not permitted by the vendor.

If D/As and industry can resolve licensing and processes around reciprocity, government agencies could potentially create a repository of reciprocity reports that would allow government app vetting teams to view each other's reports. The number of apps and frequency of app updates would still present a challenge when a D/A wants to determine if another agency had previously tested the app. For example, if one D/A team evaluates version 1.1 of an app and another D/A's team wants to evaluate the app two months later but the app is now on version 1.2, how reliable and accurate are the 1.1 results for assessing version 1.2?

Given the number of apps and versions, the most comprehensive solution would need to be automated to ensure that testing and reciprocity reports are up to date. Adding automation means that every app version is automatically vetted, the report is placed in the reciprocity repository, and administrators constantly review the automated vetting to ensure accuracy and currency.

The value of mobile app vetting and reciprocity lies in streamlining the app vetting process for large enterprises. Within an enterprise, reciprocity will allow for re-use of results and acceptance of overarching risk based on agreed criteria.

There are ongoing efforts within the federal government to realize mobile app vetting reciprocity, e.g., the work of the Federal CIO Council's Mobile Technology Tiger Team's Mobile App Security Vetting Working Group, and the DoD's App Focus Working Group.

3.5 References

- NIST Special Publication 800-163, *Vetting the Security of Mobile Applications*
- DHS Mobile Application Playbook
- NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and Common Criteria Testing Laboratory Services
- News Release, APCO Partners with DHS to Advance Interoperability and Security of Mobile Apps

4 Future Directions

The future direction of mobile application vetting will depend on which deployment model an enterprise chooses to adopt and how they will measure effectiveness. A critical factor that will support longevity and sustainability will be based on how mobile applications are distributed in

the enterprise (e.g., if the enterprise organization develops or consumes other business to business (B2B) applications, and/or if their mobile application distribution model allows any mobile application from the app stores to be installed). Some measures and metrics to help evaluate mobile application vetting solutions for current and future adoption include:

- The resources needed to evaluate and vet a mobile application based on specific standards (e.g. vetting one time and/or continuously). This includes, but is not limited to, setup time needed to install or use a tool or service for the first time, the time it takes for a tool to do the initial evaluation of a mobile application and the time it takes for re-evaluation, the labor hours needed to use a tool, and the labor hours needed to analyze and validate results to support a risk based decision.
- The scalability of the tool or service to support evaluation of multiple mobile applications (e.g., can the tool or service handle 1, 10, 100, or 1000 mobile applications), including how long it will take and how much it will cost.
- Once a vulnerability or issue is identified and confirmed, what are the next actions this tool can support? (e.g., does the tool integrate with EMM solutions (also known as MDM solutions) to take actions such as removing a mobile application from a device, forcing an update, or removing an app from an enterprise mobile application store.)
- Does the app vetting solution or service integrate with enterprise mobile device and app catalog management capabilities? Can remediation actions be streamlined?

Last, a future recommendation for mobile application vetting is to develop mobile app security training for Departments and Agencies, specifically for analysts who will validate results from the mobile application vetting tool(s) or service(s). There is general consensus that the current skillsets for mobile app vetting analysts vary from Department to Department, and consistent training could help improve the overall security posture of mobile devices and applications used in the federal government.

5 Conclusion

Providing security assurance for D/A use of mobile apps requires the enterprise to test the security of those apps against a set of common security requirements (e.g., NIAP) and enterprise-specific security requirements and make a risk-informed decision on whether to allow them to be installed on devices or published for download by stakeholder communities or the public.

Mobile application security begins with the design of the application and continues through the life of its use. Organizations should conduct app security vetting against a standard set of requirements, define organization-specific requirements, and manage apps throughout their lifecycle. As with any software assurance process, there is no guarantee that even the most thorough vetting process will uncover all potential vulnerabilities. New vulnerabilities are discovered in apps and operating systems, and old ones may remain unpatched, presenting risk to the user and the organization. In addition to app vetting, there is a complementary need for mobile endpoint protection for continuous assessment and monitoring of apps and devices. Please see the companion paper to this document, *Mobile Threat Protection Guidance*, for information on this technology.

For information on current mobile security R&D activities, please visit:

- DHS Science and Technology (S&T) Mobile Security R&D Program

6 Acknowledgements

The MSCT and the Advanced Technology Academic Research Center (ATARC) appreciate the contributions of the following individuals and organizations in supporting the efforts of the App Vetting and App Security working group and development of this guidance.

- Marika Robertson — Apcerto
- Tom Suder — ATARC
- Tim Harvey — ATARC
- John Drake — DHS S&T
- Vincent Sritapan — DHS S&T
- Anne Dalton — DHS Office of the Chief Information Officer (OCIO)
- Anthony Glynn — DHS OCIO
- Art Mosley — DHS OCIO
- Brett Pfrommer — DHS Customs and Border Protection
- Bob Clemons — DoD
- Stephen Rossero — DoD
- David Driegert — Department of the Navy
- Cathy Simpson — Government Acquisitions
- Suro Sen — GSA
- Jon Johnson — GSA
- Rick Jones — GSA
- Tom Karygiannis — Kryptowire
- Tim LeMaster — Lookout
- Carlton Northern — MITRE
- Mike Peck — MITRE
- Terri Phillips — MITRE
- Sean Frazier — MobileIron
- Michael Ogata — NIST
- Stephen Ryan — Proofpoint, Inc.
- Mark Williams — VMWare Airwatch

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Customer Experience

Working Group Document

Introduction

Federal agencies are beginning to address and create long-term plans for mobility as mobile becomes a more central part of how agencies interact with other agencies and citizens. When creating these strategies, federal agencies run the risk of excluding the most important stakeholder in a mobile strategy---the customer. We maintain if agencies don't properly address the end user experience - what we will call the customer experience, all the planning and work will be for naught.

> Customer experience should always tie into the agency's larger digital strategy, with mobile approaches falling in line with organizational mission and outcomes

Some agencies and many private sector organizations, have made the customer the center of their mobile journey. For the purposes of this document, we will define "*mobile customer experience*" as the sum total of a stakeholder's feelings towards their mobile experience from end-to-end. This includes, but is not limited to, dispositions toward application functionality, responsiveness, mobile device usability/suitability, implementable standards, etc. Customer experience is a journey, and should include every step along the path, from the first moments of awareness to the end of the task. While customer engagement is not the focus of this document, we would like to clarify that having a customer engagement strategy is necessary for any organization to practice effective Customer Relationship Management (CRM.)

This playbook articulates how to start the journey of embracing customer experience. The document lays out six principles of mobile customer experience that agencies should consider to achieve success. These are numbered one to six in no particular order. The principles were developed over a number of months and vetted with various mobile experts inside and outside of government. The principles cover everything from who to include in a mobile implementation, to leveraging real time analytics. This team believes that agencies that strategize using the best practices from other Mobile Services Category Teams and also focus their efforts on making things easier for customers, will have a more successful approach for mobility.

[1] For more information see Mobile Services Category Team Homepage

Principle 1 - Mobile customer experience requires a village

By: Lizzie Berkovitz, DHS

Customer experience should be a part of an agency's digital strategy and requires input from multiple perspectives in the organization.

Often, executives or business owners in charge of mobile set the vision, design, and requirements for creating a new app, mobile website, or mobile experience. In many instances, this could lead to building and designing a solution without speaking to a single end user. However, it is important to solicit feedback, opinions, and perspectives from everyone in the organization that the service will touch. We also note effective stakeholder engagement is essential and is specifically included in the PMBOK, is detailed in the ITIL framework and is at the heart of AGILE.[2]

This principle in practice:
In order to receive input from all stakeholders, you must first understand who your stakeholders are. To begin with, determine **who** belongs in your influencer group--It is helpful to map the structure to outline everyone's roles and responsibilities. There are two groups of people to include: decision makers and users. **Decision makers** are the group who will be involved in making business decisions around your mobile opportunity. This group will consist of anyone who needs to approve, provide context/requirements, or view some part of your application, and should include accessibility, privacy, risk, and more. **Users** are the consumers of your application, the ones who will be interacting with the application to accomplish a goal or objective. One effective way to map your influencers is to bring together your team who will be gathering requirements/building the app. To determine **decision makers,** whiteboard each person you may need to interact with to deploy your app or mobile interactions. Then, chart a plan to engage each stakeholder. To determine **users,** take a similar approach. Consider the different groups of people who will use your mobile product. This may include more than just conventional users. Will there be admins, super users, or occasional users who will use the app for one specific function? Once you have listed, defined, and established users, decision makers and obtain agreement.

- Consider the range of users for your particular solution. There most likely will be readily discernable categories of users: the customer or recipient of a service, the person serving the customer or delivering the service, administrators of the whole system, auditors of the system/solution, and potentially others. Each of those categories may also have subsets of users. For example, people with particular needs driven by their specific abilities; people with varying levels of familiarity with technology; those with headquarters-related responsibilities and those in the field; groups with different degrees of access to resources (i.e., knowledge, information, time and money).

[2] https://partnership-playbook.18f.gov/4-agile/

- Once you have identified your users are, establish the relevant demographics, background (about), technology familiarity levels, their context to the project, concerns or goals in the project, their related needs, and any identifiable drivers or blockers for the project.

- Secondly, establish your constraints. What users are you allowed to talk to? How do you reach users if you cannot access them? By knowing and understanding your constraints, you can build creative methods of working around them.

- From here, think of a plan to best engage each user. This can be through targeted surveys, interviews, one on ones, academic research, focus groups, or any combination of the above. Note that in the context of the project some will be more applicable than others, and there will be constraints that limit which can be utilized.

Principle 2 - Mobile strategy should focus on the agency's digital big picture

By: Jacob Parcell, GSA

Building an application or a web site is not the only requirement for effectively managing customer experience. Consider the problem you are trying to solve and how it relates to the organization's Digital Strategy.

Mobile customer experience approaches have a tendency to focus on one app or mobile website and the user experience of that app. Sometimes, organizations venture away from their digital strategy and focus on functionality of a particular app, which can sometimes set the organization's mobile strategy. Other organizations have a popular product or section of a site and immediately set out to build a mobile application to feature this product/service without thinking about where the application fits in with the larger organizational strategy.

While it's vital to focus on the user experience of a single app, customer experience should always tie into the agency's larger digital strategy, with mobile approaches falling in line with organizational mission and outcomes. Mobile products should be a microcosm of a government organization's digital strategy, and should align with the mission and match desired outcomes of leadership. Mobile projects that are aligned well to the larger strategy generally bring legitimacy to their project and have an easier time gaining resources. In government, mobile program managers should strive to align with the larger digital strategy of the organization. In the team's experience, the digital office can exist numerous place in a government organization and the mobile program leads should work to find where digital strategy decisions are made.

This principle in practice:

- Journey mapping: As defined by 18F[3], journey mapping is a visualization of the major interactions shaping a user's experience of a product or service. Embedding the tenants of the organization's digital goals, mission and outcomes in a journey mapping exercise that considers the complete customer experience is a good way to identify mobile moments--areas where customers' may leverage mobile or other technology that can create a great customer experience. A well designed journey map should also help mobile program manager's articulate a clear view and approach to mobile that will help bring legitimacy to the approach.

- Goal setting: When designing your mobile moments[4], clearly defined goals will help your mobile strategy align to the larger digital big picture. Consider the following: What are the goals of the specific mobile product/service? How do they fit into the overall organizational goals? The specific project goals? The team goals? Where applicable, program managers should strive ask these questions of both sub-agency and headquarters agency priorities.

- Stakeholder engagement: *How soon and when should users and decision makers be involved?* The best way to include these groups in building a mobile experience is to include them as soon as the decision is made to focus on mobile experience. The earlier you can involve users from all levels of the food chain, the better. Early and constant customer engagement is one of the tenants of AGILE methods and inclusive design. This could be before the business owner even decides what type of mobile experience to create (ex. an app or a website). However, if the idea has been generated, funds delegated, and dates set, you still can involve your users! If you're struggling to think of ensuring all users are included, try and brainstorm everyone who might use the service. Will you have an admin? Are there different profiles of users?

- Feedback loops can be small: A number of government organizations have limited resources, leading them to potentially de-prioritize customer experience. While it may be challenging to allocate the time up front, ,the purpose of early planning and designing is to focus on the core of the project, narrowing down to the essential. Feedback, iterations, and exploration are vital to a successful end-user experience and this process is simplest in execution early on in the process. You just have to keep in mind: The ultimate goal is to design a product your users love. If that product is designed in a corner office without any feedback, important perspectives might be missed. And when the user gets the product, no matter how much time, care, and effort might have been put into the design, it may meet the needs of your user.

[3] https://methods.18f.gov/decide/journey-mapping/
[4] https://www.digitalgov.gov/2015/06/01/finding-the-best-mobile-moment-is-the-first-stepping-stone-to-anytime-anywhere-government/

Principle 3- Effective user experience requires honest engagement

By: Daniel Neal, Kajeet, and Kristia Hayes, DoT

You may think you know what your users want, but they probably know better. Human-centered design approaches are more successful than those that focus mainly on the technology.

Agencies serve a variety of stakeholders. Engage them in creative and innovative ways to ensure a focus on user experience. Developing holistic solutions and inclusive design to organizational and/or service problems using mobile technology (devices, wireless networks, applications, and platforms) is best achieved by first stepping into the shoes of those for whom you are solving the problem.

Think about your user base. Engage these different types of users in conversation. Ask and listen. Take notes. Build a picture you can share for feedback. Investing a modest amount of time in this activity will likely make the difference between the failure and success of your mobile solution. This will be how you approach persona research gathering.

Think of the goals of your project. Beyond having a clear picture of all the human actors in the system, have a view as to how you are seeking to change the behavior of these different types of users. This essential first step will better enable one to predict whether your mobile solution will simplify life for those affected or whether it will create new 'points of friction' or unintended outcomes.

By spending a modest amount of effort describing in writing the categories of actors affected by your envisioned solution, their expected behavioral changes - or changes in their experience and consumption of the services you are providing - one will have a strong foundation on which to construct one's technology architecture.

This principle in practice:

Fostering an environment of trust between you and the customer is essential to effectively managing the customer experience. Often people look to avoid stress or pain where necessary. Therefore, you want your environment to promote positivity and collaboration. If a customer has expressed concerns in the past and the issue(s) was/were not resolved to their expectations, it might influence your interactions moving forward. Below we have outlined a few ways to navigate the often-murky path of customer engagement, which can significantly influence customer experience.

- Engage! Engage! Engage! - Do so early and often. When determining stakeholders, define their preferred methods of communication and adhere to those guidelines.
- Be upfront and honest – if you are experiencing issues with a particular application or having

There is a fine art in gaining your users' trust and making them a collaborator.

problems implementing a new policy, say so. Most people respect honesty and openness when working toward a common goal. Oftentimes customers are as invested in the outcome as you and want/need the product/service to work well as badly, if not, more.

- Be proactive – Don't wait and engage your customer at the last minute if there is a problem. Make it a practice of informing customers of what's in the pipeline. Do periodic checkups regardless of issues. Plan bi-annual or quarterly check-ins; by doing this, you'll establish a rapport.

- Create safe spaces – It can be stressful to have a customer that expresses displeasure in every upgrade or rollout. Instead of viewing this person as a problem, seek to add this user to your test-bed. Other customers may be having the same problem, but for whatever reason won't disclose. By giving a disgruntled user a constructive format for airing their grievances you'll have added a team-member that might become a successful change agent for whatever new plans you might have.

- Acknowledge – Acknowledge customer contributions. This can be done by email or through a certificate. Be it an end-user tester or a customer that recommends application changes that are later implemented; make sure it's recognized. By doing this, you let your user's know that you are not only listening to them, but that their feedback matters and it's changing their work experience for the better.

- Get personal – Never underestimate what the sound of a human voice on the end of the phone or eye-to-eye contact in a forum can do for your customer base. Though surveys, data calls and emails are helpful, they can't replace human interaction. A customer may be willing to disclose things in a one-on-one conversation that they may feel uncomfortable expressing through.

Have the fresh eyes of a valued colleague who is independent of your project read what you've written about your proposed mobile solution. Ask them to especially hone in on your perceived positive effects (opportunities) and the impact on the lives of the various users as you've pictured them. Are these based in reality or idealistic? Use this feedback as you enter the *process* of developing, engineering, building and operating the mobile solution envisioned to better-serve stakeholders.

Finally, make sure to keep the feedback loop open. By providing structure to feedback mechanisms, you can ensure there is a good way to collect responses that you can later analyze to determine what users like/don't like. You can do this by providing your users with a mechanism or point of contact to provide additional feedback to after initial interviews have taken place.

Principle 4- Think outside of the technology box

By: Reena Vij, IBM

Don't let technology barriers confine your thinking. Start with your user's needs, then consider technologies to support it.

> 77% of users never use an app again 72 hours after downloading it

The majority of users spend 50% of their time[5] using five native apps, so it's challenging to find a native app that will engage users. In fact, they may never download or use an app from your organization. There could be a variety of reasons--lack of interest in apps, lack of space on their phone, or even previous bad experiences with native apps. Depending on your user's habits, it may make sense to build an API or a microsite for a popular app or organization to consume (i.e. build a partnership with X org to build a microsite). Mobile customer experiences are even advancing from the traditional smartphone and now include spoken word products like Alexa and Watson. Government communities are looking at building tools for these assistants which will require smart API's.

Over 50% of the C-suite are being challenged to make progress in digital business. Mobile program managers must think innovatively so users will want to adopt their tool, versus being forced to use it as part of the job role. Challenge the team to think not from the perspective of limitations of legacy systems but from the job role journey of the work that needs to be performed. Maybe rather than logging into 5 different silo systems to enter required data a field employee might be able to access a single interface that also guides the employee through the different activities that need to be done. Maybe the tool could even provide analytics or guidance on the next best actions.

Design thinking[6] is one of best tools to help think outside the box. Understanding the customer experience by developing a customer journey map will help prioritize needs, determine what is achievable and evaluate what can be accomplished with the funding available to provide the best solution.

While this concept seems simple, it is a real shift from the way agencies have been doing business. It can be much easier to continue to invest in existing systems and focus on extending to the life to meet the business need. There is a shift now to thinking from the perspective of the user and developing tools to supporting the users based on how the work gets done. The efficiencies through this process have been recognized by several agencies.

[5] See ComScore 2017 U.S. Mobile App Report http://www.comscore.com/Insights/Presentations-and-Whitepapers/2017/The-2017-US-Mobile-App-Report?
[6] https://methods.18f.gov/

Principle 5 - Think of mobility as consumers in motion

By: JC Byrne, Perfecto Mobile

Since users are on the go, you need to ensure a consistent experience across platforms, devices, geographic areas, by leveraging industry standards.

People use mobile devices on the go, so it's important to put yourself in the shoes of the modern user. Journey mapping and user interviews may not catch modern mobile habits—i.e. what your customers are using and how they are using it. How people use their phone is different from how they use traditional desktop computers . For example, people often prefer to swipe or use voice commands on their phone, which they generally can't do on desktops. If you design an app with a lot of typing, it will fail. To achieve excellent customer experience, tap into users' pre-existing habits to design the best experience for your users.

This principle in practice:
If you do decide an app or mobile website is the best approach to mobile for your organization, you should strive to have the same experience across all devices and platforms. Customer experience on mobile and web applications isn't just about good visual design and UI (layout), there are many other factors to take into account:

- How does your application run in different devices and device types? There are a large diversity of devices and operating systems. The fact is applications perform differently on:
    - Devices type: iPhone, Android, iPad, Surface Pro, etc.
    - Device version: i5, i6, i7, etc.
    - Operating System: iOS 10.2, iOS 10.3, iOS 11, etc.
    - Browser type: Internet Explorer, Firefox, Chrome, etc.
    - Network: AT&T, Sprint, Verizon, and so on.

- Beyond that, other real-world experiences need to be factored. Consider how does your application run with:
    - High/Low Wi-Fi bandwidth?
    - High/Low Battery Power?
    - Application collision… how does your app work with others running in the background?

Test coverage: One way to ensure a consistent user experience across the board is increasing the amount of test coverage. The ability to test on more end user personas that are equivalent, or near your consumer base, the less "risk" you take in regard to providing a great user experience.

User testing: Another way to ensure a good user experience is to test your app against how your users will rely on it. During your journey mapping, you may have discovered one of your

users is always on the go while a different user sits at his or her desk most of the day. By considering each of your users' unique habits and comparing these habits to what the app offers and adjusting accordingly, you can better ensure a great experience for all users.

Compatability Testing[7]: Compatability testing focuses on determining if the hardware and software display and allow the application to function properly. Mobile compatibility testing is checking or validating that your application behaves as expected across the combination of mobile devices and browsers that your customers will be using to access your application.

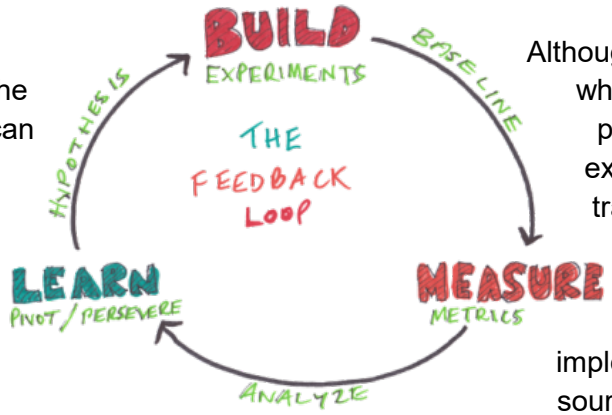
In the end, you need to determine what amount of "risk" you're willing to take by the amount of coverage you take on and how you plan for the varied mobile landscape.

Principle 6 - Good mobile experience changes in real time

By: Brian Lacey and Joshua Lilly, Mobomo

Mobile analytics is a daily or hourly pursuit, not a monthly spreadsheet.

Since user experience is vital to the success of a Web/mobile system, it is critical to establish feedback loops to inform potential changes. There are multiple methods for effective feedback loops, both involved and automated, with users regarding their experience.[8]



Although user experience is somewhat subjective on the whole, metrics and analytics are one method that can provide objective feedback and insight into user experience effectiveness trends. Analytics has traditionally been most utilized for marketing purposes, informing strategy, implementations, and trends. However, more and more user-experience implementations are relying on this quantitative data source to aid in project research and design. Modern system analytics are key to tracking the user experience and should be reviewed daily when available. Utilizing the data effectively and efficiently through a well-designed system can successfully change a user's experience (in some cases real-time) for the better.

This principle in practice:

In order to analyze metrics and data effectively, success objectives must first be established. How do you define success? To begin, here are some example goals for establishing a project's user experience success:

[7] https://www.digitalgov.gov/2015/08/14/what-is-mobile-device-compatibility-testing/
[8] https://365andrewssketches.files.wordpress.com/2013/01/bml-loop-2-1.png

1. 100 new registered users per month
2. 70% average user retention rate per month
3. Mobile experience consistent across all supported mobile devices

Initially, one effective strategy to measure success of a project's designed user experience, is to select a few key metrics and focus on them over time. One of the most prominent issues with analytics is that without proper direction, they can become a distraction or data without any context or actionable interpretation. Mobile analytics is data, only becoming valuable information when utilized in some way that furthers an agencies goals. The question then comes down to: What set(s) of analytics data is relevant to the project context? Why is the project gathering and tracking metrics to begin with? These are perfectly understandable questions and key to establishing an effective user experience feedback loop with any project.

These are high-level objectives that are established and agreed upon by the project's organizational stakeholders as measures of success. With established success measures, here are some example categorizations of relevant user experience analytics implementations:

- **Notifications** of blockers to the system's essential flows.
- **Identification** of root causes to blockers.

Notifiers provide continuously monitored information hourly, daily, or weekly. The analytics can be used to define specific issues or provide supporting information as insight to guide further investigations. Examples of potential notification analytics:

- Unique page views over a defined period of time
- Average time on page per session
- User actions (defined and tracked, - user clicks on a button, download of a PDF, filling out a form, etc.)

Identifiers are analytics implemented and used in conjunction with investigations of issues. These fall under several categories themselves, listed here, but not limited to: traffic issues, technical issues, content related issues, navigation issues, and UI design issues. Here are some examples, with their equivalent Google Analytics (GA) implementations as a starting point:

- **Traffic**: to determine if there is one traffic source that is responsible for any changes in page views.
    - GA: *Pages* - Unique Resource Indicator with Source as secondary dimension
- **Technical**: determine if there are any UI elements that are broken or non-functional
    - GA: *Event Pages* - tracking of the pages with defined User actions (see above)
- **Content**: determine if taxonomies or other media is confusing users
    - GA: In-Page Analytics - percentages for links clicked by users
- **Navigation**: determine if specific buttons or menus are not being utilized correctly

    - GA: *Pages* - Unique Resource Indicator with Navigation Summary as secondary dimension
- **UI Design**: fonts, UI elements, buttons, view layout, or other media is confusing intended user-flows
    - GA: In-Page Analytics - percentages for links, or heat maps, clicked by users
- **What they're saying**: Don't forget that user comments and feedback can also tell you how users feel about your work
    - GA: Comments on app review pages, emails to help desk, etc.
    -

Once a targeted core set of analytics has been implemented and monitored, a basic feedback loop will have been established. These analytics and data can then be utilized by the project team to evaluate opportunities to improve user experience. Does the experience need to change? How should it change? Does the information available warrant additional user testing? Specifically, does it call for A/B testing?

Conclusion

In summation, customer experience is one of the most important considerations when addressing mobility. This playbook set out to give program managers and their leaders some tips on how to make sure organizations can serve their mobile audiences appropriately. Customer experience should always tie into the agency's larger digital strategy, with mobile approaches falling in line with organizational mission and outcomes. When creating mobile moments, ensure they align with larger organization goals. Remember that users can feel a personal connection to their device and they can be finicky about the apps they download and the public websites they visit, so their input is integral to a successful deployment. By defining and speaking to a large range of users, creators of mobile moments can better increase adoption by understanding users' needs.

Furthermore, the ease and frequency of use of the mobile device in our personal lives is a much easier and richer experience than the restricted use in our business environment. This generates higher expectations of our users. If a business mobile app can give us the similar ease of use experience, it will have a huge impact on adoption rate and a reduction in transition time. A small amount of investment upfront in considering the behavior of the user can save agencies a lot of money and result in the avoidance of failed implementations and hours of re-work.

To start adopting customer experience best practices, work with people who are passionate about learning from their users and make sure you work across traditional boundaries. Discuss best practices provided in this document and how they might apply in your organization. Mobile technology is ever-changing so be sure to check out the latest user trends. We realize that each organization's mobile journey will have twists and turns. We consider this is a living document so if you pick up something new from one of these approaches, let us know and we'll add it.

We wish you and your team much luck in your mobile journey!

Glossary of Terms

Term	Definition
Application (App)	A software program that's designed to perform a specific function directly for the user or, in some cases, for another application program. Includes, but is not limited to: Web browsers, e-mail programs, word processors, games, utilities, etc. The word "application" is used because each program has a specific application for the user.
ATARC	**Advanced Technology Academic Research Center (ATARC)** is a a 501(c)(3) non-profit organization that provides a collaborative forum for Federal government, academia and industry to resolve emerging technology challenges
Customer Experience/Xperience	The sum total of a stakeholder's feelings towards their mobile experience from end-to-end. This includes but is not limited to dispositions toward application development, mobile device usability/suitability, implementable standards, etc
Customer Relationship Management (CRM)	A term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers, assisting in customer retention and driving sales growth.
Decision Maker	A person who decides things, especially at a high level in an organization. Decision makers are also considered "stakeholders."
Feedback Loops	A process where a provider seeks information from their customers and that information is then used to impact the performance of the provider.
ITIL	Information Technology Infrastructure Library, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.
Journey mapping	A visualization of the major interactions shaping a user's experience of a product or service. A customer journey may contain several diagrams that depict the stages that customers go through in interacting with a company, from buying products online to accessing customer services on the phone to airing grievances on social media.
Mobile	Generally refers to a hand held device that provides a connection to the Internet for web browsing and email and/ or allows for voice calls. Tablets, e-readers and smartphones are all mobile devices.

MSCT	Mobile Services Category Team (MSCT) works to support an agile and evolving federal workforce that seeks to meet their missions, and do their work, securely anywhere, anytime, and on any device in order to serve U.S. Citizens
Platforms	Any hardware or software used to host an application or service. An application platform, for example, consists of hardware, an operating system and coordinating programs that use the instruction set for a particular processor or microprocessor.
PMBOK	Project Management Body of Knowledge (PMBOK Guide) is a book which presents a set of standard terminology and guidelines (a body of knowledge) for project management.
PMI	The Project Management Institute is a US nonprofit professional organization for project management. The PMI provides services including the development of standards, research, education, publication, networking-opportunities in local chapters, hosting conferences and training seminars, and providing accreditation in project management.
Stakeholder	An individual, group, or organization, who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project.
Testing	Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation.
User Interface (UI)	Visual part of computer application or operating system through which a user interacts with a computer or a software. It determines how commands are given to the computer or the program and how information is displayed on the screen.
Users	The persons operating or using a mobile device or application to accomplish a goal.

Contributors

Brian Lacey, Mobomo Inc.

Joshua Lilly, Mobomo Inc.

Daniel Neal, Kajeet Inc.

Greg Hixon, GSA

JC Byrne, Perfecto Mobile

Kelly Adams, GSA

Lizzie Berkovitz, Blackstone Technology Group

Robert Duffy, DHS

Kristia Hayes, DOT

Michael Pulsifer, DOL

Reena Vij, IBM

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Device-as-a-Service (DaaS)

Working Group Document

Device-as-a-Service Overview and Requirements

1 Device-as-a-Service Overview

1.1 Overview

The Federal Government is becoming increasingly reliant upon mobility, now with approximately 1.5 million mobile devices in service costing the government over $1 billion annually for service alone. Mobility usage across the government has a wide range of diverse profiles from general business use to mission critical, high security. There is an increasing need for the Federal Government's mobile device management processes to be further improved due to increased security risks and broader use of mobile solutions.

The Category Management Leadership Council (CMLC) and the Office of Management and Budget (OMB) established and began the implementation of a Category Management strategy across the federal government identifying 19 Common Government Spending Categories. In 2016, OMB established the Mobile Services Category Team (MSCT), made up of Agency representatives across the Federal Government, to address cross-government requirements for next generation mobility. The MSCT is tasked with, among other responsibilities, establishing requirements for both core and sub-components of mobility. As such, it is the responsibility of the MSCT to establish the minimum baseline Enterprise Mobility Management requirements.

1.2 Purpose

The primary purpose of this Device-as-a-Service requirements document is:

- State the minimum set of requirements across the Federal Government for Device-As-A-Service (DaaS) specifically in the managed mobility environment.
- This document is not intended to address or in any way cover Device-as-a-Service in other managed categories.

This document establishes minimum DaaS requirements on a broad government-wide basis. Individual agencies will determine the full extent of requirements for their respective device selection and management needs. Within this context, it is also important for the Federal Government to continue to reduce costs and to both improve and simplify the acquisition and management processes for mobility and related services.

This working group document includes documentation from the United States Census Bureau (USCB) Decennial Device as a Service Request for Proposal dated December 2016. The USCB RFP included a thorough and in-depth process of documenting government requirements for DaaS and covered extensive detailed requirements specific to USCB. The attempt in this document is to utilize the content from the USCB RFP that can be generalized to government-wide requirements. When government agencies issue their respective RFPs, additional levels of

detail will need to be added to address individual Agency use cases, deployment, maintenance, and management requirements.

Additionally, the MSCT has identified an approach to the acquisition and management of mobility services that are intended to simplify mobility acquisition while enhancing cost savings. Device-as-a-Service has the potential to meet the three primary criteria of Mobile Strategy -- **Simplicity**, **Savings**, and **Standardization**.

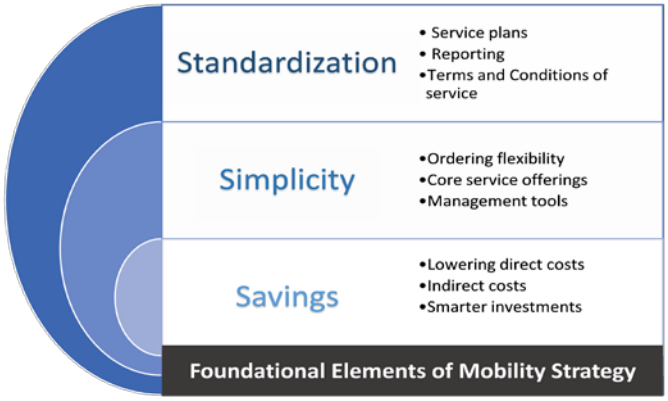


Image 1.1, MSCT Elements of Mobile Strategy

2 Definition

Definition: **Device-as-a-Service (DaaS)** includes end-to-end device supply, service, and management to include:

- Planning and Management of Agency DaaS Solutions
- Device Provisioning, Kitting, and Delivery
- Mobile Device Management and Device Refresh
- Ongoing Helpdesk Support
- Logistics for end-of-life disposal / recycling
- Wireless Carrier Network Services (may or may not be included)

DaaS is more common in the computer hardware environment than in mobile devices but as Wireless Carriers decouple Wireless Carrier Network Services from the inclusion of subsidized mobile devices, it is expected to become a more common device delivery model.

DaaS service plans can vary based upon the overall set of Agency needs and the agreement terms with the DaaS service provider. Typically, DaaS service is determined by detailed mobility needs including identifying network coverage requirements; device technology, features, and benefits; determining the initial time period for the length of service; and agreeing on a monthly fee on a per device basis for the provider to deliver a the specific devices and related management services.

2.1 DaaS Background

Historically, the device, hardware, or equipment as-a-service concept has primarily been applied to computing devices in the government or enterprise environments. There are similarities to PC-as-a-Service (PCaaS), and Hardware-as-a-Service (HaaS). In the IT environment, the primary reasons Agencies and enterprises prefer to pay a monthly fee for devices, hardware, or equipment instead of purchasing and owning them can also be applied to DaaS:

1. **Ability to Scale** - Flexibility in scaling the needed devices to changing workforce levels provides efficiency
2. **Limited Internal Resources** – Third party planning and management of mobile devices eliminates the internal strain on staff resources.
3. **Budget Structure and Flexibility** – DaaS allows an enterprise to move the outright purchase of devices from capital budget to an operating expense, which for government purposes is an annual spending allocation.
4. **Asset Obsolescence** – Ability to refresh devices more quickly and to easily dispose of and recycle older devices gives an Agency newer technology on a regular basis and eliminates the labor-intensive process of device disposal.

Many companies with hardware and equipment divisions such as HP and Microsoft are introducing new DaaS business models and programs to meet evolving government and business enterprise needs. HP has historically offered Hardware-as-a-Service in its printing division and is moving that concept to other hardware including a recent business partnership with Apple. Microsoft has also recently introduced a DaaS program for its Surface devices. It is expected that DaaS programs will continue to expand into the mobile environment as Wireless Carrier business models evolve to reduce or eliminate equipment subsidization and as companies and government agencies seek more flexible alternatives to purchasing mobile equipment and to addressing mobile device obsolescence.

The historical business model for mobility devices and services has been a monthly fee charged for a specific time period, which included the combination of Wireless Carrier service, a subsidized device, and the timeframe for which a device refresh or replacement could occur. This combination of service and device for a monthly fee generally included some aspects of device maintenance or replacement for device malfunction provided by the Wireless Carriers. In Federal Government procurement some agreements between the Agencies and Wireless Carriers as well as third parties such as TEMs providers, reflect certain aspects of the developing DaaS model. Additionally, there are aspects of MDM that overlap with a formal DaaS end-to-end device management solution.

2.2 DaaS Value Proposition

There are specific differences between the historical Wireless Carrier / mobility services model of a subsidized device coupled with wireless service and the formal DaaS solution. DaaS, in the mobile sector, is in early development and will evolve to meet changing customer requirements. There are many variations in the range of services provided under DaaS solutions.

DaaS holds the potential to provide the federal government with increased value in the wireless carrier service category. The DaaS Value Proposition may be impactful in four primary areas. Each Agency will need to develop its own tracking and evaluation process to determine the true positive impact:

- Lower Total Cost of Ownership (TCO)
- Improved user experience
- Increased productivity

- Flexibility without commitment to a specific carrier plan

The Feature Comparison Table highlights the differences between the Device-as-a-Service model and the historical Wireless Carrier Services model. The three most significant differences between the models are 1) device cost transparency, 2) single source device management, and 3) the extent of device management services provided.

Feature Comparison Table		
Feature	DaaS	Wireless Carrier Model
Stated monthly device fee	Y	N
Stated wireless services fee	Y*	N
Delivery	Y	Y
Configuration	Y	Y**
Deployment	Y	Y**
Device management	Y	Y***
Maintenance / Replacement	Y	Y**
Disposal / Recycling	Y	Y**

* DaaS solutions and Wireless Carrier services may not come from the same provider
** Services may be provided but often via multiple vendors not from a single source
*** Federal government agreements often require the replacement of devices if malfunctions occur but not always end-to-end device management by a single provider.

The DaaS model may offer the Federal Government increased flexibility and cost control especially as Wireless Carriers move to reduce or eliminate the subsidization of mobile devices. Since DaaS is still in the early stages of both introduction by providers and customer adoption, the current challenge is in finding DaaS solution providers that will offer the full set of end-to-end mobile services as defined within DaaS requirements.

The current mobility procurement model typically includes the following activities, means, timeframes and costs:

Current Mobility Procurement Model		
Procurement Activities	**Contract Vehicle**	**Estimated Procurement Time and Costs***
Procure Wireless Service (SED) • Smartphones, tablets, other connected devices	GSA, NITAAC, SEWP, Non-Commercial, OM	2-8 months ~ $62.5K-$250K
Procure Non-SED Device • Smartphones, tablets, other connected devices	SEWP, Open Market (OM)	1wk-2months ~ $10K-$62.5K
Procure EMM License • MDM, MAM, MCM, MAS	GSA, NITAAC, SEWP, OM	6-12 months ~ $188K-$375K
Procure productivity apps / software • e.g. Outlook, Office, Dropbox, Anywhere	GSA, NITAAC, SEWP, OM	6-12 months ~ $188K-$375K
Procure Infrastructure / Security SW • MSM, MTD (e.g. Lookout, Checkpoint)	GSA, NITAAC, SEWP, OM	6-12 months ~ $188K-$375K
Procure Accessories • Case, Bluetooth, Ruggedized Gear, Etc.	GSA, NITAAC, SEWP, OM	1wk-2months ~ $10K-$62.5K
Procure Mission Components • CAC/PIV, Derived credentials	GSA, NITAAC, SEWP, OM	12-18months ~ $375K-$563K
Support Services	Direct w/Agency IT, Helpdesk	$1M-$3M per year**

• Care, Tier 1, Helpdesk, Connectivity		
TOTAL		$2M-$4.7M

* Estimated Procurement Costs are based on 2.5FTE at $150,000 annual Salary. These estimated costs are extremely conservative and actual costs can be safely assumed to be much higher when including the work completed by the following individuals and activities: CO, CS, Branch review, legal review, COR, IT Program review, CISO review, functional requirements development, security requirements development, acquisition planning and execution, post award execution.
** Cost estimation an extremely conservative figure. More analysis required to determine operational costs associated with the management of each individual buy.

The procurement process is greatly simplified for the individual agency within a DaaS model because many of the individual procurements are eliminated or combined. In fairness to the current model, there are ways for individual agencies to also accomplish the reduction in procurement steps such as working with TEMs or Integrators versus conducting or managing the entire procurement internally. In comparison, the DaaS model may look much more simple - like the following in a procurement scenario:

DaaS Procurement Model		
Procurement Activity	**Available Contract Vehicles**	**Estimated Procurement Time and Costs***
Procure DaaS Combined Device and Services (Turnkey Solution – eliminates a-la-carte procurement) • **Device** • **EMM** • **Security / Infrastructure** • **Productivity SW** • **Accessories** • **Mission Components** • **Support and Connectivity Services**	GSA, NITAAC, SEWP	12-18mos ~ $375K-$563K

2.3 Added Value of DaaS

For government agencies, an expanded list of DaaS benefits may include the following:

1) Cost Transparency: Device and service cost transparency – separate distinct changes for network services and mobile devices
2) Variable Cost: Agencies may scale up or scale down device deployments as the employee base changes or seasonality impacts needs – mobile costs become more variable rather than fixed.
3) Device Refresh: Organizations can refresh devices more quickly, upgrade to new technologies, and will not be responsible for managing, maintaining, or disposing of devices.
4) Device Remain Operating Expense: As Wireless Carriers move to eliminate device subsidization, DaaS can allow organizations to maintain the device cost as an operating expense and eliminate the need to acquire and own devices.
5) Improved Resource Allocation: Agencies can concentrate human resources on mission critical tasks and potentially significantly reduce the need for using internal resources for mobile management – saving valuable time, money and the management resources to handle day-to-day management of mobile devices.

6) Mobile Device and Usage Modeling: Agencies will not need to conduct forecasting of the device refresh cycles but can rely on a third party to build it into their DaaS pricing and management model
7) Improved Employee Experience: DaaS service providers will be required to keep all mobile devices maintained, refreshed, and compliant with the contract agreement.
8) Simplicity: An option of one simple, single-contract for all device management services

As DaaS becomes a better-known and understood concept in mobility and more organizations express a need for these services, providers will emerge and grow. Current TEMs or MDM providers may take on the expansion to true DaaS services.

3 DaaS Vendor Responsibilities

The Vendor is responsible for providing all products and services in an agreement and shall be responsible for performance of all Vendor obligations under the terms and conditions as established and agreed upon between the Agency and the Vendor. The Vendor shall be responsible for providing all supplies and furnishings needed to accomplish the tasks in an agreement.

It is recommended under a DaaS agreement that the terms and conditions state clearly the management and reporting requirements needed to facilitate and simplify administrative essentials for the Agency. Table 1.7.1 Vendor Deliverables lists the generally required reporting and management documents. All reports and management plans will not be required for all DaaS agreements and deployment. The scale and volume of devices will determine the collective Vendor Management and Reporting Requirements.

3.1 Vendor Management and Reporting Requirements

Vendor Management and Reporting Requirements		
Item	**Title**	**Primary Purpose**
01	Project Management Plan	Documents the Vendor's approach and processes for managing the contract and delivery of services, and establishes agreements regarding joint contract management controls.
02	Subcontractor Management Plan	Documents the relationship with subcontractors and methods by which the primary contractor will ensure the production of quality deliverables from sub-contractors
03	Project Schedule	Provides a comprehensive breakdown of all activities that will be executed under the contract.
04	Monthly Status Report	Reports progress against plans, identifies issues and required actions, and includes specific service delivery statistics to support invoice validation and performance assessment.
05	Bill of Lading	Documents the content of each shipment to/from the Agency and its offices and or employees
06	Device Sanitization Log	Reports the status of complete data sanitization of mobile devices 3

Vendor Management and Reporting Requirements		
Item	**Title**	**Primary Purpose**
		days after the Vendor receives them.
07	Inventory Report	Reports the period status of all mobile devices – this may be monthly, quarterly, or after any systematic device refresh or collection process.
08	Wireless Carrier Network Coverage Analysis Report	Details the approach, methods, test results, hardware requirements, and recommendations for Wireless Carrier network coverage.
09	Asset Management Plan	Documents the Vendor's approach to performing end-to-end location and status tracking of all mobile.
10	Technology Refresh Plan	Documents the approach to addressing any software or hardware upgrades that become necessary and the process that will be used to collect and redistribute mobile devices to all end-users.
11	Risk Management Plan	Documents the approach to ongoing risk identification, assessment, and response and includes a risk tracker that includes all identified risks and their associated mitigation strategies.
12	Quality Management Plan	Documents the processes for conducting quality control throughout all phases of the device logistics process and provide checklists of specific quality control requirements.
13	Shipping Analysis Report	Details the recommended shipping methods based upon analysis of all available shipping methods given the delivery constraints.
14	Logistics Support Plan	Documents the Vendor's end-to-end logistics process that includes staging, provisioning, kitting, packaging, shipping, replacing, and decommissioning.
15	Mobile Device Management Plan	Documents the processes for MDM solution operations, mobile device and application updates, and help desk support for AGENCY personnel.
16	Project Dashboard	Provides a functional, near real-time view of device logistics, asset management, Wireless Carrier usage, and issues to allow AGENCY to monitor the status of ongoing operations.

The Vendor shall deliver contract-required plans, reports, and supporting documents in accordance with those elements in the table "Vendor Management and Reporting Requirements" as agreed to between Agency and the Vendor.

3.2 Period of Performance

The periods of performance for DaaS tasks and delivery should be clearly stated in an Agency requirements document, RFQ, or RFI.

4 Device-as-a-Service Objectives

The key objectives of DaaS are to simplify mobility acquisition, management and reporting; to reduce overall mobility cost through more efficient service management, and to deliver mobility

devices and services to the right locations, at the right time, that are fully functional to begin operations immediately out of the box.

Agencies should expect the following outcomes:

- **Mobile Device Acquisition:** Mobile devices that meet Agency usability, performance, and security requirements are identified and acquired (this includes smartphones, tablets, and other mobile devices) by the Vendor.
- **Mobile Device Provisioning:** Mobile devices are securely provisioned, kitted, and configured prior to deployment to multiple geographically dispersed locations.
- **Mobile Device Management:** A Mobile Device Management (MDM) solution is established, which manages all mobile devices and applications, performs remote sanitization of devices as necessary, and adheres to all security requirements as defined in the agreement.
- **Logistics:** All mobile device kits are distributed to the proper Agency personnel. Defective or damaged mobile devices are collected and replaced in a timely manner.
- **Wireless Carrier Network Coverage:** Continuous reliable Wireless Carrier network coverage is provided to all mobile devices.
- **Quality Assurance:** A Quality Assurance (QA) process is followed to ensure that 100% of devices have been tested prior to kitting and regular Quality Control (QC) checks have been conducted on all components of the logistics process
- **Asset Management:** The inventory of all accountable property is tracked and reported upon for the lifecycle of the contract from initial distribution, to replacement of defective, damaged, or missing devices, to final collection upon completion of the contract.
- **Project Dashboard:** A role-based, near real-time view of device logistics, asset management, contract deliverables, and issues is provided to specified Agency personnel.
- **Technology Refresh:** An assessment of all hardware and software is conducted every six months to determine if any upgrades are needed based upon technology innovation, age of the devices, condition of the device or operating system in use.
- **Decommissioning:** All mobile devices are collected, securely sanitized of all Agency and government data, and evidence is provided to the contracting Agency that all mobile devices have been cleansed of all government data.

The Vendor is responsible for ensuring the secure provisioning of Agency provided device images, profiles, and the secure enrollment of the devices in the MDM solution. Additionally, the Vendor is responsible for supporting Agency security plans, processes, and activities as identified in the Agency / Vendor Agreement.

5 Device Selection

As identified in the Mobile Services Category Team's (MSCT) Device Procurement and Management document issued in November 2016, Agencies must identify their specific device features and configuration requirements by evaluating usage profiles, environments, and technology needs. Agencies should collaborate with the DaaS provider to determine device requirements. In working with a DaaS provider, Agencies should evaluate the following conditions and context to determine the appropriate devices for their respective Agency:

- Expected Device Use
    - Develop use case scenarios and determine which of the three primary profiles or combination of profiles best address mobility use within the Agency:
        - General use – standard wireless use of voice, text, and mobile data
        - Vertical application use – specialized use to address a particular situation, activity, and environment
        - Custom solution – combined service, device, and software by an integrator or other service provider, which requires custom development and enhanced devices
- Device usage environment and frequency of use
- Connectivity requirements
    - Voice and data, voice only, or data only services
    - Coverage – urban, rural, or highly remote, CONUS, OCONUS
    - WiFi connectivity and calling
    - Tethered services or hotspot capability
    - Simultaneous use of both voice and data
    - Customized connectivity solutions
- Device cost parameters, which will be amortized in the monthly DaaS service fee
- Device requirements, options, features, and functionality
    - Smartphone, feature phone, or data only device
    - Data storage capacity
    - Operating system (iOS, Android, Windows, or other)
    - Mobile security or other software requirements (some software may only be available for select operating systems or versions)
    - Size and weight
    - Screen size and technology requirements (primarily indoor or outdoor use)
    - Mobile applications from major app stores (use and support needs)
    - Camera and camera focusing speed and photo quality
    - Battery life
    - Device color (some colors or device finishes incur a premium price)
    - Other special conditions
- Device or usage requirements critical to mission success
- Projected device life and required refresh cycle
- Validate device alternatives against the National Information Assurance Partnership (NIAP) Protection Profile for Mobile Devices Fundamentals (see below).
- Documentation of requirements aligned to OEM, mobile device model, OS version, and device generation

Further, it is advised that Agencies select mobile devices through the DaaS provider that meet technology specific security requirements through the evaluation and certification by NIAP (National Information Assurance Partnership) against a NIAP-approved Protection Profile. The devices meeting this requirement are a combination of approved hardware and OS versions. The list of compliant devices may be found at the NIAP website[1].

[1] https://www.niap-ccevs.org/Product/

6 DaaS Scope and Tasks

In a Device-as-a-Service relationship, the Vendor's role, and responsibility is to plan, manage, and deliver mobile devices and mobile device related services for all mobile-enabled devices included in the Agency / Vendor DaaS agreement.

The scope of DaaS is divided into 6 distinct but interdependent requirements in the form of tasks:

Task 1: Device Provisioning and Kitting

Task 2: Wireless Carrier Network Services

Task 3: Logistics

Task 4: Mobile Device Management

Task 5: Planning and Management

Task 6: Ongoing Support

6.1 Task 1: Device Provisioning and Kitting

Mobile devices will be used in geographic areas and in functional cases as described in the agreement. Typical users will include Agency management, office personnel, field and remote employees, and government contractors. In addition, home-based telecommuting environments may require smartphones, tablets, or AirCards for laptops.

The Vendor shall collaborate with Agency personnel to identify and recommend devices that meet all functional, technical, connectivity, and security needs. The Vendor shall acquire and provision all devices and provide the related accessories in individual smartphone, tablet, or AirCard kits that will be provided to the Agency as a service.

All smartphones, tablets, and other mobile devices shall be provisioned and kitted prior to distribution to the Agency employees or designees as directed within the agreement. All devices shall be inventoried and tracked and appropriate reporting provided via Vendor Management and Reporting Requirements.

6.1.1 Example Kits - Smartphone

- Provide smartphones, which:
  - Are all the same make and model per technology refresh cycle
  - Are black, silver, or white
  - Run the same major version of operating system (minimum of iOS 10 or Android 6) per technology refresh cycle as directed by Agency per technology refresh cycle
  - Are no more than two (2) years old
  - Are provided in new or like-new condition to end-users
  - Have a minimum of a 4.5-inch touchscreen
  - Include Bluetooth, Wi-Fi, and 4G LTE or higher capabilities
  - Are capable of full-device encryption at the Federal Information Processing Standard (FIPS) 140-2 or greater level at the time of contract award
  - Have a minimum of 1 GB of memory

    - Have a minimum of 16 GB of storage
    - Include a camera (rear and front)
    - Have a dedicated Global Positioning System (GPS) chipset
    - Are fully supported by the cellular carriers, the Original Equipment Manufacturers (OEM) manufacturers, and the operating systems for the duration of 2020 Census Operations
- Provision each smartphone prior to kitting:
    - Configure smartphones with the Agency provided smartphone software configuration and technical instructions
    - Enroll all smartphones in the MDM solution
    - Install and activate Subscriber Identity Module (SIM) cards in all smartphones according to the selected cellular network carrier for the area in which the smartphone will be deployed
    - Charge smartphones so that end-users receive the smartphones with at least a 75% battery charge
- Assemble each smartphone kit with:
    - Smartphone in a kit box
    - OEM or manufacturer-certified Universal Serial Bus (USB) wall adapter and USB power cable
    - OEM or manufacturer-certified car charger
    - OEM or manufacturer-certified earbuds
    - Same-brand or manufacturer-certified smartphone cases (black, silver, or white)
    - Agency provides current end-user documentation, which may include initial phone use materials and instructions to begin employee use of the smartphones
    - Printed label on exterior of kit box indicating type of kit
- Provide a mechanism to be placed on the outside of each smartphone kit box to allow for physical tracking of the kit to ensure delivery, assignment to end-user, and location throughout the flow of inventory
- Provide a mechanism on the back of each smartphone (e.g., not the case) to allow for physical tracking of the smartphone to ensure delivery, assignment to end-user, and location throughout the flow of inventory
- Ensure that the outside tracking mechanism on each smartphone kit box matches the tracking mechanism that is placed on the back of each smartphone within the respective kit
- Provide the following optional accessories upon Agency request:
    - OEM Portable Battery
    - Same-brand or manufacturer-certified stylus
    - 4G LTE (backwards compatible to 3G) Wi-Fi Hotspot (must have a minimum of 15 device connections, a minimum of a 10 hour battery life, and be chargeable via a wall charger and/or USB cable) for each cellular carrier used
- Verify all accessory specifications for all smartphones with Agency prior to ordering any accessories
- Adhere to all smartphone provisioning and kitting instructions in the ***Logistics Support Plan***, as identified in Table 1.7.1

- Conduct QC checks on 100% of smartphones according to ***Quality Management Plan***, as identified in Table 1.7.1
- Provide a sampling of smartphone kits upon Agency request prior to delivery of any kits to allow for Agency verification of QC checks
- Perform a device sanitization and factory reset (in accordance with National Institute of Standards and Technology (NIST) 800-88 Rev 1) on every smartphone prior to reconfiguration and redistribution and upon final closeout of the contract
- Document all device sanitizations in the ***Device Sanitization Log*** within three (3) days of receiving a smartphone (AGENCY must approve all entries entered into log via electronic verification)
- Perform QC checks on 100% of smartphones after sanitization to ensure successful removal of Agency data from smartphones
- Provide the customer Agency and other Government Agencies access to audit all provisioning and kitting facilities and processes at any time
- Collaborate with and receive approval from the Agency to update smartphone requirements as technology innovation drives the need for updated requirements

6.2 Task 2: Wireless Carrier Network Service

Agency's mobile devices require consistent and predictable Wireless Carrier voice, text, and data services across all defined geographies and use cases. The Agency strategy is to use a cost-benefit analysis to determine the best Wireless Carrier network for Agency employees across the entire country or more narrowly defined geographies stated in the agreement.

Agencies may require multiple Wireless Carrier network providers to meet this objective depending upon personnel or mission critical locations. Additionally, Wireless Carrier usage varies from user to user so the Vendor (or Agency in the case of separate providers) should evaluate pooling of plans, stadium plans, or other service optimization solutions.

6.2.1 Cellular Network Carrier Analysis

- As needed by the customer Agency, the Vendor shall provide an independent analysis of the cellular network coverage across the required geographic coverage areas using heat maps, telecommunications testing standards, and other applicable methods
- Include the geographic factors, cost-benefit analysis, and the determination of which carrier is appropriate (including a backup carrier) for segmented geography areas in the analysis
- Document the approach, methods, test results, separate hardware requirements (e.g., separate SIM cards), and recommendations for the best local cellular network carrier in the ***Cellular Network Coverage Analysis Report***, as identified in Table 1.7.1

6.2.2 Smartphone Cellular Network Services

- Place all Agency phone numbers on the national do-not-call list
- Provide a caller ID feature that identifies all outgoing calls as from the Agency
- Provide phone numbers which have not been used for the past six (6) months

- Provide preconfigured voicemail services for each mobile device number in English (U.S.) and Spanish
- Provide optimal voice, text, and data cellular services for all Agency required locations
- Provide all smartphones with a minimum of 2 GB of data per device per month
- Provide and limit international calling as an Agency requests and documents within the agreement
- Inform the AGENCY of any carrier network problems (any issues that could impact performance) by zip codes within 1 hour and communicate overall status/progress to the AGENCY and designated Agency technical staff on a weekly basis through the ***Project Dashboard***
- Establish and maintain a Service Level Agreement (SLA) for required cellular network voice, text, and data availability based on the results of the Vendor's ***Cellular Network Coverage Analysis Report***
- Acquire prior written approval from the AGENCY for all satellite and roaming connections
- Terminate all services within three (3) days of decommissioning devices
- Provide written notification informing the AGENCY of the termination date and time of voice, text, and data services for each smartphone upon final close out of the contract and provide continuous access to individual smartphone termination data through the ***Project Dashboard***, as identified in Table 1.7.1

6.3 Task 3: Logistics

An Agency requires that all mobile devices be delivered to the correct location within the appropriate timeframe for the respective operation. The Vendor must have deployment and shipping capabilities to supply devices on a timely basis to a broad range of locations as defined in the Agency / Vendor agreement.

Any faulty or malfunctioning devices must be returned to the Vendor, decommissioned properly (tracked and sanitized), and replaced (in the possession of the end-user) within 48 hours of notification or other timeframe as agreed upon to meet Agency needs. Per the MSCT Device Procurement – Management Guidance, Guideline #3, Agencies should require any malfunctioning device with a new like-for-like or newer device.

It is recommended that Agencies require access to a comprehensive asset management system to track and maintain all of the mobile devices and accessories provided within the DaaS agreement. The Vendor shall propose an appropriate asset management system that they will maintain responsibility for and allow on-demand access to the designated Agency personnel. Some Agencies may require use of a specific asset management system, which should be identified and stated in the agreement.

6.3.1.1 Vendor Shipping Requirements

- Device kits are to be shipped in accordance with the quantities and locations provided by the Agency.

- Define and document the contents of the ***Bill of Lading*** which will be used to accompany all kit shipments
- Provide an electronic copy of the ***Bill of Lading*** to the Agency and the person(s) designated to receive at the time of each shipment, in accordance with the ***Logistics Support Plan***.
- Procure all expendables (e.g., boxes, packing paper, and bubble wrap) required to deliver logistic and device management support in accordance with the ***Logistics Support Plan***.
- Ensure that all devices are properly secured from damage during handling and transit and meet a 98% acceptance level at time of receipt

6.3.1.2 Vendor Asset Management Requirements

- Develop and maintain an ***Asset Management Plan*** that includes end-to-end location and status tracking of all mobile devices and any other Agency required fields.
- Develop a system to perform continuous device tracking as outlined and agreed to in the ***Asset Management Plan***
- Collaborate with and receive approval from the Agency on Vendor asset tracking system that the Agency personnel can access
- Acquire an Authorization to Operate (ATO) from the Office of Information Security (OIS) for all necessary components of the device tracking system
- Provide the Agency with the solution required to track devices throughout their lifecycle (e.g., using the ***Project Dashboard*** or another interface with the tracking system)
- Maintain the tracking system and perform troubleshooting as necessary to ensure that Agency personnel are able to successfully use the tracking system for the entire duration of the contract
- Perform monthly inventory reconciliations to determine if any devices are unaccounted for.

6.4 Task 4: Mobile Device Management

The Vendor shall operate and maintain an MDM solution capable of effectively and securely managing and provisioning all mobile devices. The Vendor shall provide the Agency personnel with access to the MDM solution, as needed depending upon further agreement regarding Agency assistance in Tier 1 Help Desk Support.

6.4.1 Mobile Device Management

It is recommended that Agencies that are engaging in Vendor relationships for Device-as-a-Service and are including Mobile Device Management (MDM) as a component, refer to the MSCT Enterprise Mobility Management EMM: MDM, MAM, and MCM Requirements document to serve as a basis for Mobile Device Management solutions.

Broad criteria as identified in the MSCT Enterprise Mobility Management EMM: MDM, MAM, and MCM Requirements document include the following:

A. Qualified Secure, Scalable Solutions – Technical solutions that address the existing mobile device, application, and content management needs of government mobile technology including minimum level security and policy management. The solutions shall have the ability to scale to the extremely large and evolving nature of federal government cabinet-level Agency organizations.

B. Evolutionary and Flexible – The management needs of the Federal Government Mobility are evolving with increased mobile adoption, new mobile applications, enhanced needs for remote access, and emerging policy and security requirements in an increasingly threatening external environment. As a result, the solutions will continue to assess future requirements to ensure the ongoing Federal Government needs of MDM, MAM, and MCM are adequately met. The MSCT intends to re-assess both the Enterprise Mobility Management requirements and solution providers on a periodic basis in response to mobility evolution. This will provide government agencies with on-going, updated qualified solution providers.

C. Shared Mobility Community – The solution providers are expected to monitor and bring forth new industry developments, identify Managed Mobility best practices in both industry and government, and to present these best practices to government. The Managed Mobility space is in a state of rapid change, making it challenging and resource-intensive for agencies to stay properly informed and to adequately maintain and manage mobility within their respective agencies.

The Vendor shall:

- Ensure any cloud components are FedRAMP certified or have received an Authorization to Operate (ATO) from the Office of Information Security (OIS) prior to operations
- Ensure all components of the MDM solution comply with the security requirements within the Agency / Vendor Agreement
- Provide an MDM solution capable of:
    - Supporting a broad range of device volume
    - Supporting all smartphones and tablets proposed by the Vendor
    - Supporting iOS and Android operating systems
    - Supporting approved mobile application platforms
    - Utilizing open authentication standards (SAML2, OAUTH2)
    - Providing APIs for MDM manipulation for full lifecycle support (e.g., Registration, wiping, reset PIN, Notifications)
    - Allowing application wrapping for added security and management capabilities
    - Integrating security capabilities directly into code via a SDK
    - Supporting custom containerized applications
    - Supporting containerized native applications, hybrid application, and web applications
    - Requiring authentication to access containerized applications and encrypted data
    - Performing jailbreak/ root detection check on applications in network connected and disconnected states
    - Enforcing password/ authentication policies
    - Enforcing compliance policies for device and application configuration/version

    - Creating dynamic policies that are changeable from the central console
    - Performing automated actions based on compliance status
    - Sending notifications when a sanitization/lock has been performed and completed
    - Restricting personal applications from accessing containerized data
    - Locking and sanitizing an application container
    - Leveraging the SDK to implement a selective sanitization of the container (or sub-component) if the device is not used in a specific amount of time (time bomb)
    - Restricting/permitting copy/paste between the container and non-container areas of the device operating system
    - Allowing offline access to the container and applications within
    - Providing zero-day support of iOS and Android OS update releases
    - Deploying applications
    - Sending installation packages via SMS text and/or e-mail
    - Supporting automatic delivery of applications
    - Providing role-based access to relevant applications
    - Providing for single sign-on to access containerized application
    - Displaying a customized end user agreement/splash screen
    - Providing device location management (ability to track the GPS coordinates of devices)
    - Tracking and reporting on data usage regardless of carrier provider
- Operate and maintain the MDM solution (includes pushing updates when directed and or approved by the Agency)
- Provide any Agency help desk personnel with access to the MDM solution to allow for Tier 1 mobile device support if applicable
- Develop and maintain a ***Mobile Device Management Plan***, as identified in Table 1.7.1 Vendor Management and Reporting Requirements, which details how the Vendor will collaborate with the Agency to obtain images, profiles, and settings, operate the MDM solution, provide help desk support to Agency personnel, and update mobile devices and applications

6.5 Task 5: Planning and Management

The Vendor shall manage all activities that align to the project management standards as defined by the latest publication of the Project Management Institute's (PMI), *The Guide to the Project Management Body of Knowledge (PMBOK®)*, unless directed otherwise by the Agency.

Adhering to widely known project management best practices will enable effective, integrated planning and control mechanisms and tools. This will result in reduced risk of schedule and cost overruns, reduced likelihood and impact of negative risks and issues related to deployment, use and management; and increased ability to communicate and share implementation information between the Agency, the Vendor, and other contractors and stakeholders as appropriate. Additionally, the Vendor shall conduct ongoing risk management to ensure that all risks are identified and mitigated, and quality management to ensure that all delivered work meets the predetermined quality standards.

6.5.1 Project Management

The Vendor shall:

- Develop and document the ***Project Management Plan***, as identified in Table 1.7.1
- Provide a ***Monthly Status Report***, as identified in Table 1.7.1
- Provide a ***Monthly Status Report*** prior to or concurrently with the invoice for that month
- Provide a ***Monthly Status Report*** that will cover all tasks and align to the Agency's ***Monthly Status Report*** and any required submission thereof
- Develop and document a ***Subcontractor Management Plan***, as identified in Table 1.7.1
- Define and document a comprehensive ***Project Schedule***, as identified in Table 1.7.1
- Assess current environment to develop a baseline and identify known risks and develop mitigation strategies
- Develop and document a ***Risk Management Plan***, as identified in Table 1.7.1
- Develop and document a ***Quality Management Plan***, as identified in Table 1.7.1
- Define a schedule and criteria for conducting QC checks

6.5.2 Program Management Reviews

- Schedule and present Program Management Reviews (PMRs) on a monthly basis unless a change in frequency is mutually agreed upon with the Agency
- Conduct first PMR within sixty (60) days of the deployment
- Address technical, business, and programmatic topics with a focus on status, performance, and issues/risks
- Provide a proposed agenda to the Agency at least five (5) business days prior to the PMR so that agenda items may be amended if needed
- Provide any relevant PMR handouts to the Agency at least two (2) days prior to the PMR (revisions may be made to address any new information)
- Ensure that the necessary Vendor technical and management personnel attend the PMRs and that presentation materials and supporting data are prepared to ensure that agenda items are fully covered
- Provide a list of action items and issues from the PMR within three (3) business days

6.6 Task 6: Ongoing Support

A comprehensive logistics process is needed to prepare, distribute, collect, and replace the mobile devices required for an Agency moving from a traditional Wireless Carrier Services model to Device-as-a-Service. Multiple collection and distribution processes may be required based upon the need for technology refreshes. Most Agencies will require mobile devices to be rapidly provisioned and distributed to all personnel currently using Wireless Carrier Services. The Vendor will be required to stage, provision, kit, package, and ship all devices as required by the Agency. The Vendor shall notify the Agency of any logistics issues and provide a user-friendly ***Project Dashboard*** that provides a near real-time view of device logistics, asset management, Wireless Carrier usage (as applicable), and any potential issues.

6.6.1 Risk Management

Agencies require ongoing risk management support to ensure that all identified risks can be successfully mitigated and do not significantly impact mission critical operations. The Vendor shall implement and maintain a ***Risk Management Plan*** that will govern the processes used to conduct a baseline risk assessment and continuously monitor the environment to identify new risks as they emerge and formulate appropriate mitigation strategies. The Vendor shall perform risk management activities including, but not limited to:

- Monitor environment to identify new risks as they emerge and track previously identified risks and their impact and residual risk
- Formulate contingency plans and mitigation strategies for all identified risks
- Maintain and update a Risk Tracker as part of the ***Risk Management Plan*** to ensure that all risks are tracked and mitigated
- Submit Risk Tracker to the Agency five (5) business days prior to each PMR
- Conduct ongoing risk management in accordance with the ***Risk Management Plan***
- Support Agency risk management processes

6.6.2 Quality Management

Agencies require ongoing quality management support to ensure that all devices delivered meet expected quality standards as required to meet Agency objectives. The Vendor shall implement and maintain a ***Quality Management Plan*** that shall describe the overall quality policies, program, organization and responsibilities, procedures, and the means of ensuring that all work products will be in conformance with performance requirements. The plan shall address appropriate planning and control of work operations through reviewing, inspecting, testing, and surveillance/audit and lessons learned, both during the contract period and at contract closeout.

6.6.3 Technology Refresh

The Vendor shall develop a ***Technology Refresh Plan***, as identified in Table 1.7.1, which can accommodate technological advances that occur during the contract period. The plan shall address any software or hardware upgrades that become necessary (maintaining the same operating system) and specify the process that will be used to upgrade, collect and redistribute mobile devices to all end-users if applicable. Reviews shall take place on a six month technology refresh cycle to determine what, if any, technology refresh is required based upon changing technology capabilities, industry and supply chain dynamics, discontinued products, and economic adjustments. The technology refresh may propose alternatives to traditional technology. Agencies should anticipates that the cost per kit used during the contract period shall not exceed the cost of the original fixed-price of the kit as established in the original agreement unless otherwise stated. However, if there are circumstances that may require price adjustments, which will be in the best interest of an Agency, alternatives may be proposed by the Vendor.

Additionally, an Agency should reserves the right to initiate a technology refresh at any time based on technology innovation that causes changes to the device requirements, such as the need for devices of a different make and model. All proposed technology refreshes shall be submitted to the Agency by the Vendor and approved for compatibility with mission critical operations and Agency objectives prior to initiation. At no time shall the Vendor substitute or modify any service offering due to a technology refresh without written authorization from the CO through the issuance of a modification to the contract.

6.6.4 Shipping Analysis and Support

Agencies require the selection of a shipping method that can deliver all devices to their staff and contractors as needed. Delivery requirements may be a combination of the following: delivery time windows (normal business hours and after-hours), delivery locations (rural, urban, commercial, and residential), use of multiple shipping sizes, non-pallet packaging, bulk shipments and single device shipments, and delivery to homes/ offices (requiring inside signed delivery to an authorized Agency recipient).

6.6.5 Logistics Planning and Support

Agencies require logistics planning and support to ensure that all logistics activities can be effectively executed in the timeframe required by the Device-as-a-Service contract to support Agency activities. The Vendor shall develop and document an end-to-end ***Logistics Support Plan*** that includes staging, provisioning, kitting, quality control, packaging, and shipping. The Vendor will need to carefully plan the time required for staging and provisioning to minimize the changes (OEM updates, Agency designated software updates, and/or security updates) that may occur and require additional patching during this process. The Vendor shall notify the Agency of any logistics issues and periodically conduct process improvements to prevent recurrence of any identified issues.

The Vendor shall:

- Define and document a ***Logistics Support Plan***, as identified in Table 1.7.1, that includes:
    - Staging all mobile devices by installing the required operating systems and software
    - Provisioning all mobile devices for end-users by configuring with all required Agency applications
    - Kitting all mobile devices with the required accessories and Agency end-user documentation
    - Conducting QC checks for staging, provisioning, and kitting the mobile devices (100% of kits will be checked to ensure all accessories match the Agency specifications)
    - Packaging assembled kits for shipping according to individual shipment or bulk shipment
    - Shipping packaged kits to their designated destination using the shipping method determined by the ***Shipping Analysis Report***

- Replacing devices upon request by Agency personnel within predetermined timeframes
- Returning devices according to both individual and bulk collection through a pre-paid process
- Performing a complete device sanitization and factory reset (in accordance with NIST 800-88 Rev 1) on every returned device prior to reconfiguration and redistribution or upon final contract closeout
- Decommissioning all mobile devices to ensure that devices are collected in a timely and effective manner following the completion of all Agency operations

6.6.6 Secure Messaging

Agencies may require the option to have a secure messaging capability if one is deemed necessary for Agency use cases. The secure messaging capability may be either standalone or incorporated into the MDM solution.

6.6.7 Help Desk Support

Many Agencies require access to on-demand help desk support for all DaaS devices used by Agency personnel. The Agency may desire to provide Tier 1 help desk support to intake and triage all help desk requests. The Vendor shall provide all help desk escalation support and shall grant necessary access for the Agency to provide Tier 1 help desk support. Additionally, processes and connectivity will need to be developed to seamlessly escalate from Tier 1 support provided by the Agency to higher Tier support provide by the Vendor.

The Vendor shall provide all help desk escalation support activities including, but not limited to:

- Provide escalated mobile device support to Agency personnel
- Provide the Agency with all necessary access to provide Tier 1 support to Agency personnel
- Develop and document all help desk processes (e.g., customer service, transfer between Tiers)
- Negotiate SLA Requirements for help desk escalation support with the Agency
- Establish and maintain SLAs for help desk escalation support (e.g., hours of operation, wait time, response method)

6.6.8 Project Dashboard

The Vendor shall provide a ***Project Dashboard*** capable of providing a role-based view of device logistics, asset management, Wireless Carrier usage, and potential issues, which can generate various reports upon demand. The Agency will need to work with internal personnel and the Vendor to define specific Dashboard requirements. Overall the dashboard will require a user-friendly view and interface that provides the Agency with on-demand access to near real-time mobile device data. The dashboard will provide the Agency access to operational data such as

Wireless Carrier service usage and device tracking. Additionally, it will provide the Agency with notifications of any potential issues to ensure proper resolution and minimize the effects on the Agency operations. The dashboard will be customizable to allow for role-based views, which will display data according to the relevant defined personnel position or geographies (e.g., DaaS Project Manager or field supervisor).

The Vendor shall provide all dashboard development and maintenance activities including, but not limited to:

- Collaborate the Agency to elicit all requirements for the ***Project Dashboard*** and design any required interfaces with Agency systems and an online ordering system
- Provide a ***Project Dashboard*** that demonstrates operational readiness metrics and provides reporting activities including defining, tracking, and reporting Project-level performance and Agency metrics
- Update and maintain the ***Project Dashboard***, as identified in Table 1.7.1
- Provide Vendor contact information, schedules, and all contract deliverables
- Provide access to online ordering system for DaaS kits and partial kit components that includes a catalogue with available kit configurations
- Integrate with Vendor asset management systems to provide the location and status of the acquisition and logistics activities to include provisioning, kitting, inventory, and shipment of devices and the volumes in each phase of the process so the Agency can monitor and ensure configured devices will match up with employee hiring, training, and production efforts
- Provide a cellular service map that illustrates the specific coverage areas of each cellular network carrier
- Include real-time alert functionality that will notify the Agency of any network problems that may impact the Agency and provide additional notification of issue resolution
- Provide overall status/progress updates
- Provide the Agency with access to the ***Device Sanitization Log***, as identified in Table 1.7.1, to approve the entries
- Provide access to all past signed entries within the ***Device Sanitization Log***
- Provide access to the ***Bill of Lading*** for each shipment of devices
- Provide access to the Risk Tracker
- Provide access to the Tier 1 help desk support provided by the Agency
- Acquire an ATO from OIS for all components of the dashboard

7 Pricing

When requesting or evaluating pricing of the DaaS solution providers, pricing should be presented on a per device basis – it can be presented in the context of price ranges, pricing tiers based upon volume, pricing based upon pre-defined product configurations or some other scenario or set of scenarios.

One of the key benefits of DaaS is the ability for Agencies to receive pricing transparency for the specific Tasks and or components of Wireless Carrier Services and other mobility components.

To keep with the purpose of this document and to scale across government, it is recommended that pricing submissions be kept to simple structures so that a cost per device can be easily determined and understood in the context of total services delivered.

Pricing may either be customized or may be submitted based upon availability through publicly accessed source. Pricing should be submitted as an integral part of the DaaS solution.

Agencies should request that DaaS solution providers indicate the range at which their product is sold to their federal customers, inclusive of the discounted rate that is offered to their best federal customer. It is recognized that not every federal customer purchases solutions identically, and often pricing is dependent upon specific agency needs and requirements. The intent is to indicate the range of potential pricing, subject to the particular requirements that go beyond the specifications. Additionally, agencies should request a pricing table, which reflects the price structure and currently listed prices for the solutions on Federal contracts/task orders.

For those solution providers offering their solution under IT Schedule 70 the solutions must be on the vehicle and the pricing must correspond to what is found on the schedule. If the solution is offered via a solution's IT Schedule 70 contracts, the solution must currently reside on that contract vehicle to be considered. For pricing related to other government-wide acquisition vehicles the rules would be consistent with those of that particular vehicle necessary to reach the DaaS solution set.

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Virtual Mobile Infrastructure (VMI)

Working Group Document

Virtual Mobile Infrastructure

What is Virtual Mobile Infrastructure?

Virtual mobile infrastructure (VMI) is an emerging mobile technology. VMI is an application delivery model in which a "virtual" mobile device runs the OS, authentication, applications, mobile security, and data access from a tactical server, data center or cloud instead of being stored on the device. The mobile applications can be streamed to any mobile device including IoS, Android and Windows smartphones or tablets. VMI can also remotely access physical mobile device sensors such as the camera, microphone, GPS and Bluetooth connected devices or other data collection devices. The user can move from one device to another seamlessly without loss of data or functionality since all data is stored centrally and not on the physical device.

VMI minimizes the need for MDM/MAM at the device level. There is little need to harden devices since no data is stored locally and security is centrally managed. If a device is lost or stolen, it can be deactivated with no data loss and little risk to the organization. Management of mobile devices, applications, and security is significantly simplified. VMI can run on 3G or later networks and can function on download speeds of 250Kb or higher (depending on solution deployed).

However, VMI is not without risks or concerns. Since it is a virtual operating system, most existing VMI solutions are dependent upon being connected to the network through either a cellular or Wi-Fi connection. While connectivity is currently a limitation in the VMI solution, it is important to note that some non VMI vendors have made progress to alleviate the connectivity limitations by providing OS or hardware virtualization solutions, thereby allowing the user to continue working in low or no-connectivity situations.

Virtualization Types

- Device Virtualization - This deployment type virtualizes the entire device and is a pure definition of Virtual Mobile Infrastructure (like desktop VDI) in that it requires constant connectivity to the VMI Servers. There is no data at rest on the device and most of the content in this document references this deployment type.
- OS Virtualization - This deployment type creates a profile for each user within the OS and limits them to the permission set described by this profile. This deployment type can work in a disconnected state and has data at rest on the device. The user profiles are encrypted when not in use.
- Hardware Virtualization - This deployment type utilizes a Type 1 Hypervisor to directly control the device hardware creating virtual (or guest) machines. This deployment type can work in a disconnected state and has data at rest on the device. Virtual machines are encrypted when not in use.

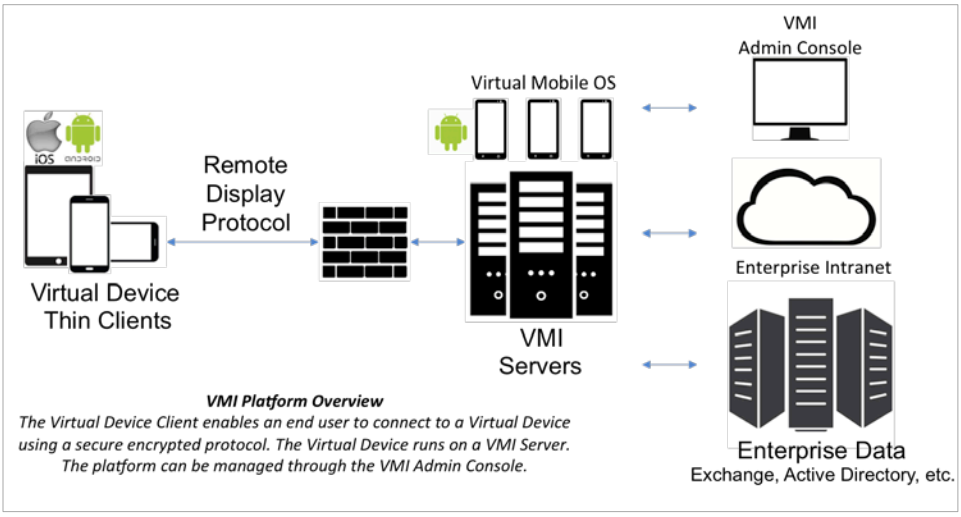
VMI Benefits and Risks

Features and Benefits	Risks and Concerns
• Central control of authentication, access, applications, and capabilities – including GPS, Bluetooth and other device sensors • Data encryption and centrally managed security • IT management simplified with single platform • App development – one version across all devices • Organizational data accessible remotely enabling mobile business processes • Enables access and control via BYOD devices eliminating privacy concerns with agency data on personal device • Both iOS and Android devices are supported as endpoints in this technology • Potential to have lower cost devices	• VMI devices may not be accessible offline and is dependent upon connectivity (may be mitigated through additional solutions working in conjunction with VMI to allow operational capability with low or no connectivity) • VMI is a relatively new technology and therefore, not completely proven • There are a limited number of vendors offering VMI

How VMI Works

The VMI platform enables mobile operating systems, applications, and security to run on the mobile device through a secure, encrypted connection to remote VMI servers, which are connected to the VMI Console, the Enterprise Intranet and Enterprise Data sources. The VMI Console is the central control point for mobility management enabling user authentication, access control, application approval, and mobile security for all the connected devices. Only a thin client app is required to be on the device, which allows device access to the VMI platform. The thin client app can run on either Android and iOS mobile devices. The VMI servers maintain connectivity to Enterprise data or Enterprise Intranet allowing access and use by the end-user without having any data stored or saved on the device itself, thereby maintaining data security and controlling potential data loss.

VMI Architecture



Ideal Usage Scenario for Agencies Considering VMI

Factors within end-user environments and related mobility requirements that support VMI as a viable platform for mobility services include the following:

- **Coverage**: Contiguous cellular or Wi-Fi coverage in all areas of the end-user environment
    - Large city, urban environment locations
    - Covered highways and secondary locations
    - Generally, not adequate for very rural or geographically remote areas
- **Security**: Mobile Security is a primary requirement and data loss is a primary risk for end users and the organization
    - Current users regularly have sensitive or restricted data on their phones
    - Encrypted communication (FIPS 140-2) and data transfer is a requirement
    - In case of lost or stolen devices, it is necessary to have quick device disablement
- **Device Mix**: End-user community has a mix of Android and iOS
    - Support is necessary for both Android and iOS
    - Mobile app development required to support Agency mission and activities
- **Personal and Business Use**: Need to isolate and separate Agency use from personal use on devices
    - Users need to have both government and personal use of a device
    - BYOD is a viable option for providing mobility services

VMI Inherent Capabilities and Support Considerations

Secure Communications:

- VMI can provide mobile device security comparable to that found on desktops and laptops. Mobile security and the potential for a security breach is a primary concern for organizations and one of the reasons that more organizations do not implement remote access to enterprise data. VMI provides a virtual OS and devices do not store any data on a device, this risk is strongly mitigated.
- There are no enterprise apps at-rest on the mobile device, which results in the highly secure delivery of enterprise apps and data.
- If a device is lost or stolen, the organization's data is not at risk or compromised because the device is centrally controlled and no data or apps are stored on the device.
- Traveling to high-risk locations can also potentially put communications at risk. With VMI, all apps and data remain in the enterprise data center and therefore remain secure.

Mobile security is an inherent capability in Virtual Mobile Infrastructure due to virtualization, encryption, and no data at rest on the device. However, there are providers who can add significant security capabilities to mobile devices even within virtualization. Their technologies are in the form of firmware that allow for multiple personas; protection of the device, data, and applications; and they work complimentary to MDMs, VPNs, and

containerization. While transitioning from one mode to another, all data is cleared. Added protection can be integrated by adding run-time integrity checks to privilege escalation preventions. The additional protection and security is achieved through isolation of the device at multiple layers within the OSI model. The security policies, which control access to networks, applications, data sources, and other backend services, can be customized to a specific user or operational environments. One downside from a total solution perspective is that these solutions, due to their nature as firmware, are currently only supported through Android and are not supported in iOS.

Mobile Applications:

- Enterprises can reduce cost and complexity of developing multiple versions of mobile apps to accommodate iOS and Android as well as other operating systems. With VMI only one version of the app is developed and placed on the VMI platform. Then, it is accessible and usable by multiple operating systems when accessed through the thin client to the VMI platform. This significantly reduces time for development and associated costs. Enterprises often cannot meet end-user demands for specific apps; they struggle to make most commercial mobile apps available because these apps cannot easily be wrapped, containerized, or otherwise secured. Using VMI all enterprise apps and data remain in the secure data center for both easy management and maintenance. Even legacy applications that are written in earlier versions of Android or different OS's are supported. Due to this capability, enterprises can reduce app development and update costs.
- Third-party cloud services and mobile apps such as Office365 and Salesforce often have difficulty managing employee access. It is much more easily managed at the VMI central location resulting in cost and management benefits.

BYOD (Bring Your Own Device):

- Enabling BYOD in businesses and government has been a difficult user model to establish in most organizations due to business or government policies as well as employee concerns over privacy. Employees do not want enterprise security software loaded on their personal devices because they are concerned that their employer may access or delete personal data or track the location of the employee's mobile device. However, enterprises are seeking ways to reduce mobility costs to their organizations so they would like to implement BYOD as a cost cutting measure.
- VMI may provide solutions to both facets of this issue. VMI solutions can be deployed on any device with no MDM agent, thereby minimizing end-user privacy issues for BYOD. Since mobile devices are virtual, there are no data or apps at-rest on the physical device, making the solution very secure. VMI allows the enterprise to only monitor work data that is located on the virtual device, which meets regulatory and compliance requirements in the mobile use case.
- Since the virtual mobile device runs in the enterprise data center, IT and compliance teams can maintain oversight into mobile access and usage to fulfill compliance and audit requirements.
- Enterprises often only allow specific devices to be eligible for BYOD use; they spend resources on higher-end, corporate-provided devices to ensure that devices have necessary security features and to minimize the complexity induced by device model

fragmentation. VMI can help eliminate the requirement for higher end devices and achieve lower costs.

Contract Workers:

- VMI helps enable enterprises to provide security, application access, authentication, and device management to contract workers who otherwise may be limited from having necessary access or may create a higher risk to the organization due to use of less secure devices. The VMI thin client can be deployed on any device. Additionally, apps and data delivery are secure because there are no enterprise data or apps at-rest on the physical device.

End-User Mobility Management:

- Enterprises have no accurate means to determine data usage on work-related activity versus personal use. As a result, they implement insufficient and often higher costs policies such as fixed stipends or arbitrary cost splits. VMI enables accurate data metering for both Wi-Fi and cellular connections, so enterprises can reimburse specifically for work-related activity. Workers tend to reject the use of secure productivity apps due to the difficult steps in accessing them. VMI enables organizations to provide commercial productivity apps in a secure manner since the application resides on the central VMI servers delivering a native use experience for the end-user.

Provisioning Capabilities:

- Rapid provisioning is an on-going problem and high cost to large organizations. Whether provisioning new employees, upgrading devices, or installing new software; enterprises often expend critical resources and negatively impact productivity through provisioning and related disruption. VMI simplifies user provisioning since the enterprise controls the profile of virtual mobile devices in the data center and can provision end users quickly.
- Provisioning different groups of users with different profiles can also be a management challenge when individual devices must be loaded with specific software and applications. Since all apps and data reside within the VMI platform, making customer usage profiles for each end-user is much simpler both initially and when changes are required.
- VMI also allows a single device to have multiple user profiles; thereby enabling device sharing for workers who may have sporadic needs for mobile access. This can reduce cost by reducing the number of devices an enterprise must purchase.

Government Compliance:

- VMI enables compliance much more easily. Since data does not leave the data center, geographic policies can be adhered to without unnecessary burdens upon the workforce. When workers must keep to a strict set of hours, VMI can enable access during those set ranges supporting compliance requirements.

Helpdesk Cost

- Helpdesk costs can be significantly reduced using VMI because there is only centralized OS, applications, and data access. Only the hardware must have individual support.

IOT / Sensor Networks:

- As with end-user mobile devices, IOT Sensor Network devices do not have resident OS or data on the devices. Therefore, enabling IOT is a much simpler process and lower cost initiative.

Potential Sources of Supply

Sources of Supply	Acquisition Paths
Hypori • Austin, TX; • www.hypori.com	• DHS SBIR-2016.OATS-16.OATS-001-0001-II • GSA SCHEDULE 70 (Carahsoft) • NASA SEWP
Graphite Software* • Ottawa, Canada; • www.graphitesoftware.com	• GSA SCHEDULE 70 o Via Triad Technology Partners
COG Systems* • Newtown NSW, Australia; US 1-855-662-7234 • cog.systems	• Direct Purchase: Agreement with Immix Group
Redwall Technologies LLC • Beavercreek, OH; • www.redwall.us	• Direct Purchase. Not on GSA/GWAC vehicles. • Purchase via ODM/partners is available.

* Graphite Software, Cog Systems, and Redwall are not VMI providers by definition, however, they provide OS and Hardware Virtualization solutions that can be used in conjunction with Virtual Mobile Infrastructure.

Mobile Services Category Team (MSCT)
Advanced Technology Academic Research Center (ATARC)

Mobile Identity Managment

Working Group Document

Executive Summary

The processing power and memory of some of today's devices is greater than desktops. The device that we still call a mobile phone or smartphone….is more computer than phone….in fact, is more powerful than computers used for the Apollo 11 Moon Landing!

Mobility is impacting most every aspect of our lives. It is a change-agent that drives new possibilities for businesses, government and people/citizens, allowing more business to be conducted virtually any time, anywhere, in ways that were not previously possible.

In an ever-changing digital world, the need for trusted identification tools and services is more pressing than ever before. As digital technology evolves, the concept of identity becomes more complex and multi-faceted. A person can have one personal identity based on their actual physical entity, and yet have multiple digital or virtual identities based on the various relationships they are involved in on the Internet, at work and the online universe.

Digital identity is often defined as the set of electronic credentials or attributes required in-order to gain access to a service or resource in the real or virtual world.

Mobile identity is the secure integration of the attributes which unerringly identify a person in the physical and the online worlds, within the mobile device. Mobile identity is at the core of a digital society and the entire emerging identity management ecosystem has a significant role to play in building trust in the digital economy.

In the first of a series of documents/playbooks we provide a view into the mobile identity ecosystem, the key players and a deeper dive into derived credentials (a critical near-term requirement for government agencies). This has been a collaborative development process drawing on experiences and expertise of industry, government agencies, and standards groups.

Initial Learnings & Highlights:

- At an operational level, there are **currently no vendors that provide an end-to-end solution** for secure mobile identity from device through…person…credentials and…transactions.
- **Interoperability is key.** Look for open standards, established and tested alliances between critical components such as MDM/EMM and Credential Management Systems and standard API's to interconnect systems.
- **Leverage learnings and best practices** in-order for government to accelerate the move to mobility. Agencies should work together, building on the lessons learned in enterprise and early federal pilots. We have discovered some great pockets of knowledge and success in the Federal space.
- There is useable COTS. Avoid creating GOTS/agency specific solutions.
- The landscape is changing quickly through Executive Order and the anticipated NIST Publication 800-63-3. However, **there is no need to wait before getting started**.
- Enabling a secure mobile workforce and citizenry is already an ask.

- Security is critical but is not an obstacle.

Although the government makes up a relatively small percentage of mobile devices, there is an opportunity for government to partner with business leaders to get support from device manufacturers and carriers for stronger security features out of the box. (i.e. the EU Payment Services Directive)

Threats to the Government's use of mobile devices are real and exist across all elements of the mobile ecosystem. The enhanced capabilities that mobile devices provide, the ubiquity and diversity of mobile applications, and the typical use of the devices outside the agency's traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstations. These are the conclusions of the DHS study submitted to Congress, April 2017.

https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

In a parallel effort to the release of this paper, we are seeking a better understanding of agency progress with Derived PIV Credentials (DPC) so that we may better connect those who have made progress with those just getting started. We would like to ask you or your delegates to participate in our data collection efforts by participating in a survey on your DPC/Mobile Identity & Access Management efforts. To make the best use of your time we are happy to have the survey submitted by email or we can arrange a short call to collect the information over the phone. Details of the survey are available at:

https://www.atarc.org/working-groups/mobile/id-management-survey

Thank you for taking the time to read this paper. We hope it will provide value for the adoption of Derived PIV Credentials in your agency.

Glossary of Terms

ATARC – Advanced Technology Academic Research Center is a 501(c)(3) non-profit organization that provides a collaborative forum for Federal government, academia and industry to resolve emerging technology challenges. See https://www.atarc.org

Authorization Server – OAuth component that provides support for a user to grant authorization to an application (typically mobile) to access user content.

BYOD – Bring Your Own Device model of supporting personally owned mobile computing devices connecting to enterprise networks.

CAC – Common Access Card - Roughly the equivalent of a PIV card. See http://www.cac.mil/common-access-card/

COPE – Corporate Owned Personally Enabled model of supporting personal use of mobile devices that are owned by a corporate entity, in this case the U.S. Government.

CRL – Certificate Revocation List – A list of certificates that have been revoked that can be accessed over the internet by a relying party to confirm validity of a presented certificate.

Cryptographic Hardware – Devices that contain a protected cryptographic key that typically must be unlocked before use. Commonly a smart card.

Cryptographic Software – Cryptographic keys stored on disk or other storage media that typically must be unlocked (often by a password or PIN) using a cryptographic protocol of some kind.

DoD 8520.03 – Department of Defense Instruction on Identity Authentication for Information Systems

DPC – Derived PIV or Derived CAC Credential. A PKI credential that is issued for use on mobile and other devices that are not well suited for the use of a CAC or PIV. This credential is referred to as a "Derived PIV Credential" (DPC) yet there is no mathematical derivation or relationship between the PIV and the DPC. The relationship is purely administrative requiring a system to relate the existing DPC to the PIV that was provided as proof that a user was entitled to it.

EMM – Enterprise Mobility Management – Software platform that is generally broader than a Mobile Device Management (MDM) platform in that it typically combines MDM, Mobile Application Management (MAM), and perhaps other capabilities. While MDM is typically focused on device management, an EMM considers the systems and data accessed by mobile users as well.

FICAM – Federal Identity, Credentialing, and Access Management program. The FICAM program supports Federal agencies through the entire identity management lifecycle.

FIPS 201 – Federal Information Processing Standard Publication 201, Personal Identity Verification of Federal Employees and Contractor

FPKIPA – Federal Public Key Infrastructure Policy Authority – Members are appointed by each agency CIO and the group serves to set policy regarding FPKI Trust Infrastructure, approving cross certification with the Federal Bridge, and providing oversight to the Certified PKI Shared Service Provider Program.

GFE – Government Furnished Equipment – Computing equipment owned and issued by the government.

Identity Proofing – The process of verifying that an individual is who he or she claims to be. In the case of mobile identity this is done prior to issuing a digital credential for mobile and is based on possession of a PIV or CAC which has its own identity proofing process under FIPS 201.

Identity Provider – A system which can provide identifiers for users who it knows about and have authenticated to the system. (e.g. an identity provider can authenticate a user with a DPC and provide a SAML or other assertion of identity).

Keychain – A password management system developed by Apple. It provides a mechanism to store highly sensitive data including passwords and cryptographic keys.

Keystore – A repository of highly sensitive data including passwords and cryptographic keys (similar to a keychain but on platforms other than Apple).

Level of Assurance (LOA) – The degree of confidence in the claimed identity (or in some cases, attributes) of a subject (i.e., a user or computer system) authenticating to a system or application. Different factors that can establish assurance include the strength of an authentication credential, the security of an authentication protocol, and identity proofing that occurs prior to issuance of a credential.

OAuth – Standard framework for token-based authorization. Supports the delegation of user rights to a service or application to operate on behalf of a user. Commonly used to provide mobile applications the ability to communicate with mobile API to perform actions. For example, to allow a mobile Facebook app to connect to the Facebook service to read posts and post new updates on the user behalf. See https://oauth.net/2/

OpenID Connect – An identity layer operating on top of OAuth 2.0 to support end-user identity verification performed by an authorization server. See http://openid.net/connect/

PIV – Personal Identity Verification, see FIPS 201.

Relying Party – A server providing access to secured data that relies on a digital identity issued by another system. It does not maintain its own database for user authentication.

MDM – Mobile Device Management – A system designed to manage mobile devices and apply policy controls to them.

SAML – Security Access Markup Language - An XML-based framework for communicating user authentication, entitlement, and attribute information. See https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SP 800-63 – Special Publication 800-63 - NIS published guidance on guidelines for the issuance, storage, and use of digital identities.

SP 800-157 – Special Publication 800-157 – NIST published guidance on the process by which a new PKI credential is issued based on proof of possession of a current valid PIV. This credential is referred to as a "Derived PIV Credential" (DPC) yet there is no mathematical derivation or relationship between the PIV and the DPC. The relationship is purely administrative requiring a system to relate the existing DPC to the PIV that was provided as proof that a user was entitled to it.

TEE – Trusted Execution Environment. A separate operating system running in parallel on the same chipset as the primary (normally Android) operating system. Provides separation of sensitive security functions enforced by the system CPU.

Introduction

Derived PIV Credentials (DPC) – A cryptographic token issued in accordance with FPKI policies in accordance with LOA 3, LOA 4, Credential Strength C, or Credential Strength D identity proofing requirements. Outlined in NIST SP 800-157

Derived credentials have been a technical option on mobile devices for over a decade, yet the deployment and ultimately, usage of Derived PIV Credentials (DPC)[1] is a relatively recent innovation for agencies. The NIST framework outlining the use of DPC, Special Publication 800-157, was released in December 2014. It defines the administrative process required to ensure a user can prove possession of a valid Personal Identity Verification (PIV) card prior to the issuance of a new PKI credential for use on mobile devices or other platforms that don't easily support a PIV and associated reader. However, thus far many agencies have not engaged closely with NIST and the Federal Identity, Credentialing, and Access Management program to align internal policies and move forward with DPC. As a result, the U.S. Government either continues to rely on username and password or has forgone access to business and mission applications from mobile devices lacking built-in or attached smart-card readers.

The findings of this Government/Industry working group suggest that while the creation and issuance of DPC is relatively well understood, issues associated with credential storage and management, as well as PK enablement of service providers (aka relying parties, web servers, mobile API's), remains a significant hurdle to mobile enablement and use.

The continued use of memorized secret token (e.g. a password), presents a significant risk across the board as demonstrated by multiple recent hacks that started with a single compromised password. A single compromised password is bad enough but with password reuse across sites, one cracked password may lead to serious compromise of multiple systems. Consider the following from a 2012 article in Wired. "How do our online passwords fall? In every imaginable way: They're guessed, lifted from a password dump, cracked by brute force, stolen with a key logger, or reset completely by conning a company's customer support department."[2] So the elimination of passwords or passphrases is of urgent need and has been for years. However, added complexity for authentication, especially on mobile devices with their limited keyboards, is itself a significant risk. In this case, there is significant risk of avoidance of mobile apps, increased help desk costs, and inefficiency if end users find systems and apps too difficult to use.

---

[1] For the purpose of this paper, DPC refers to credentials issued based on proof of possession of a Personal Identity Verification card (PIV) or a Common Access Card (CAC).

[2] Kill the Password: A String of Characters Won't Protect You, by Mat Honan, Wired, November 15, 2012, last accessed on 5/30/2017 at https://www.wired.com/2012/11/ff-mat-honan-password-hacker/

The ATARC Mobile Identity Management Project Team is therefore providing a several recommendations in hopes of accelerating the replacement of passwords with a strong cryptographic token (Derived CAC/PIV Credential) stored in either a software or hardware cryptographic store to support the increased adoption of mobile devices for business and mission use. Additionally, the team is working to share lessons learned from implementations and pilots across government agencies, to be released separately.

At a high level, the project team is recommending an architecture that builds a trust foundation beginning with a PIV or PIV-I credential which serves as a birther, or existing identity that is highly trusted, for a DPC. The DPC, in turn, is used as the foundation of more transitory, industry standard, authentication and authorization mechanisms. In this way, agencies may have increased flexibility in the security architecture employed while accelerating the adoption of strong authentication.

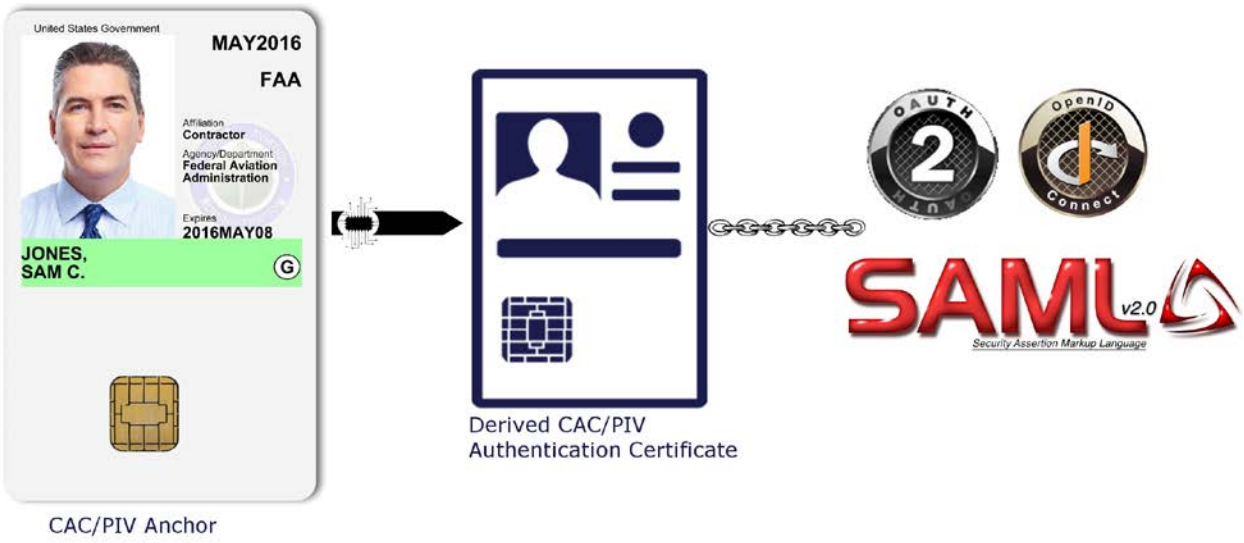


Figure 1: Alternative Authentication/Authorization Protocols Rooted in a DPC

The recommendations of the team logically link broadly accepted authentication and authorization protocols to strong U.S. Government credentials grounded in HSPD-12, FIPS 201, and NIST SP 800-157. The recommendation also seeks consistency with the goals and framework established in FICAM, FPKIPA, NIST SP 800-63 and DoD 8520.03.

Assumptions

In developing the recommendations contained in this document, the ATARC Mobile Identity Management team held multiple collaboration sessions which brought industry and government leaders together to discuss requirements, hurdles, and opportunities for success. The following are a list of assumptions for the reader to consider:

Strong, Multi-Factor Credentials – Federal authentication assurance requirements specify multi-factor credentials for users conducting Government business on mobiles devices. In other words, users must supply something they have and something they know to prove identity to the services and apps they use. This paper focuses on Level of Assurance 3 (LOA 3) and LOA 4 credentials issued based on possession of a CAC or PIV credential and the identity proofing and vetting performed prior to its issuance. It describes different usage models for these credentials including direct presentation to a Relying Party (RP) application and for authentication to an Identity Provider (IdP) or Authorization Server (AS) that then presents an authentication assertion to applications. While lower-assurance credentials are still accepted for some transactions, particularly for non-CAC/PIV users, this paper also discusses stronger credentials for those users.

Device Ownership Models – Government Furnished Equipment (GFE), Bring Your Own Device (BYOD), and Corporate (Government) Owned Personally Enabled (COPE) models were all considered as options across the U.S. Government with individual departments and agencies adopting a more restrictive model as necessary. However, the lack of specific policies allowing the use and management of BYOD or personal space in a COPE model means that, from a practical perspective, most agencies will be deploying to GFE for the foreseeable future.

Mobile Devices – While the primary focus is on iOS and Android devices, the recommendations contained herein may generally be applied to other "mobile" devices like Windows Phone and laptop computing equipment. iOS and Android are a greater challenge in most cases due to the lack of a robust and easily accessed cryptographic service layer. These platforms feature built-in isolation between key storage locations which enhances security but also increases difficulty of use.

Level of Assurance – At the time of this writing NIST had just closed for comment Special Publication 800-63-3 and with it a more refined notion of levels of assurance. We have maintained the notion of LOA 1-4 consistent with Special Publication 800-63-2. However, many of the concepts described are applicable when 800-63-3 is released barring any major changes.

Credential Storage – While some departments and agencies may have a need for LOA 4 credential storage only (i.e. the use of a multi-factor hardware token) it is assumed that a wide variety of use cases exist and LOA 3 will suffice for many use cases.

Credential Usage – While PK enabling consuming applications (aka relying parties) may be a desired end state for some use cases, it is acknowledged that doing so may be impractical in terms of cost for a great many legacy applications. Further, PK enabling relying parties may be impractical given development skills and established authentication patterns that leverage "modern" standards like SAML, OAuth, OpenID Connect, and FIDO.

PIV vs CAC – For this paper we are considering PIV and CAC to be equivalent; a smart card issued through strong identity proofing process which forms the basis for the issuance of a derived CAC/PIV credential (DPC).

PK Enabling – The process of enabling an application for the use and/or consumption of a public key cryptographic token (e.g. a PIV Credential or a Derived PIV Credential). This may include enabling relying party web servers to support certificate authentication, enabling mobile apps to query for user credentials and build-in certificate based client authentication processes, and more.

Derived PIV Credential Usage & Architecture

A DPC ecosystem requires more than simply issuing a certificate to a device. It is a complement of products and solutions that together issue and maintain certificates, may provide integration to mobile device management or enterprise mobility management systems, and support a broader array of authentication and authorization mechanisms to facilitate a variety of use cases. In short, this architecture can provide a trusted digital identity ecosystem.

After issuance, credentials on a mobile device support many functions including:

- Wi-Fi authentication over EAP-TLS
- Virtual Private Networking (VPN)
- User Authentication to COTS, SaaS (e.g. SalesForce, ServiceNow, etc.) and GOTS (timecard, travel, etc.) Applications and Services
- HTTPS/TLS Data in Transit Protection
- Data Encryption (Data at Rest or Individual Records)
- Signing of Individual Documents or Records

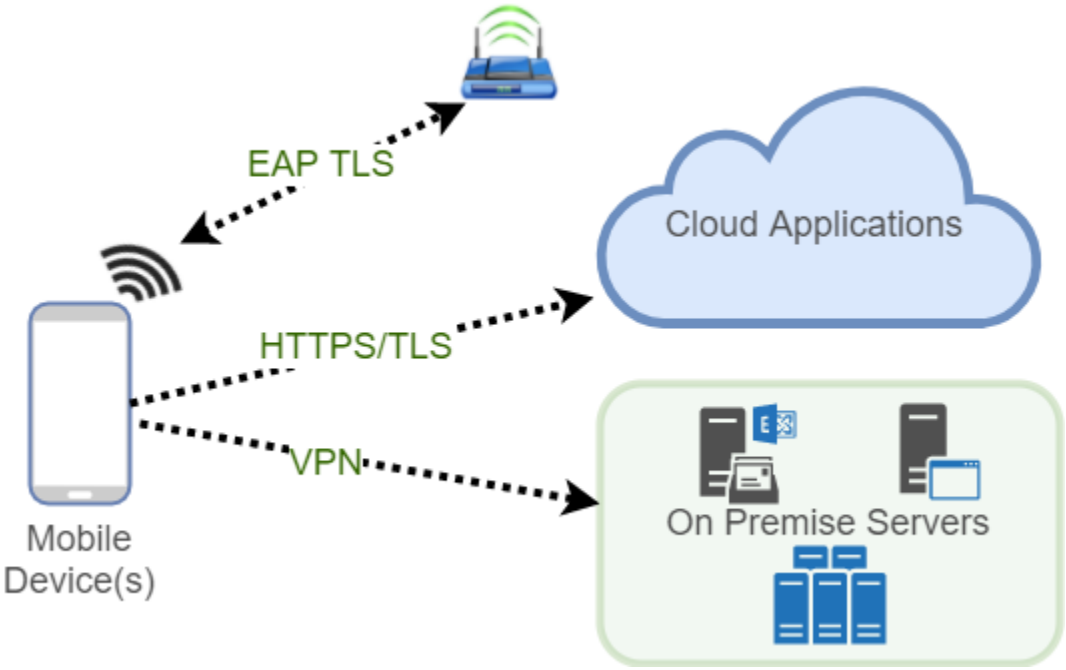


Figure 2: High Level DPC Usage Architecture Example

Derived CAC/PIV Credential Issuance

User certificates for email signing and authentication, as well as encrypting certificates have been issued to mobile users for over a decade. Early credential issuance processes were often very manual, requiring the generation of new key pairs on a separate PC before being copied to a

mobile phone. While effective, this method didn't scale well and had substantial risk of the migration of credentials (i.e. copying the private key to more devices than anticipated/desired).

Today user and device credentials may be delivered to devices in a variety of ways. Some methods provide greater assurance that certificates can't be copied or moved to additional computing devices. Likewise, some provide more capabilities for timely revocation and removal, and ensure certificate renewal and update as required. Modern mechanisms for delivery of DPC's typically center around a user self-service model for creation of an LOA 3 credential. In this case, users either browse to a website configured for CAC/PIV authentication or they use a kiosk that includes PIV card authentication prior to issuance. This step serves to satisfy the requirement that a user demonstrates proof of possession of an authentic and valid credential. The DPC issuance platform must support additional requirements outlined in NIST Special Publication 800-157 as well. Systems must have a mechanism to periodically validate the user's status as an authorized CAC/PIV card holder so that the derived credential can be revoked or modified as required by events like termination of employment or changes to name or department.

There are two major ways to issue a LOA 3 DPC:

- Devices create public-private keypairs before communicating through a registration authority which performs actions necessary for the issuance of certificate(s).
- An intermediary generates the public-private keypairs and communicates with the CA for certificate issuance prior to exporting the private key and certificate in a special format (PFX) for import into the mobile device certificate store.

While a DPC must be issued from a trusted certification authority connected to the Federal Bridge, this system may or may not be the same system used to issue PIV cards. A valid PIV card is required for issuance of a DPC, yet it only matters that the PIV is valid and trusted, not that the underlying PIV issuance platform is still in use.

While encryption certificates and related private keys (a.k.a. archived certificates), for the protection of mail or other data, are recovered to mobile devices (a copy of the private key is securely copied to a mobile device), authentication and signing certificates are different. Although it is allowable for LOA 3 to generate key pairs on another system before injecting them onto a mobile phone, this is not desired. If possible, it is preferred that all keys for signing and authentication certificates be created on the device itself to limit the risk of key migration or interception. The underlying idea is that the more opportunities there are for a private key to be stored on more than one computer, the less confidence exists that the correct user has possession and control of the private key.

Issuance of an LOA 4 credential requires additional steps to include in-person registration with an authorized individual, biometric authentication, and the generation of signing/authenticating keys on a FIPS 140-2 Level 2 approved hardware device.

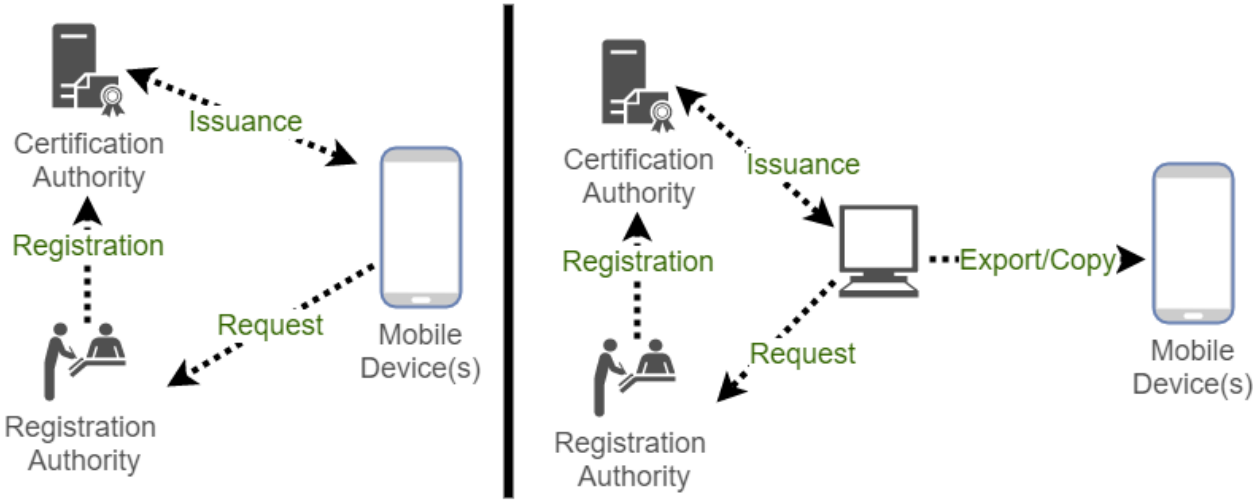


Figure 3: Credential Issuance Device Centric vs External System Generated

DPC Solution Considerations

When selecting a solution for the issuance of a DPC the following options should be considered depending on agency requirements:

- Mobile Operating Systems/Platforms (iOS, Android, BlackBerry, Windows Phone, Laptop with Virtual Smart Card)
- Delivery of Credentials to Keystore(s) for Required Apps (1st party, 3rd party, custom/wrapped)
- Mobile management architecture and attendant requirements (BYOD? Work device? COPE?)
- Support for LOA 3, LOA 4, or Both
- User-Self Service with Mandatory PIV Authentication
- Certificate Issuance from Multiple Certificate Authorities
- Private Key Generation on Device for All Key Stores
- Full Lifecycle Management (including revocation and renewal)
- Integration with MDM to Further Control Devices Receiving DPC
- Toolkits to Support MDM/EMM Ecosystem Apps Access to DPC
- Automated Federal Bridge Checks & Follow Up per SP 800-157

Derived CAC/PIV Lifecycle Management

The issuance of a DPC is only one part of a larger lifecycle process with credentials. Certificates have a specific lifetime with a beginning and an expiration date and contain information about the user which may need to change during its lifetime. On a mobile device, the primary concern after issuance is renewal prior to certificate expiration and updates like name changes. The

process needs to be relatively seamless to the user to avoid disruption and must be able to address certificates in all key storage locations.

Just as with a physical CAC or PIV, it must be possible to revoke certificates contained on a mobile device. Traditional smart cards have no wireless remote-wipe capacity, however, mobile devices under a managed solution provide additional capabilities. So, while the first step in the loss of a mobile device, just like with a CAC/PIV is certificate revocation, MDM/EMM solutions may also provide more timely destruction of credentials and removal of applications which could use them. Having a managed device or workspace offers the additional options to:

- Remove the DPC issued under an MDM profile.
- Remove applications which might use the DPC.
- Wipe the enterprise workspace that may contain a DPC.
- Wipe the entire device including any stored credentials.
- Automate revocation of DPC and addition to a CRL.

Mobile Device Certificate Storage

In theory, there are a wide variety of locations that user certificates may be stored for use by applications and services on a mobile device. On Windows, which has a robust built-in credential service layer and trusted platform module (TPM), the issuance and use of credentials, DPC or otherwise, is relatively easy. The credential service layer both enforces PIN's for access to private keys and provides an abstracted interface for applications to use such credentials. In other words, it is easy for developers to request operations involving a certificate.

However, on iOS and Android, which lack a robust and flexible cryptographic service layer, the selection of the "right" location can be a large problem, and normally the location and type of app needing access to the certificate will drive which credential store location is necessary.

Options for location of certificate storage can be one of the following:

- Cryptographic Software (for LOA 3)
  - System Key Store/Key Chain
  - Application Key Store
  - Mobile Device Management/Android for Work Key Store
  - Trusted Execution Environment (strengthening other options)
- Cryptographic Hardware (for LOA 4)
  - Universal Integrated Circuit Card (UICC)
  - Embedded Secure Element
  - MicroSD

As may be obvious right away, there are numerous options and the selection of certain locations will automatically exclude certain operating systems or applications or use cases.

Cryptographic Software – Level of Assurance 3

The issuance of LOA 3 derived CAC/PIV credentials requires, among other things, storage in a FIPS 140-2 level 1 software storage container. Today, most mobile phone platforms provide such a storage container. Yet issuance alone does not enable use of a DPC. The objective is to use a DPC for authentication, signing, and/or encryption. Thus, PKI-aware applications need to be able to access the DPC. On Windows and BlackBerry this is straight forward, with the operating system having a robust built-in credential service layer which provides applications access to credentials regardless of where they are stored.

Did You Know? Microsoft Apps on iOS/Android aren't PKI aware. They rely on the use of Modern Authentication. In other words, they use federation passive redirection for authentication to Microsoft Federation Service (an IdP) which supports certificate based authentication and then passes a token to the app in question for authorization to use an O365 resource.

On iOS and Android, an applications ability to access credentials depends on app signer (author) and location of certificates. For this reason, the location selected for issuance of credentials is driven more by the consuming application and less on a desire to store credentials in the most secure location

Multi Factor Cryptographic Software[3] – System Keychain (iOS)

The iOS platform provided by Apple includes a keychain mechanism designed to allow the secure storage of security critical information like user passwords, or in the case of DPC, the private keys associated with them. Storage of certificates in the iOS system keychain provides a great deal of flexibility for agencies since it allows use of certificates with Safari, the default mail application, VPN, Wi-Fi profiles, and other certificate aware apps authored by Apple.

These apps, authored by Apple, are also known as 1st party apps. Note that certificates placed in the iOS system keychain are available to any 1st party application once the device is unlocked. There is no additional user prompt or certificate specific PIN that must be provided before use of the certificate so it is essential that such devices are under enterprise control with screen timeout/lock to be considered acceptable for LOA 3.

Multi Factor Cryptographic Software – System Keychain (Android)

Like iOS, Google's Android platform offers a system location for the storage of security critical tokens like user passwords or private keys for DPC. Google authored applications (a.k.a. 1st party apps) can access certificates stored in the system keychain. Unlike on iOS, however, any other app on Android devices can also access these certificates. This configuration makes it very easy to utilize a DPC on Android by the default browser and mail client. However, it also allows any other application, including malicious software to use a user credential without impediment

[3] NIST SP 800-63-3 Draft, Section 5.1.6 Single-factor Cryptographic Software, https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

after the phone is unlocked. Certificates stored in the system keychain may be used by the default mail client, default browser, VPN, and Wi-Fi profiles.

As with iOS, certificates stored in the system keystore on Android do not allow an additional PIN to protect their use so it's imperative that these devices are under enterprise control with a required screen timeout and lock.

Multi Factor Cryptographic Software – Application Keystore (Android)/Keychain (iOS)

As an alternative to the system keystore/keychain, a developer can opt to store key materials in an application specific location. More accurately, key material can be stored such that only the application signer (author) can access it. Multiple applications can access key material long as they have a signer in common. By storing keys in this way, the attack surface is reduced but so is usability since access to the certificate is much more limited. This option provides the opportunity to prompt users for a PIN which might protect private keys yet it also requires the app developer to have a greater understanding of public key cryptography, protection, and usage. The ability to enforce PIN protection of the certificates in an application keystore/keychain is consistent with requirements for user intent outlined in DRAFT 800-63-3.

Multi Factor Cryptographic Software – Mobile Device Management/Android for Work Keystore

Like an application key store, this option also reduces the attack surface and usability but not as far as an application specific key store. In this case applications have an MDM/EMM signer in common and thus all MDM deployed applications have access to key material. To assist application developers, many MDM/EMM platforms provide an API or SDK framework to simplify access and operations related to public key cryptography; essentially easing the burden on the app developer and simplifying access to FIPS 140-2 evaluated cryptography. As with an application specific keystore/keychain this option also is consistent with demonstration of user intent outlined in DRAFT SP 800-63-3.

Hardware Backed Multi Factor Cryptographic Software – Trusted Execution Environment

Over 1 billion phones on the market now are equipped with a Trusted Execution Environment (TEE). This technology effectively enables phones to run two isolated operating systems; one the Android operating system, and a second secure operating system that cannot be directly accessed by applications in the Android environment. The intent with a TEE is to further restrict access to highly sensitive secrets as well as sensitive functions like cryptographic operations or payment processing. Although not physically separate hardware, the chipset itself enforces hardware isolation, preventing access to the secure OS even from a rooted Android operating system on the non-secure side. Software developers write applications with two components; a public component which runs in Android and is available from Google Play or other app market, and the secure component which must be delivered through a Trusted Application Manager (TAM).

Storage of derived credentials requires development of a customized application comprised of two parts. First, a standard Android App available to users by app store or MDM/EMM delivery. Second, a trusted application delivered securely to the TEE via a Trusted Application Manager, a service specifically developed to cryptographically protect and facilitate delivery of trusted

applications. The standard Android App would work in conjunction with the trusted app, requesting sensitive operations.

The TEE architecture enjoys global investment and requirements driven across markets. Billions of dollars are being invested and the technology provides a future platform for secure information sharing, Blockchain and IoT controls. Recent devices support a trusted user interface to provide isolation for PIN entry, data Input and secure display. Trusted display and trusted PIN entry assures that malware on a device will not be able to access the TEE protected credentials without user permission. TEE also supports basic capabilities for attestation of the supply chain integrity and the TEE operations are functioning in a reference condition, thus providing the real-time assurance that the TEE in a remote device is operating in a known condition

It should be noted that many of the cryptographic software storage options discussed above are already working somewhat transparently with a TEE on devices from some hardware manufacturers. Thus, the use of a TEE is not necessarily exclusive of other software storage options. The TEE does provide added security in the form of a separate measured and monitored execution environment for the protection of key material and secure user consent, the platform is not currently considered to be suitable for LOA 4 due to a lack of physically separate hardware and FIPS 140-2 Level 2 certification. It is important to note that LOA 4 and FIPS 140-2 level 2 do not address the advanced assurance capabilities manufacturers are building in. Draft NIST 800-63-3 is beginning to contemplate secure display and attestation as part of the levels of assurance. As the TEE develops, it would be helpful to request FIPS support from device manufacturers to ensure the additional value in the TEE can be realized.

Cryptographic Hardware – Level of Assurance 4

Storage of derived PIV/CAC credentials for use in LOA 4 environments requires the use of cryptographic hardware. In other words, a hardware device, specifically designed to be used in a computing platform that meets or exceeds FIPS 140-2 Level 2 overall and Level 3 for physical security. The requirements associated with LOA 4 significantly limit the key storage options for mobile devices, and few solutions are for iOS, so most agencies today are focused only on LOA 3 with a future eye towards LOA 4 for limited groups. Agencies should consider establishing clear requirements for secure PIN entry and or secure biometrics for future procurements. In addition, all hardware should be provided with sufficient data to verify the supply chain integrity of any cryptographic hardware (addressed in aspects of NIST 800-147).

Multi Factor Cryptographic Hardware – Universal Integrated Circuit Card (UICC)

One alternative for hardware storage of cryptographic keys and modules is within a UICC (aka SIM though a bit more modern). Since the UICC is effectively a smartcard, though in a smaller form, it is possible for the card to contain the same data containers as found in a CAC/PIV, providing integrated LOA 4 support. While access to the real estate provided in a UICC is generally owned and managed by a mobile network operator, it is possible to work with both the mobile network operator (MNO) and card manufacturers to leverage this option.

Multi Factor Cryptographic Hardware – Embedded Secure Element

Another alternative for cryptographic hardware storage of keys and modules is an embedded secure element (SE). Unlike the UICC, the SE may have additional processing power and storage. However, access to this is also limited as "owned" real-estate within a phone. Moreover, technical advancements and a desire to reduce phone manufacturing (aka BOM) costs, means SE's are disappearing from many phones. Even if access to the SE were an option, the shrinking number of devices with an embedded SE would mean enterprises may have significantly reduced choice and difficulty maintaining supply.

Multi Factor Cryptographic Hardware– MicroSD

MicroSD offers significantly more memory and processing capability, thus making it a good alternative for devices which support MicroSD. Its use is likely to be ideal for very specific use cases, however, since there is only one FIPS 140-2 Level 2+ approved product (GO-TRUST) and Android is the only platform with an available slot for a MicroSD card. For iOS devices, an additional hardware attachment is needed to provide the MicroSD slot. Increasingly, many manufacturers are also no longer including a MicroSD capability so an already limited option may become even more limited in time.

Key Storage Locations for LOA 3 & Implications

While the initial inclination might be to select a key storage location first, this approach may quickly limit the usability of a stored mobile credential. The architecture of Android and iOS in some ways is more secure than a traditional PC. On both platforms, certificates may be installed in several different locations which impact access by applications on the platform. Applications can store sensitive data in keychain or keystore locations that are application specific. When this is done access to such material is only allowed by the app or other apps having the same signer. MDM/EMM platforms sign applications deployed and managed and thus certificates issued to the MDM keystore can be accessed by a wider range of applications sharing the same signer. Issuing certificates to the iOS system keychain allows access by any Apple signed app like Safari or the system mail client. Issuance to an Android system store allows access by any application installed on Android.

The variety of locations that certificates can be written to makes it critical to determine which apps need access to certificates first. Once the application suite is determined then it becomes possible to determine which key storage locations will be available as options to support the needs of the agency.

Additionally, the use of a browser to perform authentication to an IdP which is discussed later provides significantly increased flexibility as apps can offload the need for certificate access to a browser that handles authentication to the IdP and simply hands the app an authorization token.

Certificates Issued to Mobile

While DPC Authentication certificates are the primary focus for SP 800-157, there are a variety of functions that can be performed with certificates available to a mobile device. Some operations may be consolidated in terms of required certificates but this will depend on the agency. Some of the certificate types that may be of interest are outlined in the table below.

Certificate	Purpose
DPC Authentication	Authentication certificate showing proof of identity backstopped by Government Issued PIV – Used to prove identity in a manner that is administratively tied to Government Issued Personal Identity Verification badge.
Signing Certificate	Document or Data Signing – Used to generate proof of authorship and integrity where such proof is required.
Encryption Certificate(s)	Email or Data Encryption – Protection of data which may be stored on a mobile device, sent via email, or otherwise requires data privacy.
VPN Certificate	Support Device or App Level VPN – Support user authentication and encryption of network communications between a mobile device and the enterprise where data privacy is required.
Wi-Fi Certificate	Support Network Access via EAP-TLS – Support user authentication and encryption of network communications between a mobile device and an enterprise wireless network.
Device Certificate	Issued to Authorized Enterprise Devices – Establishes trust that a mobile device is managed by the enterprise.

Credentials for Multiple Users

There are several use cases across the government to support issuance of more than one DPC to a single phone. Most of these use cases relate to shift work in some manner, like physical security personnel, hospital staff, etc. While issuance of certificates of different types and for different users can be done today there are significant limitations and the configuration presents both usability and security challenges to manage.

From a usability perspective, the large number of potential certificates issued to devices means that the selection of the correct authentication certificate may be a challenge if certificate naming is not carefully considered. Limiting the number of certificates issued to such a device will help dramatically both in terms of usability and avoiding practical limitations around the maximum number of certificates some UI's will show for user choice.

The security implications of multiple certificate issuance are likely to be the larger obstacle. As discussed, certificates placed in the system store on iOS and Android are available with no

additional PIN prompt once the device is unlocked. In this case, while system applications may be able to use the certificates, there is no way to ensure the user selects their own certificate. What's more, if mobile applications are desired which operate on behalf of a user there isn't an easy way to terminate active sessions and tokens across all applications when the device is "handed off" at a change of shift.

At present time, multi-user solutions with DPC is generally not considered to be practical and is an opportunity for commercial innovation.

Roadmap to Mobile Identity Management & Usage

A common concern for U.S. Government agencies is the cost and labor associated with elimination of usernames and passwords in favor of Derived PIV Credentials. Two concerns stand out; the cost and labor involved in updating existing systems and choosing a flexible, standards-based, authentication model that can grow with the agency and does not tie them to a specific vendor.

In support of strong, DPC based authentication and authorization, we recommend an identity provider (IdP) centric approach that supports a wide variety of authentication standards, all of which are anchored in a DPC on a mobile device. This DPC, of course has been issued based on proof of possession of a PIV and the strong identity proofing processes already established in FIPS 201 and HSPD-12.

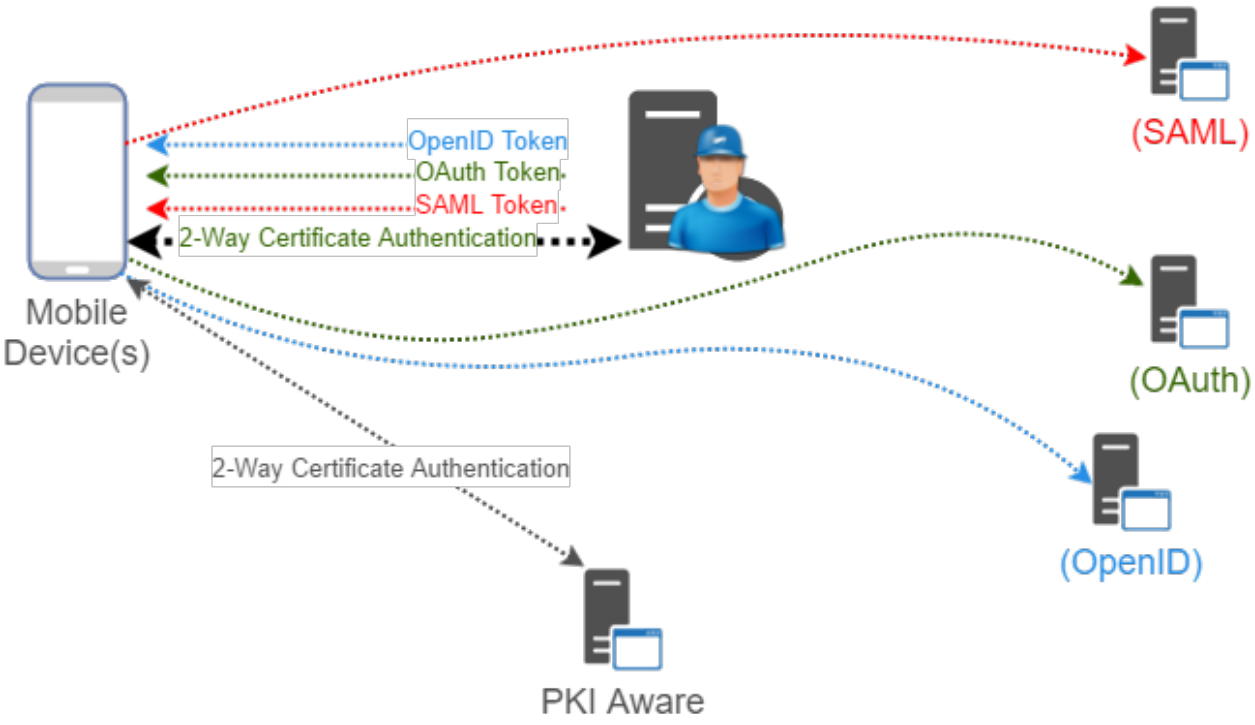


Figure 4: Usage of a DPC with Alternative Authorization Protocols

An IdP centric model which supports authorization tokens linked directly to a DPC allows significant flexibility for agencies as they both modernize and build new systems to support mission and administrative functions. Where higher assurance is required, a system may be fully enabled for certificate based authentication with the DPC or enabled for document signing or encryption with alternative certificates available to the mobile device. However, in use cases where only user authentication is required, token-based protocols like SAML, OAuth, and OpenID Connect which leverage a DPC for initial authentication will offer agencies more effective alternatives including the use of authentication and authorization patterns which may be easier for vendors to implement and support out-of-the-box in commercial applications.

The use of an IdP centric model provides an added opportunity for federation rooted in a DPC and ultimately a PIV. This model can support inter-agency federation as well as the potential for new partnerships with non-US Government entities. Among other things, the model allows for additional data privacy afforded through a reduction in data provided in an assertion. For example, an agent with the FBI can strongly authenticate to an IdP which then provides an assertion for a state website that the user is merely an authorized US Government law enforcement user, obfuscating additional details that would be available in a DPC like agency and name.

Website Authentication

There are several mechanisms in use for user authentication to websites with, predictably, username and password being the most common. However, aside from email authentication, the use of a DPC on a mobile device for strong authentication to a website is a logical early step. Many agencies have already begun the process of PK enabling websites for user authentication, though the progress that has been made varies widely. Even within the Department of Defense there are many websites that are still unable to support certificate based authentication using a DPC. Many of those that are capable of supporting certificate based authentication aren't configured to distinguish between certificate types that may be configured for authentication, those configured for authentication, and those that have been issued for LOA 3 vs LOA 4.

Across the U.S. Government the sheer number of websites currently in use combined with the relative lack of PKI specialists may make full PK enablement of all websites impractical or impossible. Instead, full PKI enablement should be considered one tool in the arsenal. The goal needs to be strong user authentication that can be traced to a DPC anchor. The "last mile" of authentication and authorization, however, may use Kerberos, SAML, OpenID Connect, or even OAuth. Expanding options for the "last mile" leverages alternative authentication and authorization patterns that also have broad adoption and vendor support, providing a foundation for easier integration of future applications and services.

Enabling Mobile Apps

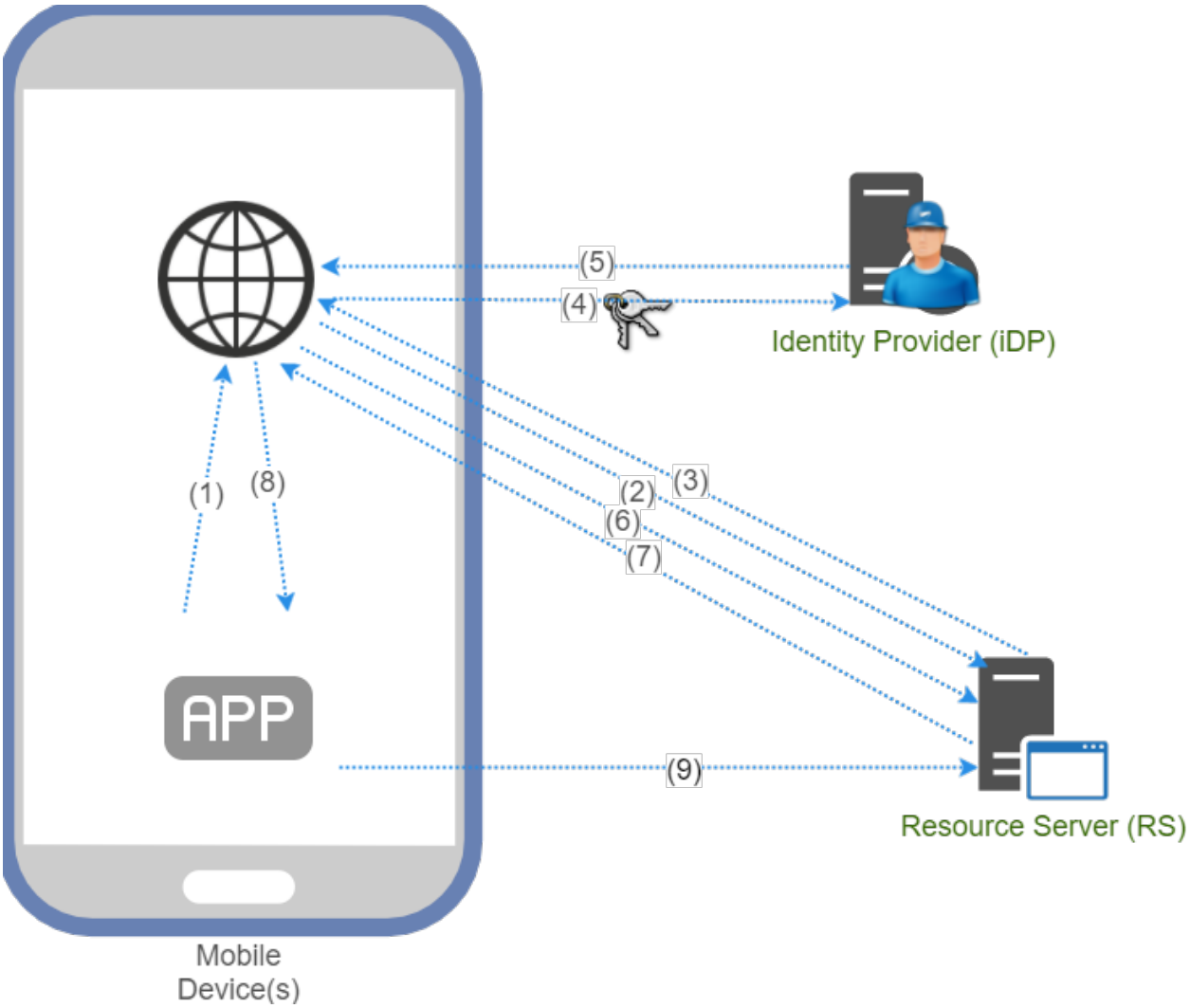
There are several ways to leverage a public-key based DPC for use in mobile devices, from building fully PK enabled applications to using certificate based authentication before

transitioning to SAML and/or OAuth protocol flow or other tokenized solution. Directly PK enabling mobile applications is likely to be more technically complex than many application developers are used to, and overkill for many use cases. Doing so requires significant attention to the location of the certificate(s) for use, an understanding of development for public key cryptography, and minimizing complexity of the overall user experience. Fully PK enabled applications can enable capabilities such as non-repudiation, document signature, and encryption of data using a DPC and related encryption key(s). However, for many applications the primary objective is strong authentication.

Many existing systems, especially those in the cloud, utilize SAML to facilitate Single Sign-On, eliminating the necessity for resource servers to maintain their own user credential database. For example, enterprises incorporate the use of an IdP platform (for example Ping Identity or OKTA) to support authentication for SAML enabled applications like SalesForce.com, Jive Software, and ServiceNow. The configuration allows enterprise users to leverage their existing enterprise username and password to gain authorization for such cloud applications. SAML is a well-known authentication pattern for cloud services and is increasing in use.

Existing authorization patterns for mobile apps typically use OAuth, granting apps the ability to communicate with resource servers on behalf of a user. Its use is commonly seen with third-party developed apps that interact with the likes of Facebook and Twitter on behalf of an individual user. The user downloads the third-party app and, on launch, is redirected to an authentication portal which ultimately issues an OAuth grant to authorize the app to operate on behalf of the user. Like SAML, it too is a well-known authorization pattern in use for both cloud and mobile applications.

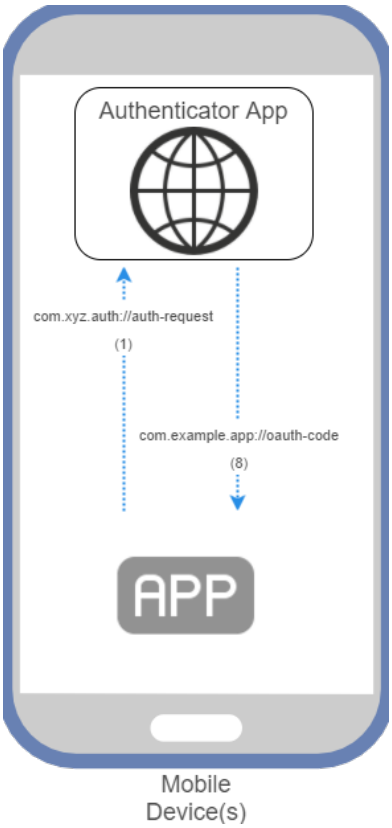
To extend these models such that the authentication chain is directly linked to a DPC, we build upon available Inter-App Communication conventions found in iOS, Android, and other platforms in combination with SAML 2.0 and the draft IETF publication OAuth 2.0 for Native Apps with a combined authentication and authorization pattern for native mobile apps as depicted below:



1. The Mobile App, requiring an OAuth grant to communicate with a resource server (RS), makes a request of a common browser (not an embedded web-view) to begin authentication.
2. The browser initiates a request to authenticate with the RS.
3. The RS recognizes the request from the system browser for authentication and re-directs to an identity provider (IdP) that is PK enabled.
4. The browser makes an authentication request to the IdP, prompting the user to select a certificate to authenticate.
5. The IdP returns a SAML assertion along with a redirect URL.
6. The browser requests authorization, presenting the SAML assertion to the RS.
7. The RS generates a unique OAuth 2.0 authorization code returning it to the browser with a URI that will open in the Mobile App using a custom scheme, app link, or other inter-app communication mechanism.
8. The browser makes the request to the initiating native application which picks out the OAuth 2.0 code.

9. The native app makes the request to the RP with the auth code. An access token is returned to the App which stores it for continued communications with the RS API's.

Skip the Embedded WebView for Authentication



While embedded WebViews were once the only mechanism within a native mobile app to facilitate authentication to the IdP, more secure alternatives are now available on major mobile platforms. Although less of a risk when using certificate-based authentication, the use of WebView allows the 3rd party app developer full access to credentials provided in their app. In the case of username and password the use of WebView allows a potentially malicious app developer to capture username and password of the user. Further the WebView lacks awareness and trust of the server one is connecting to, reinforcing a potentially dangerous user behavior of providing credentials to an unknown server.

Best practice is to use an external authenticator, commonly a system browser but alternatively a trusted authenticator app designed for this purpose, instead of an embedded WebView.

Enhanced Security

The described flow above leverages the system browser to facilitate authentication to an IdP. Unfortunately, on iOS and Android, certificates stored in the system keychain can be used directly without secondary PIN prompt. For additional security, a customized Authenticator App may be deployed in conjunction with the app used for DPC creation. This may be a single app in the form of a customized browser plus functions for creating PIV Derived credentials, or two apps, one as authenticator and one for creation of PIV Derived credentials, so long as they have an app signer in common.

In this case the app would use Inter-App Communications to pass its request for authentication to the authenticator app. The authenticator app, in turn will prompt the user for the PIN protecting the client cert private key which is stored in its own app-specific keystore, before continuing-on.

The benefits of this model are two-fold. First the private keys used by the authenticator are isolated and access to them is highly controlled. Second, since these certificates are stored in an app-specific keystore, it's possible to mandate input of a user PIN before the certificates may be used for authentication.

On the downside, this model does require the developer of the native mobile app to know the Custom URI convention declared by the authenticator app, and more importantly requires development and maintenance of a customized browser.

Usability & Security Enhancement Opportunities

Friendly Certificate Naming

The Federal PKI ecosystem plus any additional PKI certificates that might be issued to users creates a challenge for the overall user experience. Not all solutions support adding a "friendly name" to certificates and even if they did, such schemes externalize this work onto users who do not have a working knowledge of PKI. Harmonized naming of certificates, using a name meaningful to end users, would significantly improve the overall user experience.

MDM/EMM Certificate Issuance & Management API

Many agencies have a desire to more tightly integrate DPC issuance and management within an MDM ecosystem. As it stands today most MDM integration is a loose coupling intended to make it easier to both deploy a credential issuance app by the MDM/EMM and for the user to collect their DPC in a way that makes it available to MDM/EMM managed apps.

Credential revocation and deletion can be particularly problematic though not for the obvious reason of device loss/theft. In most agencies BYOD as a supported model is still coming of age so most devices remain as GFE. These devices often migrate throughout an agency moving from user to user as positions change, new hardware becomes available, or for other organizational reasons. In this case a device needs to be wiped and re-issued. However, user certificates must also be revoked and appear on a CRL. Therefore, support processes need to be developed that account for certificate revocation if this process doesn't occur automatically when an MDM transfers ownership or wipes a device.

There is currently significant work underway by most MDM/EMM players on the integration of capabilities of Credential Management Systems and the full capabilities vary significantly. The integrations today can include any number of functions including:

- Capacity to deploy a credential issuance app into an MDM.
- App ecosystem integration where MDM/EMM managed apps have a common API that apps can call to use issued credentials.
- Enrollment integration to couple enrollment and DCP issuance into a more streamlined experience for the user.
- Lifecycle integration to coordinate credential removal from device and/or revocation and addition to a CRL when an EMM/MDM is used to wipe a device.

Certificate Checking by Relying Parties

The Federal PKI Policy Authority has established a number of OID's to be asserted by various types of certificates. Examples include OID's to assert that a certificate is stored in cryptographic software (LOA 3) or in cryptographic hardware (LOA 4). However, relying parties across the government are inconsistent at best in their application of certificate checking. In many cases

relying parties simply look for individual identity or agency but do not confirm that the OID asserted matches the level of assurance required by the relying party itself.

Credential Unlock with Secure User Interaction

When necessary, mobile solutions require the user to enter a PIN or provide a fingerprint to unlock access to a DPC. However, these actions are potentially at-risk to applications and malicious software on the mobile device. By default, there is no trusted user interface available to mobile apps. Today most mobile devices include a TEE built-in with their ARM chipset. A unique security feature of the TEE is the capacity to secure the user interaction on devices (e.g. PIN entry, fingerprint recognition). Indeed, many Samsung/Android (BBDTek is hardened out of the box) devices already are supporting the Trusted User Interface and secure fingerprint as a way to mitigate potential risk of malicious software intercepting user sensitive biometrics and pin numbers. Trusted User Interface also provides the ability for the user to visually confirm the details of the request for an authentication or a signature. This can dramatically reduce the Phishing attack models that rely on tricking users. Secure display is also part of the chipset capabilities from Intel on most Intel devices. Detailed review of commodity hardware procurement should be done to verify that requirements for secure display and secure input are part of the standard specification. This should also include the required level of certification. Increased demand for such capabilities from US Government and regulated industry customers is an opportunity to increase availability of such features in future devices.

Attestation

Everything has an identity…people, apps, data, transactions and devices. In fact, mobile devices have multiple identities adding to the complexity of ensuring trusted identities, credentials and transactions. The figure below, originally published in the Study on Mobile Device Security by the Department of Homeland Security, Science and Technology Directorate[4], illustrates how many things, including higher level applications, services, and data, rely on a strong root of trust down at the silicon layer of modern smartphones (as well as IoT and other computing devices as well).

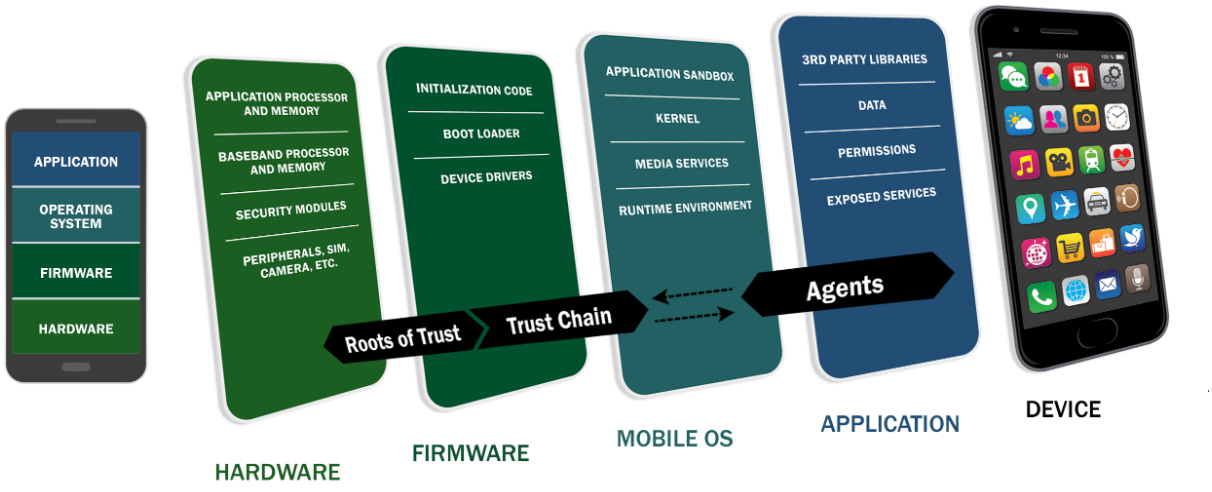


Figure 5: Mobile Device Technology Stack

An important future consideration for all devices is to integrate a cyber security control for any credential store (hardware or software). Attestation provides a mechanism to measure the integrity of the embedded trust system and to make a claim that the trust system is operating in a measured condition or state. Attestation assures that the software and hardware that is providing the vault assures the protection of the secrets at rest and during use. IdP systems should all consider how validation of a real-time measurement can be verified against a reference measurement. Attestation provides a strong architectural component to assure the protections are continuously monitored and can be proven to be in-compliance for any identity transaction.

Device Acquisition - The Device Matters

"Any device" has been part of many specifications and the result has held cyber security back. Devices support varying levels of assurance and capabilities. Manufacturers seek to create varying packages at price points for specific market segments and the lower price points often sacrifice features and security components. For organizations that require strong identity assurance, consider hardware that supports measured isolation that can be proven to be in a known state. TEE, trusted display, secure PIN and Biometrics on ARM and Intel chipsets is being deployed in millions of units per day and provides the industry standard commodity hardware to make a huge difference going forward to the quality of the protections available in mobile devices out of the box.

Future Mobile Identity for the U.S. Government

While working on the Mobile Identity Management project our group had much discussion around alternative and complementary technologies that could be used instead of or alongside DPC. The group had strong interest in two areas specifically; increased use of biometrics, especially for hands-free operation and FIDO.

In drafting this paper the group had a clear objective to focus on how the use of Derived PIV Credentials could be increased today, under existing policy. For this reason, we have tabled the inclusion of biometrics and FIDO. However, it's likely that both will become important to the mobile identity discussion in future years. Indeed, the writing is on the wall for some of these things. At the time, we came together, NIST was well into the development of SP 800-63-3 which takes significant steps to separate identity proofing, credential storage, and federation allowing for significantly more granularity. While it does not go so far as to outline use of biometrics as an authentication token, it does include its use as an access factor for multi-factor authentication.

It also appears from discussions with NIST that there is interest in exploring other "derived" authentication tokens beyond a DPC. So, while a DPC is the primary cryptographic token today there may well be other options for the future. One such option with significant interest in the community is FIDO which is attractive to the community for several reasons. FIDO support is already built in to a great many devices and services. There are FIDO U2F tokens which have

been certified for FIPS 140-2, applicable for LOA 4 usage. Finally, FIDO may offer a flexible, low-overhead, solution for temporary workers, those for whom possession of a PIV represents a security risk, or others who may not necessarily warrant a PIV.

Conclusion

The foundation for the issuance and use of Derived PIV/CAC Credentials is in place today. Most agencies are loosely comfortable with the administrative process required to issue a DPC based on an existing PIV/CAC. Most are also somewhat comfortable with the solutions that can be used for issuance of these credentials. However, there are two major areas where agencies could use some added guidance; integration with mobile device management/enterprise mobility management solutions and the actual use of a DPC for authentication and authorization to existing applications.

Integration of Credential Management Systems with MDM/EMM systems in only in its infancy. For the most part the emphasis is on issuing derived credentials within the confines of MDM managed apps and making it easier for those apps to find and use a DPC. Minimal work has occurred to more fully automate the onboarding process for bringing a device under MDM/EMM control and kick-starting the issuance of a DPC. Further, very little work has been done so far on the automated processes for removal of a DPC from a device and an integrated process for revocation and addition to a Certificate Revocation List. There is plenty of innovation to be seen in this area over the coming years.

When it comes to consumption of credentials, the overall recommendation is to expand the aperture on authentication and authorization protocols used to connect a user with a DPC to resource servers. While it may be necessary to PK enable the services to which users authenticate at LOA 4, this is likely not the case for LOA 3 services. PK enabling an identity provider which can, in turn provide authorization tokens using other industry standards can add substantial flexibility to agencies and may serve to speed adoption and reduce costs associated with moving to multi-factor authentication.

Agencies can get started today by breaking down their DPC programs into the following phases:

Phase 1 - Credential Issuance Foundation

- Install a Credential Management System to issue DPC or extend the existing CMS to issue DPC's as well. The only link between a PIV/CAC and a DPC is administrative, defined by SP 800-157, so there is no requirement to tie a DPC solution to a PIV/CAC issuance platform.
- **Benefits:** Provides a foundation for the issuance of DPC meeting 800-157 that ensures proof of PIV possession before issuance of a DPC that is logically linked to a PIV/CAC, performs 7-day follow-up, and ongoing checks to ensure user is still entitled to hold a DPC.

Phase 2 – Enable System Browser & Email

- Deploy DPC Auth certificates to iOS System Keychain/Android System Store for use by system browser and mail client.
- Enable access to non-PK enabled websites by PK enabling an Identity Provider (IdP) that can pass SAML or OpenID Connect tokens or Kerberos tickets after DPC authentication.
- **Benefits:** Provides basic email access using DPC for authentication. Enables access to PK enabled websites as well as websites which support other authorization tokens issued by a trusted IdP to which the user has authenticated with DPC.

Phase 3 – MDM Integration

- Automate DPC enrollment so that a user with an MDM/EMM enrolled device can request a DPC via self-service.
- Automate the removal of certificates from devices and revocation of certificates with addition to appropriate CRL through the use of MDM/EMM and/or CMS API's.
- **Benefits:** Reduces opportunity to use certificates on a lost/stolen device and reduces the time taken to add a certificate to a revocation list.

Phase IV –Authentication Patterns for Mobile Identity

- Provide guidance on when to fully PK enable an application vs leverage a PK enabled IdP with the downstream app or mobile API accepting SAML, OpenID Connect, or OAuth
- Develop guidelines for how to develop PK enabled mobile apps which directly use a DPC.
- Clearly articulate agency strategy for accepted key storage location.
- **Benefits:** Accelerates mobile use and application development by clearly establishing development requirements for supporting DPC.

Anytime – Enable VPN & Wi-Fi

- Deploy DPC for VPN usage.
- Deploy DPC or Device Certificate for Wi-Fi (EAP-TLS)
- **Benefits:** Adds an additional layer of transport security for devices connecting from outside the enterprise and for those using agency Wi-Fi deployments.

Acknowledgements

The MSCT and the Advanced Technology Academic Research Center (ATARC) appreciate the contributions of the following individuals and organizations in supporting the efforts of the Mobile Identity Management working group and development of this guidance.

David Coley, Intercede

Wendy Fairfield, SurePassID

Paul Grassi, National Institute of Standards and Technology (NIST)

Shoaib Ibrahim, Department of the Treasury

Florent Joubert, Trustonic

"DJ" Don Kachman, Department of Veterans Affairs

Simone Rees, Department of Agriculture

Mark Russell, MITRE

Gaurav Seth, DoD/VA Interagency Program Office (IPO)

Neil Sethi, Department of Veterans Affairs

Steven Sprague, Rivetz

Appendix A – Survey Questions

- Does the issuance and management of Derived PIV Credentials (DPC) mirror that of PIV? I.E. Does the same group oversee both activities?
- What is the status of your Derived PIV Credential (DPC) program? What stage is your department/agency in? (Pilot, IOC, FOC, Other)
- Please describe your current mobile architecture in support of mobile app enablement? Is the architecture designed with any particular model in mind? VPN Model? Access Gateway Model? Other?
- What is your desired mobile architecture if different from the current architecture?

Business use of DPC

- Has your agency/department taken steps to DPC enable email and calendar?
- Has your agency/department DPC enabled time cards, purchase and supply chain, or other broad use application?
- Has your agency/department DPC enabled any mission apps? Please describe if possible.
- What would be the top applications or business functions that you would want to DPC enable if you could do so today?
- Where are the largest benefits from DPCs, once issued in your organization (e.g., productivity, access to applications, improved employee experience, etc.)?

DPC Issuance & Lifecycle

- Where is your DPC solution hosted? On-Premise or Cloud? What was the primary driver for this decision?
- What challenges have you faced related to the location of your DPC solution and how were they addressed?
- Are you using an MDM, a CMS, or something else for the delivery of DPC? What does the issuance process look like?
- How is lifecycle management of DPCs accomplished? (e.g., revocation, linkage to PIV cards, issuance of multiple DPCs to one individual).
- Are you doing daily, hourly, 7 day checks for revocation of PIV?

Support of DPC

- How was DPC support integrated into existing helpdesk processes?
- Have you developed and can you share training documentation?

- Any lessons learned documentation from agencies that have begun or completed a DPC project (e.g., challenges encountered, risks, mitigation strategies, user experience, hosting considerations, etc.)

App Enablement

- What approach are you using to DPC enable apps for mobile? (PKI Enablement, PKI Authentication to IdP with SAML, OAuth, OpenID Connect, or other afterwards)?
- How are you approaching the process training technical teams to build in capability to support DPC? (e.g., level of support provided to application and system owners, enablement technical guidance, details on stakeholder outreach program, etc.)?
- What challenges have you experienced DPC enabling apps?

Appendix B - Component Providers

CMS Vendors

- Entrust
- Intercede

MDM Vendors

- Airwatch
- BlackBerry
- IBM
- Microsoft
- MobileIron
- Citrix

Identity Provider Vendors

- Centrify
- ForgeRock
- IBM
- Microsoft
- OKTA
- PING Identity
- SailPoint
- SurePassID

Trusted Execution Environment Vendors

- Solacia
- Trustonic
- TrustKernel

References

Department of Defense Instruction 8520.03, May 13, 2011, Identity Authentication for Information Systems, http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf

Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0, December 2, 2011, https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNNBAA4&field=File__Body__s

Federal Identity, Credential, & Access Management; Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-On (SSO) Profile, Version 1.0.2, December 16, 2011, https://gsageo.force.com/IDM/servlet/fileField?entityId=ka0t0000000TNKHAA4&field=File__Body__s

FIDO Alliance White Paper: Leveraging FIDO Standards to Extend the PKI Security Model in United States Government Agencies, https://fidoalliance.org/wp-content/uploads/White-Paper-Leveraging-FIDO-Standards-to-Extend-the-PKI-Security-Model-in-US-Govt-Agencies.pdf

NIST Special Publication 800-63-2 Electronic Authentication Guideline, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

NIST Special Publication 800-63-3 (DRAFT) Digital Identity Guidelines, https://pages.nist.gov/800-63-3/sp800-63-3.html

OAuth 2.0 for Native Apps, draft-ietf-oauth-native-apps-09, https://tools.ietf.org/html/draft-ietf-oauth-native-apps-09

Payment Services (PSD2) – Directive (EU) 2015/2366, The European Commission of the European Union, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

Study on Mobile Security, Department of Homeland Security, Science and Technology Directorate, https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

Trustonic TEE for Derived Credentials, https://www.trustonic.com/about-us/downloads/

User Identity Authentication Enterprise Design Pattern v2.0, http://www.techstrategies.oit.va.gov/docs/designpatterns/Privacy%20and%20Security%20User%20Identity%20Authentication%20EDP%20V1.7_For%20Signed.pdf

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Internet of Things (IoT)

Working Group Document

Introduction

The ATARC/MSCT Combined working group on Internet of Things (IoT) has as its goal to produce materials and artifacts that advance the working knowledge of IoT conceptually and practically. It is our belief that once federal agencies and industry use similar language to define, describe, and outline IoT conceptually, it will facilitate a more rapid understanding and create efficiency of thought, information exchange, and eventually adoption. In the context of this document, the common-vernacular term of "IoT" (Internet of Things) is used interchangeably with "NoT" (Network of Things).

The promise and potential of IoT is clear. It allows for greater efficiency and innovation, doing what we are doing now, but better. That being said, this is a technical capability that is emerging. Little of IoT is concrete at this point, and there is no obvious ROI associated with this technology, however like the emergence of the internet itself this will occur when taking a long view.

The emergence of IoT is considered an iterative process. Unlike waterfall or agile development, an iterative process emerges rather than being purposefully built towards. With IoT, there are things that we know today and are capable of doing; there are things that we would like to apply this technology towards but do IoT know how it will fit or function; and there is the most exciting aspect of this development which will be the adoption to scenarios that we have yet to imagine, realize, or envision but will most certainly emerge.

The goal of this document is to define the term IoT, identify essential and desired characteristics, its benefits, and how it is evolving.

A Simple Definition of IoT

"IoT is an infrastructure of networked objects (cyber-physical devices, information resources, and people) that interact with the physical world through sensors and actuators. This infrastructure enables the collection, transport, storage, assessment and action on data done with or without human intervention."

Note - This is how the working group defined IoT. We recognize that other definitions may exist, however, may differ in scope.

Component Details

- "**An infrastructure**" The term IoT is used to describe both the systems created using IoT (perhaps better referred to as IoT systems) and the environment used to build the IoT systems.
- "**Networked Components**" IoT is similar to traditional IT in that the components are connected to other components in a one to many relationship. The network is IoT defined as a specific type of network technology or architecture, but does need the capacity to connect one component to multiple other components. This networking capability is what differentiates IoT from a generic cyber-physical system [provide definition of CPS]
- "**Information Resources**" The traditional IT resources are an important part of IoT. The ability to store data, process data, and move data are central to any IoT system. When considered in an IoT environment new concerns related to the interaction with the physical world must also be considered in addition to the concerns of traditional IT systems. Information resources can process, store and transmit data.

- "**Cyber-physical Devices**" Components providing the sensing and actuating capabilities. These devices are the key to interacting with the physical world.
- "**People**" People are very important to IoT. They take on three very different types of roles (and may have more than one type of role at a given time). The first role is one most of us consider when we think of IoT – the role of system user. The second role type is that of physical entity of interest – the entity that a IoT system observes and acts upon. The third type of role is that on system participant – people that participate as a component within an IoT system.
- "**Sensors and actuators**" These digital transducers are the components that interact with the physical world. Unlike traditional transducers that convert energy from one form to aIoTher (usually from or to some form of electrical energy), digital transducers convert energy into digital data or digital data into energy.

Essential Characteristics

While the above definition seems extremely simple, it captures the core ideas that all IoT systems are based on. There are two key concepts that make IoT such a new and important concept:

- Components have standard interfaces and are connected together via a network
- Some components have the ability to interact with the physical world through sensing and actuation

Desired characteristics

Below are some characteristics that are common in any IoT system. These characteristics are essential to the success of the deployment of an IoT system.

Component description and discovery

IoT systems are composed from a set of diverse heterogeneous components that can perform differing functions. To this end the architecture should provide components whose characteristics and behavior are well defined and these components should be well described, (i.e. provide identification and description using standardized semantics and syntax so a system builder has confidence the components will provide the desired functionality within the IoT system). Components should use standardized component/service definitions, descriptions, and component catalogs where possible. IoT components also need to be discoverable – both the component itself and the component description.

Component composition, orchestration and re-composition

For the system to integrate different components into a working system, the components should be modular and the interfaces to these components should be based on well defined, interpretable, and unambiguous standards so the components can interact together. To be a 'working' system, an understanding of the composed systems behaviors should be accessible from the understanding of these standards for the components.

Security authentication and encryption

The process of verifying the identity of a user, process, or device is a prerequisite for granting access to the system or components. This process must work for small localized systems and scale to work with large complex systems. Each component of the IoT system should be secure against unauthorized access, use, disruption, modification, or destruction. Since each component may be part of a larger virtual system, if a component is compromised (either through a cyber intrusion or a physical attack) the effects may propagate through other components in the system.

The IoT environment should allow controlled access to resources only by appropriate actors with mechanisms in place to monitor access. It should IoT prevent the use of a particular component due to technical barriers. Instead, access to a component should be based on business policies/plans. Mediating user access to a resource (component) in the system allows legitimate use of a resource while prohibiting illegitimate use.

IoT components are connected together through communications networks. These communications networks should also be secure and hardened against cyber intrusion.

Additional "desirable characteristics"

Timely

Timely is a characteristic of providing a service within a specified time, is necessary to deal with a range of functions at different levels within the IoT system. In order to keep time synchronicity among the actions of interconnected things when using communication and service capabilities, time synchronization is required. Accurately associating a time measurement with a measurement from the physical world is an important aspect of IoT components. It is needed to accurately combine or associate data from multiple sensors and data sources. Both the time value and uncertainty of the value are needed to properly assess whether a specific component can perform the requisite task.

Trustworthiness

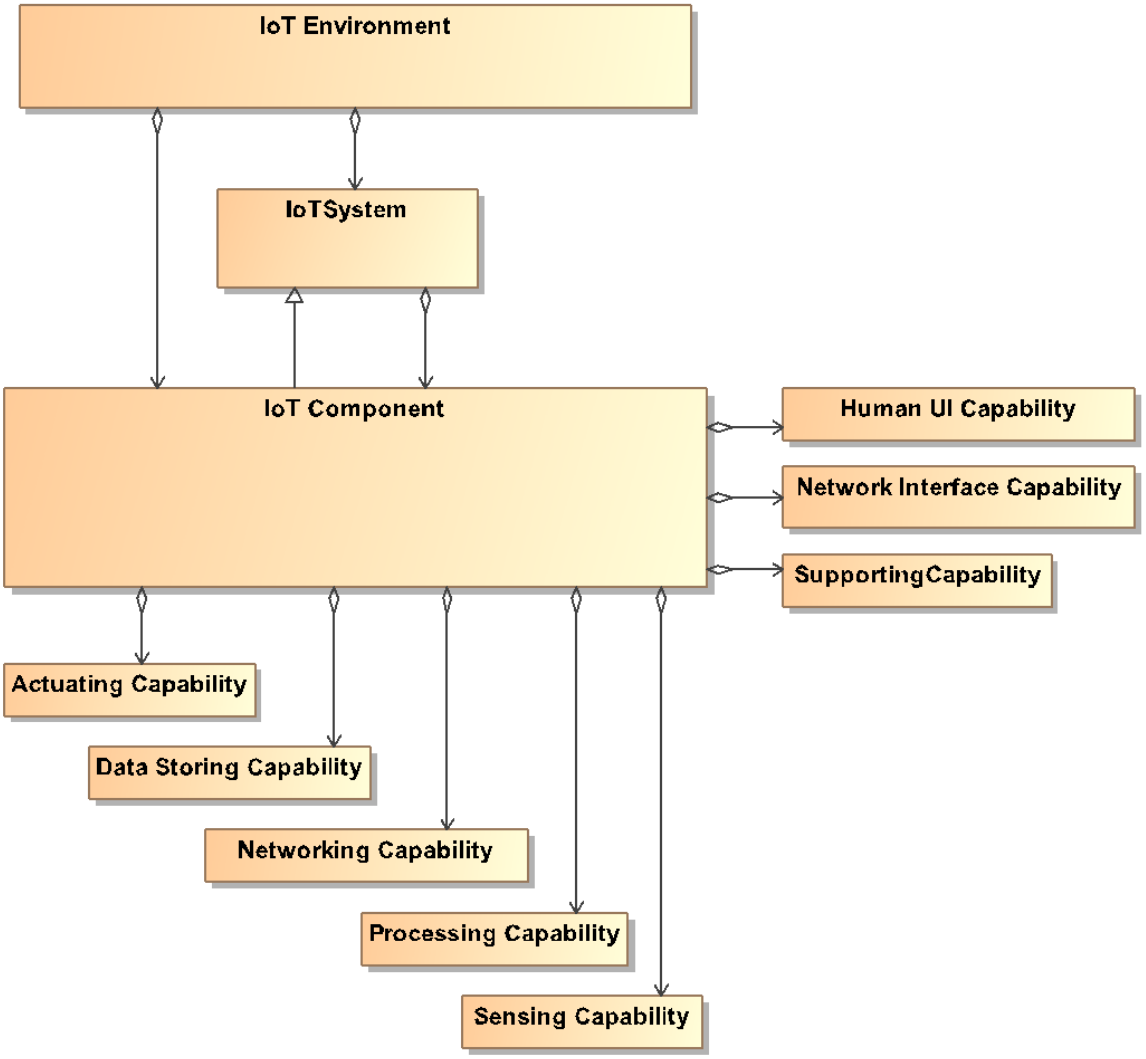
Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but IoT limited to, safety, security, privacy, reliability and resilience. It is important for IoT stakeholders to be able to build IoT systems that perform according to specification.

An IoT Capabilities Model

From an IoT perspective, a "black box" viewpoint of each component is useful, because an IoT system builder may IoT have access to any details of the internal workings of an IoT component. In fact, the internal workings of a component may change over time. This is especially relevant for IoT components that are themselves composed of other IoT components. If the capabilities

of a component are accurately described, including the details necessary for the system builder to compare capabilities to system requirements, the details of the inner workings are IoT important. If an IoT component uses standardized interfaces through which these capabilities can be described, configured, and accessed, the IoT components can be easily combined into systems, regardless of internal implementations.

Figure 1: Capabilities of an IoT Component



An IoT system builder will combine these capabilities with the capabilities of other components create a system that can achieve a set of goals. By understanding each component as a set of capabilities a system builder can match those capabilities to their system requirements. Using

this capabilities viewpoint, an IoT component can be understood by the set of capabilities it provides. The following eight IoT capabilities are included in Figure 1, above.

Actuating

The actuation capability provides the ability to make a change in the physical world, based on a digital input signal. Some examples of actuation capability include; heating coil (heating capability), electronic door lock (lock/unlock capability), servo motors (motion/movement capability), robotic arm (complex motion/movement capability).

Data Storing

The data storing capability provides the ability to store data and information over time. Some examples of data storing capability include cloud storage capability, database storage capability.

Human User Interface (UI)

The human UI capability provides the ability for the component to interact directly with people. IoT all IoT components will have a human UI capability (i.e., a processor component may only provide data through the network interface, while a cell phone has several human interface capabilities in the form of the touchscreen, audio and camera). Some examples of human UI capabilities include: display capability, touch screen capability, and audio capability.

Network

The network capability provides the ability to move data from one physical location to another. Network capability affects the timeliness of information flow in a system as well as the availability of the information. Some examples of communicating capability include; the Internet (global communicating capability, home area network / local network communication capability).

Network Interface

The network interface capability provides the ability to interface with a communication network. Every IoT component must have at least one network interface capability and may have more than one. Some examples of network interface capability include; Ethernet adapter interface capability, long-term evolution (LTE) radio interface capability, ZigBee radio interface capability.

Processing

The processing capability provides the ability to transform data based on a defined algorithm. The transformation may be very simple, with a single input variable and a single output, or it may be complex very multiple inputs and outputs. Some examples of processing include: data

aggregation capability, proportional-integral- derivative (PID) control capability, and binary (Yes/No) decision making capability.

Sensing

The sensing capability provides the ability to sense an aspect of the physical world. IoT components with sensing capability have typically one or more transducers combined with A/D converters. Information about sensor observations is exposed to other IoT components through the network interface. Examples include: temperature sensor (temperature measurement capability), video camera (video capability), and microphone (audio capability).

Supporting

The supporting capability provides nonfunctional capabilities that support the main capabilities of IoT. Some examples of supporting capability include: encryption capability and authentication capability.

Internet of Things (IoT) / Network of Things (IoT) – Scenarios

1. **GSA SMARTBUILDING**
2. **VA HEALTHCARE – e-ICU**
3. **ARMY SMART FLEET MAINTENANCE**

Scenario #1: GSA Smart Building

The GSA Headquarters Building located at 1800 F Street, NW, DC includes over 750,000 square feet of space, 2/3 of which has been modernized, and incorporates a variety of smart building technologies to help its occupants work comfortably, yet improving energy efficiency, and achieving various sustainability goals as mandated by the government. The various technology components implemented form an integrated automated environment (see diagram below), that help building and facilities managers achieve their goals of occupant satisfaction, energy use intensity, maintenance costs, water usage and CO_2 emissions.

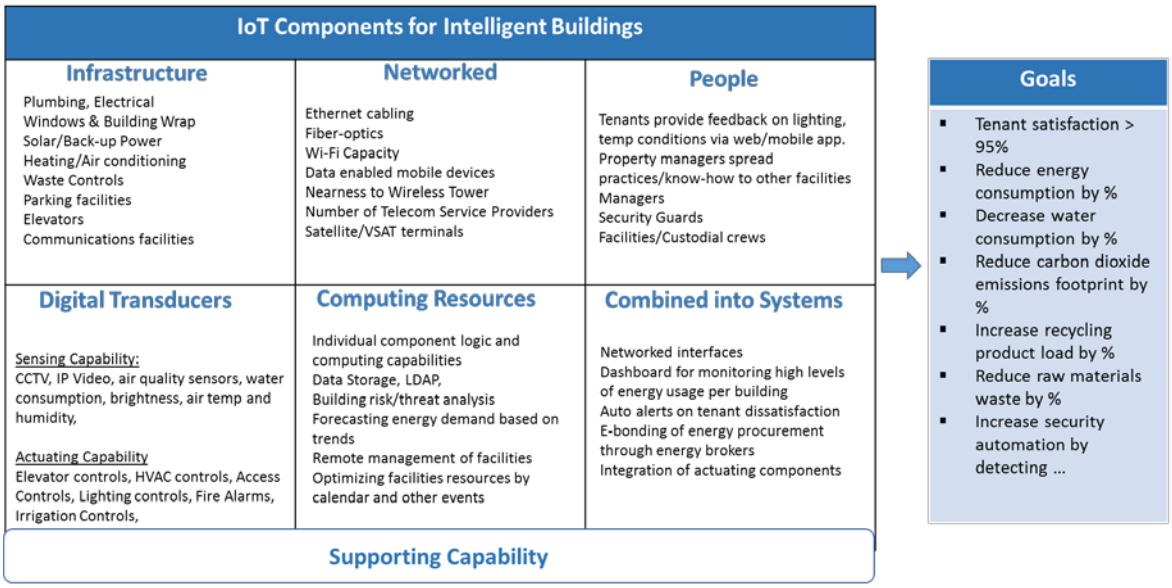
Scenario: - Before GSA staff began arriving Tuesday morning, a Universal Control system reviews its business rules and informs the HVAC system controller that a 20% higher occupancy rate is expected. The system also checks the Hoteling Book-it system to estimate power and ventilation demands of all pre-scheduled meetings. The HVAC system initiates its cooling routines to compensate for the increased demand. As GSA staff and guests arrive, the Card Access & Security System sends data wirelessly to the Universal Control system that verifies that the rate of occupancy is within the projected arrival rate and no additional BTUs are needed.

At around 2pm, a significant cold front moved into the area. The building's Weather Station system, which is tied to the NOAA Internet Weather Service, detects the drop in the outside temperature and feeds

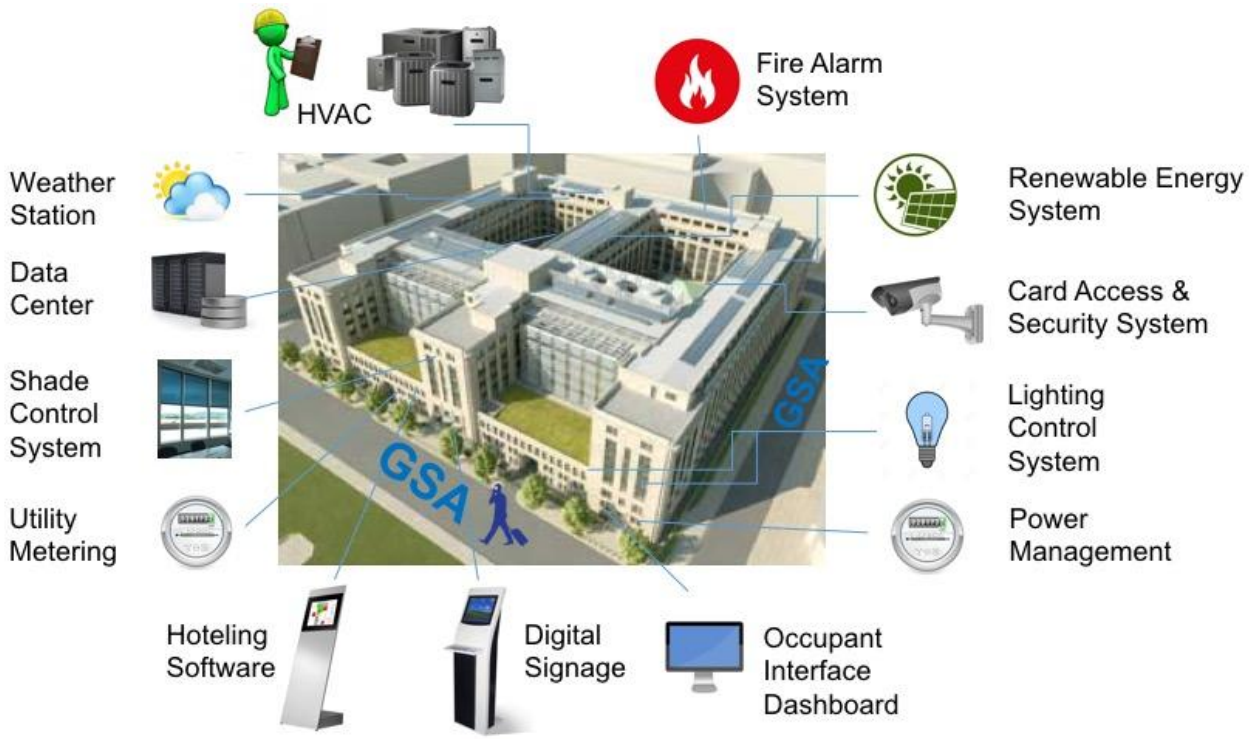
that data to the Occupant Interface Dashboard which controls the Window Switch Report and Shade Control system within each zone floor plan. As the outside cloud cover increases, the window shades are raised automatically and the interior lights are increased by the Lutron Lighting Control System. After a while, several users begin to complain that it is too cold. Individually, they open the building control app and submits their request to lower the temp in their Bay area and increase the lighting. The system receives this feedback and averages the input from other users to make current adjustments, as well as record it for future adjustments.

By now, the meeting in GSA's largest conference room reserved until 3pm, has ended. The Hoteling Book-It system alerts the Universal Control and Monitoring system which verifies that lack of occupants. To conserve energy, the air conditioning is placed into Stand-by state and lights are turned off until the space is occupied again. At the end of the day, the facility manager reviews the energy consumption for the day and checks tomorrow's meeting calendar. The dashboard alerts the manager of a large conference, with over 200 attendees, planned for tomorrow, starting with a 7am breakfast. The manager verifies that AC and ventilation will begin one hour earlier and adjusts the power metering to ensure plug loads are adequate for the A/V equipment and number of devices.

Applying the IoT Framework to Smart Buildings



GSA Smart Building Diagram



Scenario #2: Improved Healthcare: Electronic Intensive Care Unit (e-ICU)

Intensive Care Units (ICUs) in hospitals are a vital component in delivering critical care to their community. ICU patients depend on a complex ecosystem of sophisticated monitoring and control devices and a support team of highly skilled health care practitioners. There are approximately 6,000 ICUs in the U.S that account for more than 10% of all hospital beds and more than seven percent of all National Health expenditures. Almost six million patients are admitted annually to ICUs in the U.S. Rising ICU demand from an aging population, shortage of intensivists (ICU specialists), and the flood of information from specialized equipment are some of the contributing factors to overloaded ICUs and the need for technology to complement, qualified staff.

This IoT healthcare case study examines two e-ICU concept(s):

1. Tele-ICU - centralized or remote critical care service that interacts with patients, bedside ICU teams, and other provides networked through audio and visual communications and various information systems. Hospitals have used different forms of Tele-ICU for more than 20 years. Ten years ago, approximately four percent of adult ICU beds were covered by Tele-ICUs[1]. Tele-ICU staff typically provides support for 100 -300 ICU patients, covering disparate geographical locations or multiple hospitals.

[1] Tele-ICUs: Remote Management in Intensive Care Units, New England Healthcare Institute and others

2. Smart ICU - Integrate independent device components and other medical information systems, store large data sets, and provide predictive data analytics to the ICU team.

Tele-medicine is the underlying technical concept of today's e-ICU. The best example of tele-medicine in Government is the Department of Veterans Affairs' Pacemaker and National Cardiac Device Surveillance Programs [2]. This long-standing program illustrates how various aspects of IoT in health care have evolved over time.

The following table compares the two e-ICU examples from an IoT component definitional framework perspective.

e-ICU – COMPONENT DEFINITION FRAMEWORK

IoT Components Per IOT Component Framework	Tele-ICU Buyers: Academic and Commercial Hospitals, Managed Care Networks. Vendors[3][4] Avizia, Connected for Life™, INDEPENDA, LG CNS, Ideal Life	Smart ICU Vendors/Products: ehCOS by everis health, tIME model[5], eCareManager by Philips, LILAH™ by ConstantCare
Network Interface Capability	Enterprise LAN, Cellular, Bluetooth, high-speed Internet connectivity; video conferencing.	Interoperability for capturing patient data from biomedical equipment, EMR, and other systems.
Data Storing Capability	▪ Monitoring systems have limited storage. ▪ Electronic Medical Record (EMR) / systems contain large data sets--lab results, digital images, nurses and physician IoTes, etc.	Supports high-resolution physiologic data acquisition, archiving, or anIoTation with bedside observations for clinical applications.
Processing Capability	▪ Extensive, real-time sensor data into numeric and graphical waveforms used by bedside and other specialty monitors. ▪ Rules-based conditions/parameters trigger alerts and alarms.	▪ Implementation of predictive models between vital signs and treatments. Detects patterns of practice to assess patient care and treatment. ▪ Single decision support and control panel.
Communicating Capability	▪ One-way and two-way audio/video communications with patient, other hospital/ICU staff, and e-ICU team. ▪ Device specific alarm capabilities based on general thresholds.	Customized, alarms based on patient medical history and clinical event-based decision support algorithms.
Actuating Capability	Multiple, independent actuating components; mechanical ventilators, medication and other pumps, compression devices, controllers, electric switches.	Integration of biomedical equipment from different vendors.
Sensing Capability	Multiple sensors-intravenous, topical, volume or weight sensors attached to patient or on other devices capture and transmit physiological waveform signals.	Similar capabilities

[2] National Cardiac Device Surveillance Program Database, Department of Veterans Affairs

[3] Tele-ICUs: Remote Management in Intensive Care Units, New England Healthcare Institute and others

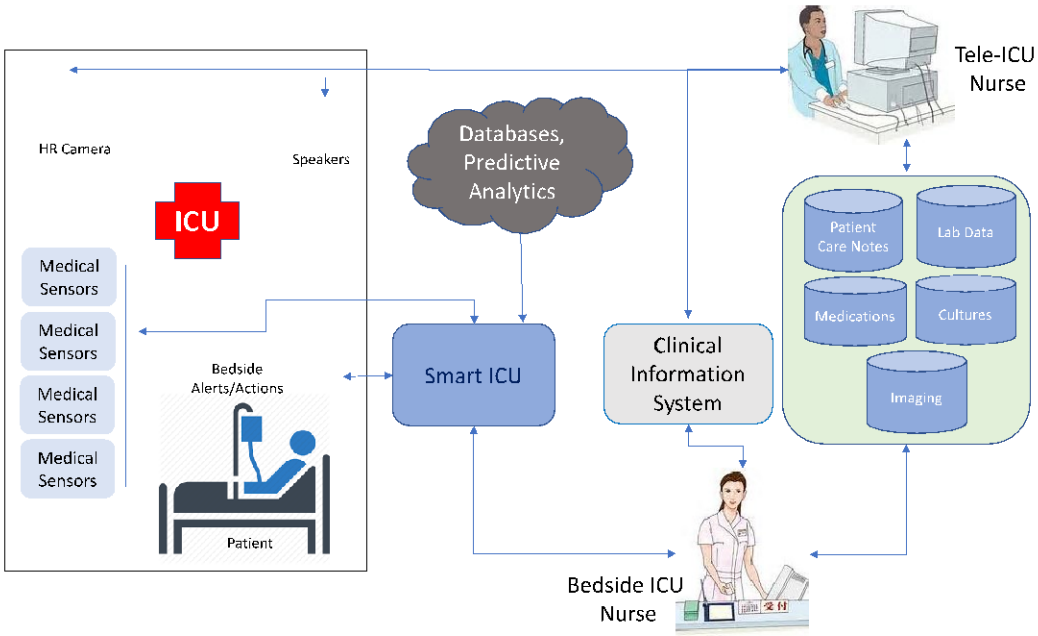
[4] 2016 Telehealth and Remote Patient Monitoring (RPM) Selection Matrix, LeadingAge CAST

[5] Information Technology in Critical Care, Scientific World Journal

Supporting Capability	• Device batteries and electrical back-up facilities • Asset tracking, maintenance and equipment utilization • Enhanced patient and building security • Device security and patient information security	• Measure effectiveness of certain protocols, therapies, or techniques • Peer benchmarking to other clinical data results.

In the diagram example below, the Smart-ICU clinical information system drives the early identification and intervention imperative to treat sepsis. Sepsis accounts for 215,000 deaths and costs $16.7 billion annually in the United States. The clinical information systems utilize comprehensive patient assessment data and use algorithms to continuously assess a patient's acuity and recognize changes in their sepsis status. The system then alerts clinicians if patients develop risk for severe sepsis, promoting earlier intervention which reduces mortality and length of stay in the ICU.[6]

e-ICU Illustration Diagram



[6] Tele-ICU: Delivery on the gold mine of data; Becker's Health I CIO Review, February, 2016.

Scenario #3: Army (DoD) Fleet Management & Maintenance or Data Driven Transportation

Predictive maintenance (PdM) is the servicing of equipment when it is estimated that service is required, within a certain tolerance. PdM is to maximize the value and useful life of assets including transportation railroads, industrial equipment, manufacturing plants, oil and gas processing, etc.

Machine-to-machine (M2M) is defined as the technologies that allow machines to communicate with each other. The Internet of things takes M2M to the next level by including a third element: data.

Preventative Maintenance:	Predictive Maintenance:
• Statistics related • Time/Operation count-based • Performed whether its needs or IoT • Labor-intensive • Ineffective in identifying problems developed between scheduled inspections • IoT cost-effective. • Unreliable and time consuming • Breakdowns or outages are reactive • Technical resource coordination is difficult	• Based on real-time data and correlations • Current situation and hints/failures related • Performed if needed • Performed when the maintenance activity is most cost-effective • Performed before the equipment loses performance within a threshold

More Control, Lower Cost:

To build upon the Asset tracking pilot that was done by TACOM with sensors and a big data platform (hybrid cloud, Transvoyant), he Army would like to explore the capability of adding/activating sensors within vehicles to provide data, performance metrics to drive predictive maintenance and "call-ahead" capability for parts and resources. Phase one would be for the base and Depot levels. Phase 2 would be a secure version for in Theater.

Mission Critical – Readiness: Rather than performing routine calendar-based inspections and component replacement, predictive techniques monitor equipment for pending failures and IoTify you when a part replacement is required. Sensors embedded in equipment check for abnormal conditions and trigger work orders when safe operating limits are breached.

Benefits: When a predictive maintenance strategy is working effectively, maintenance is only performed on machines when it is required. This reduces the parts and labor costs associated with replacements.

Real-Time Data Analysis (including historical): The availability of all machine data in one virtual network gives original equipment manufacturers (OEMs) the ability to aggregate and analyze the data to generate better predictive analytic models.

Benefits: Rather than waiting for a system to fail, manufacturers can accurately predict failure because sensors start reporting back when operating conditions trend out of specification. By accurately mapping user behavior, identifying failure patterns and quickly recognizing recurring issues, OEMs will be able to design out failures, improve their product and guarantee uptime/Asset Utilization/Life

Better Metrics: Availability, reliability and other key performance metrics such as mean time between failures (MTBF) and mean time to repair (MTTR) can be calculated automatically by the system and fed

to reporting dashboards. This removes the human element in capturing all downtime, ensuring the data is as accurate as possible. In addition, reliability metrics from different sites can be analyzed to identify best practice for implementation around the world.

When equipment goes down, failure data from various sources can be gathered, aggregated and analyzed in real time within the cloud. Repair options can be taken automatically by the system, and actions can be recommended to the technician if necessary. All possible failure data will be used to direct the repair, including system operating conditions at the time of failure, previous repair data from the computerized maintenance management system (CMMS), wear patterns and operating data from the equipment fleet. In effect, the technician will be presented with the aggregate of a universe of data providing all the information needed for more effective decision-making and the fastest route to resolution.

Tighter parts & Inventory Control: Effective inventory control can have a significant impact on limiting equipment downtime and controlling maintenance budgets. Connected stockrooms that proactively monitor inventory movements and stock on hand to ensure the site is only holding what is needed will become commonplace in facilities everywhere. Through predictive maintenance and data analysis, OEMs/suppliers will be able to optimize the recommended spare parts lists, freeing up much needed capital and improving performance.

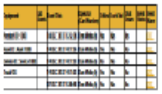
Benefits: The right parts, where they are needed, when they are required. Additional benefit of freeing up space and weight within a vehicle/asset

Vehicle tracking & Asset management- the IoT is particularly valuable for the predictive maintenance of geographically dispersed assets.

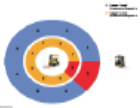
The true value of the Internet of things can only be fully realized when you take a holistic view of asset management. Powerful virtual cloud networks continually collect, aggregate, and model data to accurately predict failures and put contingencies in place to limit their impact on system availability. The IOT will become fundamental in improving asset reliability and driving cost takeout by delivering real-time, intelligent and actionable data to connected systems or the end user.

MAJOR COMPONENTS OF FLEET MANAGEMENT

Operational Fleet Monitoring and Management
Real-time equipment tracking, KPI management per truck, fleet and location



Equipment dispatching
Assigning equipment to customers



Technician scheduling
Location, skill requirement, shift of work based crew scheduling

Asset tracking
Linked to overall fleet management, allows the tracking of all goods and physical items allocated to fleet operations

Condition based, predictive maintenance
Remotely view and manage equipment servicing

Security and safety
Equipment and driver security during operation or while stopped, recovery of stolen vehicles

IoT & PREDICTIVE ANALYTICS

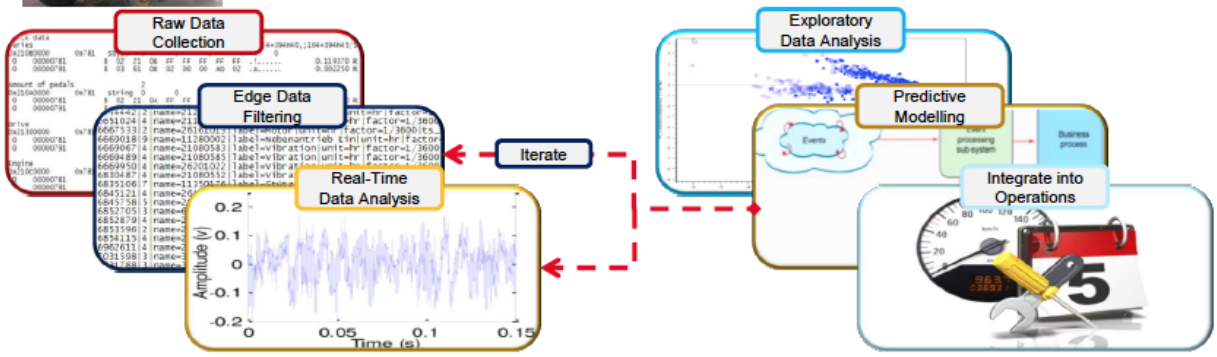
Signal Analysis

Event Analysis

Root Cause Analysis
Sensor value distribution analysis
Linear regression …

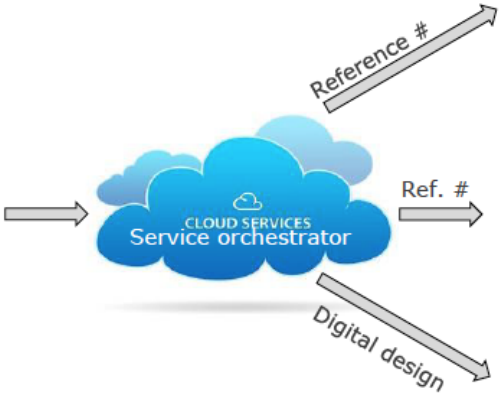
Event Tracking & Filtering
Event Correlation
Event Aggregations …

PREDICTIVE ENGINE



INTELLIGENT SPARE PARTS

Predictive Maintenance
Self diagnostics identify failing components resulting in automated parts ordering



Spare parts supplier

OEM Manufacturer

3D printing factory

Embedded sensors
Real time, condition based monitoring
Part identification and direct ordering
Classical or additive manufacturing

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Mobile Backend as a Service (MBaaS)

Working Group Document

MBaaS General Definition

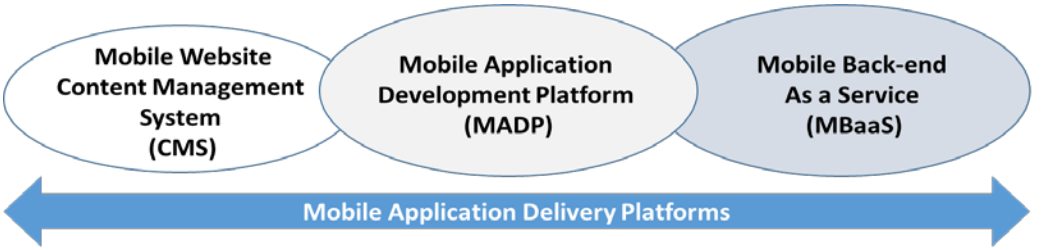
MBaaS is an emerging technical capability that provides mobile app developers with a way to connect applications to backend cloud storage and processing, while also providing common features such as user management, push notifications, social networking integration, and other features that mobile users demand from their apps. MBaaS, has a lot of the same intent as PaaS, to speed up the application development process, however MBaaS is purely a backend, providing an infrastructure that automatically scales and optimizes, bundled with a set of essential resources developers require, like content, data, messaging tools and all the best 3rd party, API driven services they are used to like Facebook, Twitter and Dropbox.

MBaaS Technical Definition

An MBaaS (Mobile Backend-as-a-Service) is the primary point of contact for end user applications for both mobile and web. The MBaaS hosts Node.js applications as REST API servers and/or Express.js based web apps. The primary purpose of the MBaaS is to allow users (developers) to deploy Node.js server side for their mobile apps. The MBaaS also provides functionality such as caching, persistence, data synchronization and a range of other mobile centric functionality for mobile app developers. Multiple MBaaS may be utilized for client segregation and/or lifecycle management (environments).

Mobile Application Delivery Platforms

MBaaS is part of a broader set of technology solutions that enable the delivery of mobile applications. The three major mobile delivery platforms in the marketplace today are Content Management Systems (CMS), Mobile Application Development Platforms (MDAPs), and Mobile Back-end-as-a-Service (MBaaS). MBaaS is the newer category and represents an emerging set of technologies that interface and support other mobile delivery systems. The diagram below represents the three major types of mobile delivery platforms and their associated uses and benefits.



- Supports creation/delivery of Tier 1-type* mobile applications;
  - Delivers information to mobile devices
  - Same system for delivering website and mobile content
  - Efficient means for repurposing content
  - Works with search engines to drive awareness and traffic
- Requires less technical skills
- Significantly cheaper than building a native app
- Less engaging user experience

- Supports creation/delivery of Tier 2-type* mobile applications, allowing;
  - Development of native apps for iOS and Android devices
  - Apps with faster performance, greater convenience, and "stickiness" with users
  - Support of personalization and location-based services
  - Delivery of contextually-relevant information
- Requires significant technical skills and investment
- Moderate – High security posture
- Works together with MDM/MAM solutions

- Supports creation/delivery of Tier 3-type* mobile applications;
  - Facilitates building and maintaining complex native apps.
  - Provides toolkits and libraries to speed development.
  - Offers pre-built APIs for faster integration with external resources
  - Resources can scale quickly and easily for high-demand situations
- Lowers CAPEX
- Works together with an MADP/CMS to provide back-end infrastructure and services

* *Tier 1, 2, and 3 type mobile applications defined by ATARC MBaaS Working Group Members*

MBaaS Features

The following is a high-level set of features of an MBaaS platform:

MBaaS Features		
Features	**Sub-Features**	
User Management	User Listing User Property Management Enable/Disable Users Create New Users Social Logins Session Control	Multiple Logins Password Reset Relationships Data Validation Export/Import User Data
Data Management	Graphical Data Browser Complete Object Persistence Solution Rest Console Cross Platform APIs Relational Data	Built-in Paging Support Complex object hierarchy Schema management Data security Data to geo relationship
Geolocation	Geo metadata Location data Search in radius SQL driven search Security / Permissions Geo clustering	Client Code/App Generation Geopoint to data object relations Interactive geofencing design Geofencing manager Geofencing events and actions Geofencing monitor
Media Streaming	Cross platform streaming Ready to use media Publish live from iOS / Android Create video on demand	Powerful stream management Play video everywhere Instant on-demand media deployment Client code app generation
Publish/Subscribe Messaging	Cross platform message delivery Powerful data broadcast Conditional subscriptions Push vs Pull	Games Online message publishing Instant mobile chat Customizable business logic
Push Notification	Send notifications from server Cross platform push Scheduled notifications Badges, popups, sounds Group broadcast	Target specific users Customized business logic Online message publishing Device management
Custom Business Logic	Event handler API customization Timers	Server code debugging Integrated logging Manage custom code in production
Analytics	API filtering API consumption by client type Error analysis	Hosted services analytics New vs Returning users Rich media analytics
Mobile Code Generation	Multiple client types Generate starter code Registration / Login Data management code	Chat apps Geo browser Video broadcaster / player File management apps

Mobile Applications Tiers

Mobile applications can be categorized into three tiers:

- Tier I – Static Content, simpler design, display functionality.
- Tier II – Static & Dynamic content.
- Tier III – Comprehensive MBaaS Solution – push, geo-location, storage, security, etc.

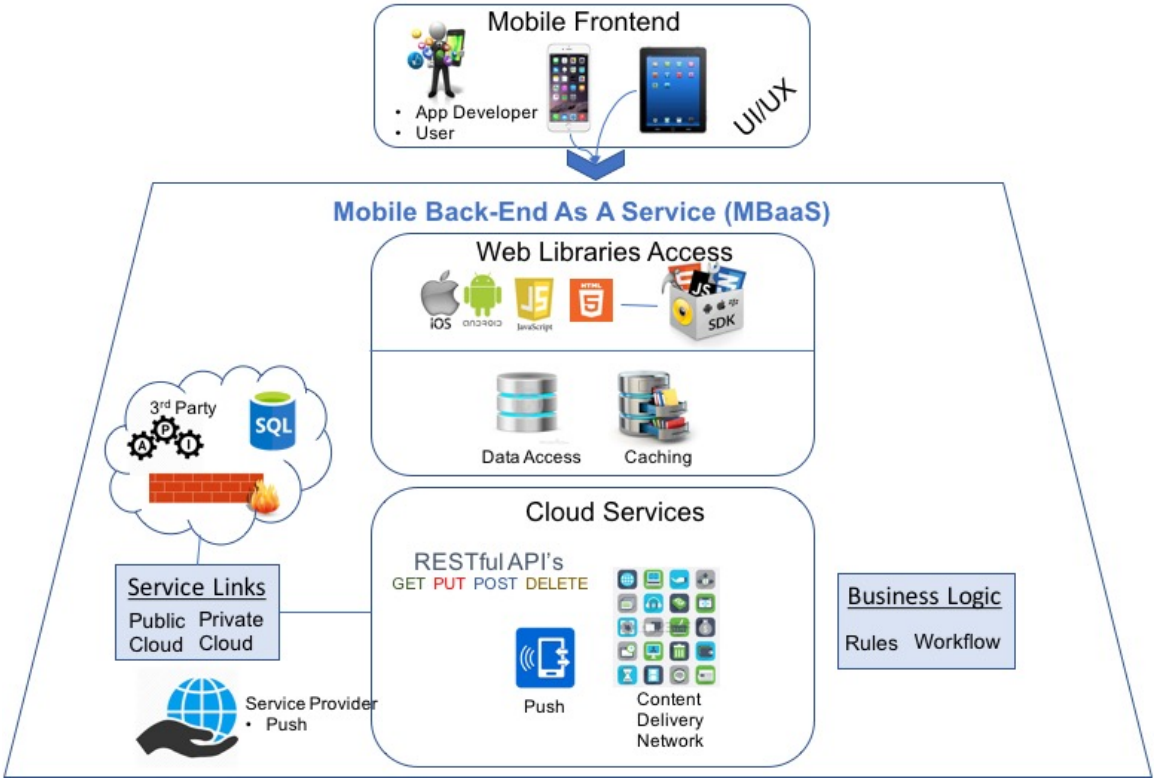
Tier 1 Mobile Applications – Static Content

Description:
This type of mobile application retrieves and displays static content which is formatted to fit the navigational scheme and form factor of mobile devices, including tablets. A Tier 1 mobile application typically involves a user launching a web browser via their mobile device and accessing a resource (website) that contains static content or hyperlinks to other resources/websites. Information is pushed to the end-user via a web server(s). The Tier 1 app may interact with an external website (extranet), a closed environment (intranet), or some combination of the two.

Examples:
In the government space, a secured, agency intranet site(s) or agency external-facing website (i.e. www.omb.gov).

Backend Components Accessed:
Technologies that support the development and delivery of Tier 1 applications include mobile Web Content Management systems with Mobile Content Management capabilities, Mobile Application Development software, and an MBaaS solution used in conjunction with a mobile frontend UI/UX. The following diagram depicts a Tier I Mobile Application MBaaS architecture.

TIER I – MBaaS Architectural Diagram



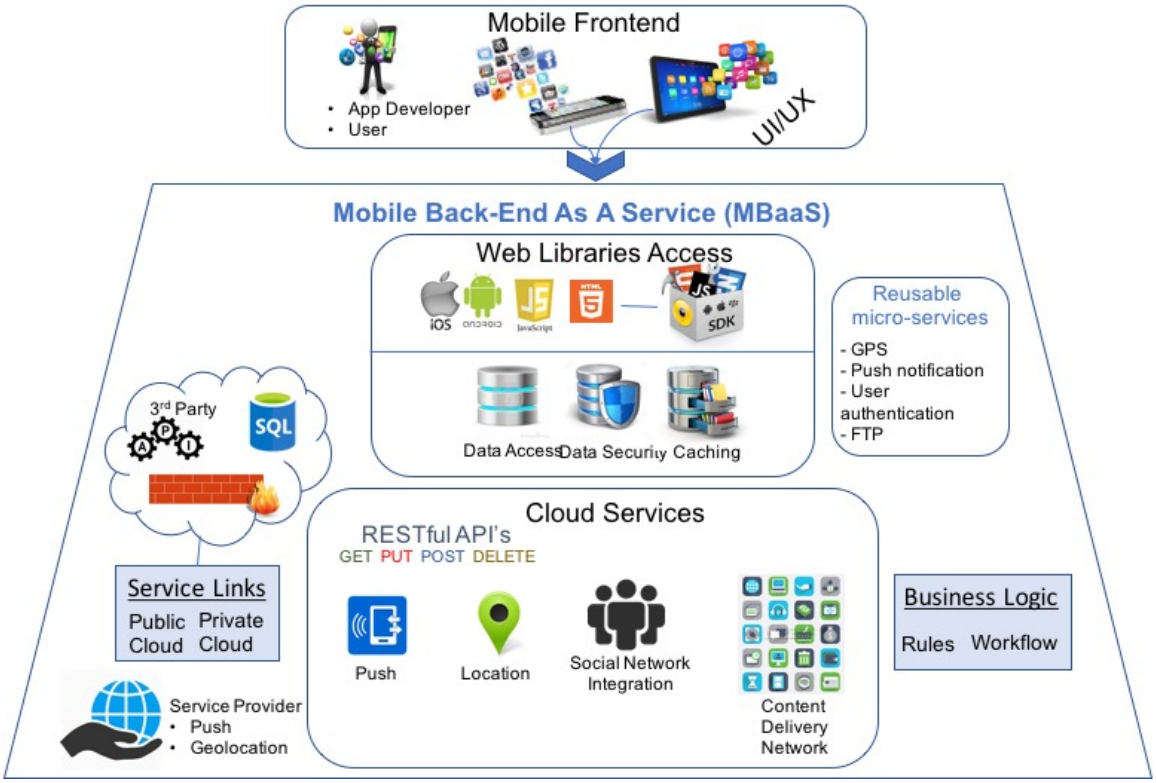
Tier II Mobile Applications – Static & Dynamic Content

Description:
This type of mobile application retrieves and displays a combination of static and dynamic content formatted to fit the navigational scheme, OS(s), and form factors of various mobile devices. Tier II mobile applications requires orchestration of a variety of information sources to provide an enriched user experience. The Tier II application may be initiated through a commercial web browser or the native mobile device browser. Specific data elements may be tagged, rated, searched, and retrieved in context. Data access/retrieval is performed as an independent function. Information may be pushed or pulled to the end-user or to external databases depending on the requirements. Tier II mobile apps may interact with external websites (extranet), intranets, or invoke web services to enable communications among various applications.

Examples:
This type of application is used to access financial data from one source, general news from another source, passes your browsing history data to an advertising-server that displays from previously visited sites, and provides geo-located GPS data. In the commercial space, an electronics sales distributor may deploy a mobile app for its salesforce that optimizes pricing for hundreds of thousands of products by compiling, aggregating and structuring competitor pricing data in real-time. A government data analyst may require a mobile app that keeps up to date on new sanctions and regulations at international, federal and state levels to ensure compliance with terrorist financing.

Backend Components Accessed:
Technologies that support the development and delivery of Tier II mobile applications include Content Management Systems with Content Integration capabilities, Mobile Application Development software, and an MBaaS solutions used in conjunction with frontend UI/UX software. Diagram below depicts a Tier II Mobile Application MBaaS architecture

TIER II – MBaaS Architectural Diagram



Tier III Mobile Applications – Comprehensive MBaaS Solution

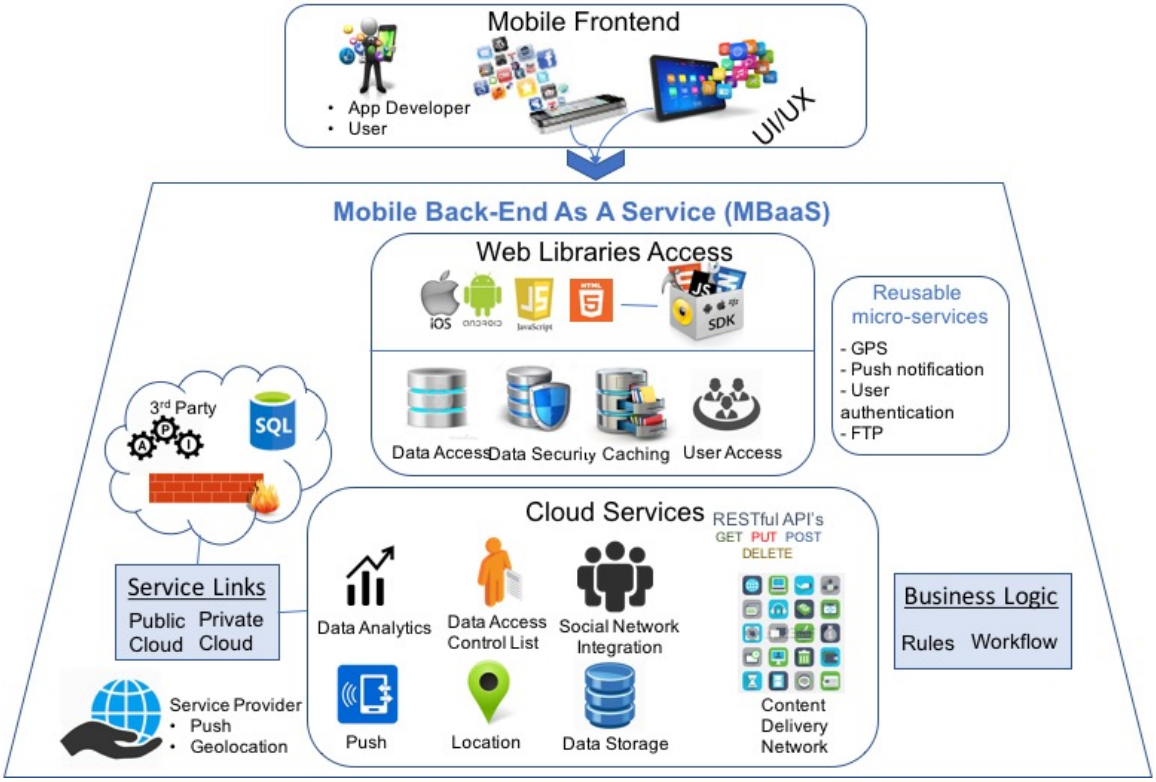
Description:
These mobile applications are more sophisticated with integrated and related functions, that are complex to develop, maintain, and deploy. They share many of the technical functional characteristics of Tier II applications, but often integrate mission-critical information sources. The nature of Tier III mobile applications often require specialized work-flows and inter-dependent functions between data sources and business rules. Tier III mobile applications may be programmed to automatically activate/control other activities or processes. They are often used in advanced intel operations or sophisticated decision-making situations. Security requirements are of highest concern.

Example:
A USDA field inspector, using an app on his tablet, confirms his assignments for the day which cover a 100-mile radius over three counties. The app tracks his route and findings at each facility visited, along with his location, using the device GPS. The app is tied to a weather forecasting

site that predicts dangerous weather at the time of his third visit. The app sends an alert to the tablet looking up an alternative USDA field office nearest his current location. The app launches WAZE commercial site and presents the fastest route to the USDA field office nearest him. In addition, the app presents alternative USPS offices that are open and closer. The consumer example would be the UBER driving service.

Backend Components Accessed:
A Tier III mobile application will access a full suite of backend integrated services including data access, security, user management/control, analytics, social networking, geo-location, storage, push services, business logic, and cloud services. The diagram below highlights the comprehensive MBaaS architecture needed to support a Tier III mobile application.

TIER III – MBaaS Architectural Diagram



Open source MBaaS Architecture

An open source MBaaS Architecture should include -the following services, which are deployed during product installation on an open source PaaS:

- mbaas: management of configuration of MBaaS
- messaging: analytics messages interface, recording of raw data
- metrics : generate stats and aggregations recorded through messaging
- statsd: store stats in memory
- mongodb: storage with 3 replicas recommended
- nagios: events monitoring
- redis: caching

- docker containers: for management and app hosting
- kubernetes pods: orchestration of containers

To estimate the infrastructure configuration there are several variables to be considered, for example, the number of apps, number of app users, functionality in the apps, the number of services, and the number of transactions to/from devices and to/from backend integrations.

An Open source MBaaS can be deployed as a series of containers and pods on a dedicated PaaS.

The initial recommended deployment includes one MBaaS, however, two or more MBaaS will ensure network separation from other VMs (containers and pods) running on application nodes. For example, if the enterprise decides to have the development environment on a different data center.

Multiple environments such as Development, Testing, Pre-production and Production are defined in these MBaaS. Default configuration can have all these environments in a single MBaaS or separate MBaaS.

Open Source MBaaS overall architecture includes:

- Master Nodes
  - Minimum 2 VMs to assure resiliency and at least one VM always operating PaaS. In this definition etcd hosts are included in the VMs for master nodes.
- Infrastructure Nodes
  - Routers and docker registry separated from services in the master
- MBaaS Infrastructure
  - MBaaS components including: mbaas, messaging, metrics, statsd and Nagios and MongoDB replica sets (minimum 3)
- Cloud Application Nodes
  - For your mobile app cloud code and MBaaS services. Depending on the subscription level (SKU) these nodes can be deployed in shared or separate VMs.

Connectivity

In order to allow MBaaS connectivity with MAP, and for apps deployed on mobile devices to communicate with the MBaaS, a permanent connection to the public Internet is required either directly or via an accessible web proxy. The following outbound access is required:

- TCP/80 (HTTP) / TCP/443 (HTTPS)

To support communication with apps deployed on mobile devices, the MBaaS requires a dedicated IP address used in the PaaS router. Depending on the type of mobile devices used and the nature of their connectivity, a public IP address may be required (e.g. for telephony devices using a Public APN) whereas other configurations may only require a private IP address (e.g. Private APN or Internal WiFi). MAP sends a small volume of email (e.g. user registration,

password reset, monitoring). For on premises installations, a locally accessible mail server/relay operated by the customer is required.

Challenges

Although MBaaS offerings provide developers with increased efficiencies and ease of use, they are not perfect. There are challenges to consider while evaluating whether an MBaaS meets your needs. Some of those hurdles include:

- **Security:** Companies often perceive that data kept or accessed on the cloud will never be as secure as when it is stored on premise or behind their firewall. This manifests into a reluctance to allow outside vendors to either store or access their data in the cloud. There are security considerations to keep in mind while deploying MBaaS solutions:
    - Control and secure how apps connect to the enterprise – Best Practice
    - Do not directly expose your enterprise systems
    - PKI/Derived Credentials
    - Integrate with Active Directory and other Identity Management systems
    - Add keys, token, encryption to your mobile apps, no restrictions or extra charges
    - Secured development environments (dev, test, pre-production, live)
    - VPN connectivity
    - MTD/App Vetting
    - NAIOP/NIST Change responsiveness
- **Performance:** Latency and performance issues are sometimes a concern when an app accesses data, security, push messaging, and offline capabilities from the cloud. If latency is a concern then an on premise capability may be a better way to go.
- **Mobile Network Communications**: By performing data retrieval and business logic and computation in the cloud through MBaaS, you are making yourself susceptible to carrier network availability and performance.
- **Enterprise Integration:** While most MBaaS provides claim to integrate to any backend system, however this is not always true. A good MBaaS provider should be able to use all customizations, not have to replicate data or use a middleware.

Benefits of an MBaaS

Some of the advantages of deploying an MBaaS solution include the following:

- Faster deployment of front end applications
- Ease of Use – MBaaS platforms offer self-service interfaces, which are easy to use, and get off the ground.
- More time to focus on the frontend user interface.
- Flexibility: - With RESTful API's MBaaS offers an open stack platform for developers who are not restricted to one set of tools for designing, engineering, and managing apps. This lets the developer choose a backend solution independent of the design tools, libraries, studios, and toolsets to build the frontend.

MBaaS Sources of Supply

Given that MBaaS is an emerging sector, there are a limited set of vendors that truly qualify as MBaaS vendors. There are many vendors that have emerged from Platform-as-a-Service (PaaS) and Backend-as-a-Service (BaaS) spaces. The intent of this vendor list is to arm federal agencies with some basic knowledge on MBaaS vendors to get started with. Further evaluation is needed to evaluate individual needs.

The following is a list of sources of supply to consider while selecting an MBaaS vendor:

MBaaS – Sources of Supply		
Sources of Supply	**Platform**	**Product**
Amazon Web Services	AWS Mobile Services	• Amazon Cognito, Amazon Mobile Analytics, AWS Device Farm, AWS Mobile Hub, AWS Mobile SDK • Comprehensive solution. • Best fit for companies willing to support mobile initiatives with a set of services, instead of a single, managed product.
AnyPresence	AnyPresence Enterprise Platform	• New entrant. • Suited for customers that need flexibility in deployment.
IBM	IBM MobileFirst Platform Foundation v.8.0	• IBM Bluemix • Best fit for customers that focus on data integration, especially complex integration scenarios.
Kinvey	Kinvey Platform	• Easy for customer that focus on using the platform and not managing it.
Microsoft	Comprised of product set	• Azure App Service, CodePush, HockeyApp, Intune, PowerApps, Visual Studio 2015, Visual Studio Code, Visual Studio Team Services, Xamarin Studio, Xamarin Test Cloud. • Focused more on front-end. • Well suited for existing Microsoft customers.
Oracle	Oracle Mobile Cloud Service v.2.0	• Oracle Developer Cloud Service, Oracle JavaScript Extension Toolkit, Oracle Mobile Application Accelerator, Oracle Mobile Application Framework
Red Hat	Red Hat Mobile Application Platform	• Open Source Focused - Red Hat enterprise linux, Openshift, NPM community, Raincatcher, Feed Henry open source, 3Scale, BPMS
Salesforce	App Cloud	• Force.com, Heroku Enterprise, Lightning, Mobile SDK, Salesforce1

SAP	SAP Mobile Platform 3.0 SP11	• SAP Hana Cloud Platform, mobile service; SAP Web IDE
Telerik	Telerik Platform	• Offers a full suite of web content management, MADP, and MBaaS solutions at various subscription rates. No on-premise solution available (analytics only).

MADP

Mobile Application Development Platforms – Sources of Supply		
Sources of Supply	**Platform**	**Product**
Appcelerator	Appcelerator Platform	• Best fit for customers that need to build cross-platform solutions.
Kony	Kony Mobility Platform	• Front-end tool (Visualizer) and back-end (MobileFabric). • Best fit for customers that need mobile support in multiple areas of their SDLC's.
OutSystems	OutSystems Platform	• Platform for developing mobile apps and integrating them with Cloud-based providers Azure, SAP, AWS.

Mobile Services Category Team (MSCT)
Advanced Technology Academic Research Center (ATARC)

Telecom Expense Management (TEMS)

Working Group Document

1 Introduction

1.1 Background

The federal government is becoming increasingly reliant upon mobility, now with approximately 1.5 million mobile devices in service costing the government over $1 billion annually for service alone. Mobility usage across the government has a wide range of diverse profiles from general business use to mission critical, high security. There is an increasing need for the federal government's mobile device management processes to be further improved due to increased security risks and broader use of mobile solutions.

The Category Management Leadership Council (CMLC) and the Office of Management and Budget (OMB) established and began the implementation of a Category Management strategy across the federal government identifying 19 Common Government Spending Categories. In 2016, OMB established the Mobile Services Category Team (MSCT), made up of Agency representatives across the federal government, to address cross-government requirements for next generation mobility. The MSCT is tasked with, among other responsibilities, establishing requirements for both core and sub-components of mobility. As such, it is the responsibility of the MSCT to establish the minimum baseline Enterprise Mobility Management requirements.

The primary purpose of this document is:

- State the minimum set of requirements across the federal government for Telecom Expense Management (TEMS) and Lifecycle Management of mobile devices.

This document establishes minimum TEMS requirements government-wide. Individual agencies determine the full extent of requirements for their respective telecom expense management, security needs, and mobility software. Within this context, it is also important for the federal government to continue to reduce costs and both improve and simplify the acquisition process for mobility and related services.

This functional technical requirements document includes requirements from the previous Managed Mobility TEMS RFTC solicitation in 2012, requirements obtained from a National Science Foundation Statement of Work (SOW) which had been based on that 2012 TEMS RFTC solicitation, and ongoing inputs from the inter-agency TEMS MSCT working group.

The TEMS solutions must meet a broad set of requirements that address the following set of criteria:

A. Qualified, Secure, Scalable Solutions – Technical solutions that address the existing mobile device, application, and content management needs of government mobile technology including minimum level security and policy management. The solutions shall have the ability to scale to the extremely large and evolving nature of federal government cabinet-level agency organizations.

B. Evolutionary and Flexible – The mobility management needs of the federal government are evolving with increased mobile adoption, new mobile applications, enhanced needs for remote access, and emerging policy and security requirements in an increasingly threatening external environment. As a result, the solutions will continue to assess future requirements to ensure the ongoing federal government needs of Telecom Expense Management are adequately met. The MSCT intends to re-assess both the TEMS requirements and solution providers on a periodic basis in response to mobility evolution. This will provide government agencies with on-going, updated qualified solution providers.

C. Shared Mobility Community – Solution providers are expected to monitor and bring forth new industry developments, identify Managed Mobility best practices in both industry and government, and to present these best practices to government. The Managed Mobility space is in a state of rapid change, making it challenging and resource-intensive for agencies to stay properly informed and to adequately maintain and manage mobility within their respective agencies.

By centralizing requirements gathering, establishing government-wide minimal requirements, and conducting solution assessments; the MSCT intends to reduce the burden on agencies while increasing the quality of their options.

1.2 Objective

The federal government must address agency's mission needs in a secure, cost-effective manner. This objective is driven by the MSCT as directed by The Office of Management and Budget (OMB). Telecom Expense Management Services (TEMS) is a core capability for effectively scaling the deployment and management of mobile devices, inventory management, reporting functionality, invoicing, and savings. Controlled device deployment, management, tracking, rate plan optimization, and reporting will lead to cost reductions over time.

1.3 Solution Requirements

1.4 Baseline TEMS Requirements

Figure 1 below summarizes the vendor-provided TEMS capability, which may be integrated with existing agency systems on an as-needed basis, and which shall be compliant with all relevant agency and government-wide policies.

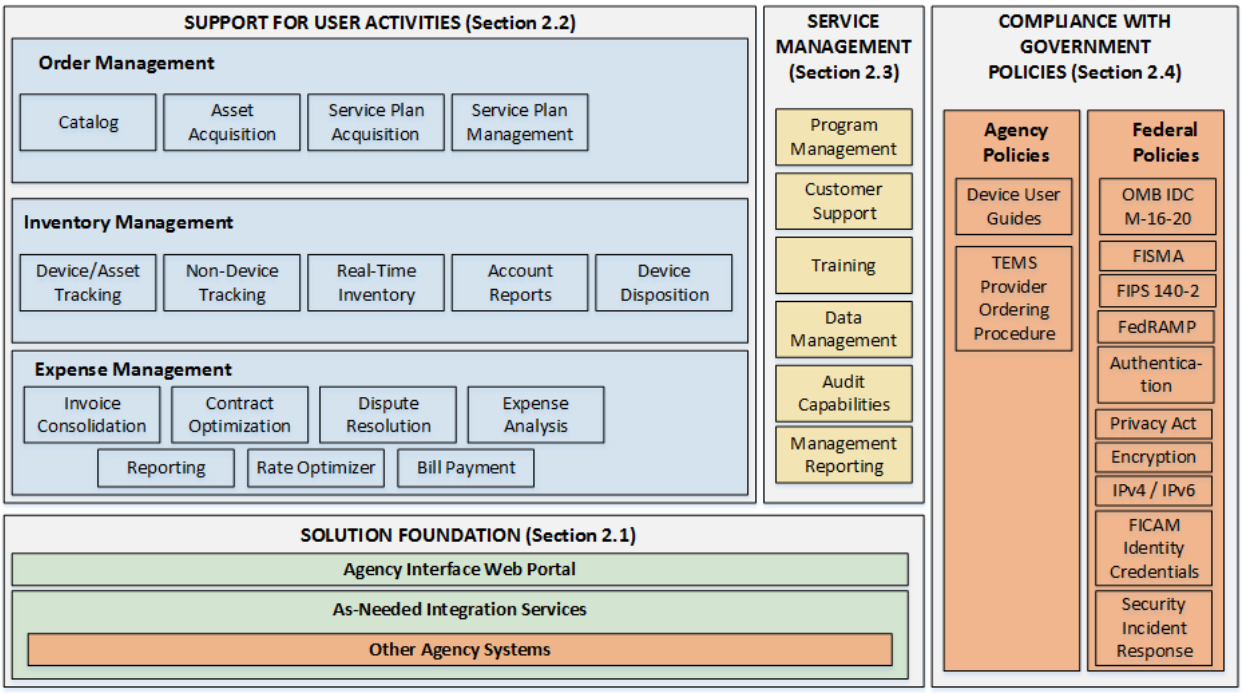


Figure 1: Integrated Vendor-Provided TEMS Solution

The Vendor-provided TEMS solution incorporates the following solution blocks which are outlined in more detail within this functional specification:

- Solution Foundation
  - Agency Interface Web Portal
  - As-Needed Integration Services
- Support for User Activities
  - Order Management
  - Inventory Management
  - Expense Management
  - Documentation Management
- Management Services
  - Program Management
  - Customer Support
  - Training
  - Data Management
  - Audit Capabilities
  - Management Reporting

- Compliance with Government Policies
    - Agency Policies
    - Government-Wide Federal Policies

2 Solution Foundation

2.1.1.1 Agency Interface Web Portal

A web-portal is an access point between the agency and the Mobile Lifecycle & Expense Management provider, that allows for management functionality after an initial inventory is conducted. This web-portal must be defined and secure, and be capable of accessing connectivity with the carriers. The portal may be hosted within the government IT environment, within the Contractor-provided IT environment, within a FedRAMP-approved cloud provider, or a combination at the discretion of the ordering Agency. The Vendor-provided web portal shall be accessible using current industry-standard web browsers (e.g. Explorer, Chrome, Firefox, Safari)

The Vendor shall be responsible for development, testing, reporting, implementation, maintenance, troubleshooting, and hosting of the secure web portal; and ensure that the portal is and remains Section 508 compliant and Federal Information Processing Standards (FIPS) 140-2 certified at the portal and/or Secure Socket Layer (SSL) as required.

The Vendor's IT WTEMS system and secure web-portal shall undergo an initial and periodic IT Security Review(s); and the Vendor shall document and address any defects, deficiencies, or vulnerabilities identified by the government, or when known or discovered by the Vendor; and ensure the system meets all federal requirements (e.g., FIPS 140-2 certified encryption where encryption is used). The Vendor's web-portal shall remain secure, accurate, available, and accessible to designated government and Vendor personnel, in real-time, to:

- Access Agency TEMS user data, as necessary, and to monitor and manage the Agency's wireless enterprise. Access will be supported from multiple types of devices, including desktop / laptop PC's, and miscellaneous mobile devices (e.g. tablets, and cell phones)
- Define, assign, and view user roles on the system
- Verify and manage functionality after the initial inventory of TEMS data
- Serve as the master inventory data base
- Provide consolidated-centrally managed access to all Agency TEMS data
- Serve as the single/comprehensive ordering and reporting portal for use by Agency customers
- Provide current, detailed instructions and allow all wireless transactions to be executed within the portal environment including (but not limited to) device and service requests, look-up provider plan(s) and devices, order creation, tracking and cancellations, account requests and management approvals
- Provide current, detailed instructions on and allow the initiation of moves, additions, changes, and disconnects (MACD) associated with agency wireless assets
- Provide current, detailed instructions and allow designated users to modify, configure, and customize data to meet agency requirements; ensures governance / policy compliance of approved devices and plans,. Maintains both role segmentation and agency maintained security policies, device assignments, and specifications
- Allow for the assignment of permissions that enable authorized staff to receive requests for devices, services and accessories, make approvals and forward approved request to vendor for appropriate action

- Provide tools and processes to deliver spend/savings analysis and optimizations beyond what is provided by the wireless carriers, and optimizes cost savings across carriers.
- Provide reports on actions taken by the TEMS vendor to deliver cost savings to the Government, and recommendations provided to the Government for additional actions to obtain savings and service optimizations.
- Permit the Government to assign and manage tiered accounts (e.g. administrator accounts with all privileges or user accounts with different access (read/write) to various portions of the TEMS functionality

Federal agencies are encouraged to have the Vendor provide the following to ensure the portal meets agency needs:

- A description of how the Vendor will provide a consolidated, centrally managed web portal with access to all data, and use of this portal by federal customers.
- A description of how the portal will allow all wireless transactions to be executed within the portal environment including device and service requests, provider plan and device look-up, order tracking, account requests and management approvals.
- A description of how the portal will allow for any moves, additions, changes, and disconnects (MACD) associated with both wireless assets, how it can be modified, configured and customized to meet agency requirements, and how access will be allowed based on system user roles
- Ease of configurability to meet day-to-day user needs, including:
    - How the solution's application interface can be configured to meet the requirements of different users in the organization
    - How the solution can restrict user access to system data and functions
    - How reporting capabilities can be configured to meet user requirements
    - How the application can be configured to support fixed and mobile procurement policies
    - How the solution can support configurable mobility management workflows
    - How other business process workflows (e.g. Human Resources, Finance) can be configured to meet user requirements if needed to support Agency business processes
    - How the web-based portal addresses workflow to allow assignment of permissions that enable authorized staff to receive requests for devices, services and accessories, make approvals and forward approved request to vendor for appropriate action.

The portal shall be Section 508 compliant and Federal Information Processing Standards (FIPS) 140-2 certified. FIPS 140-2 compliance may not be required for the portal itself, but the Secure Socket Layer (SSL) will require FIPS 140-2 certification.

2.1.1.2 As-Needed Integration Services

As determined by each Agency to meet unique requirements, the Vendor will integrate the Vendor-provided web portal with all necessary Agency IT systems in order to provide effective and comprehensive TEMS service. As part of the integration services, the Vendor must address:

- How the Vendor's web portal shall be capable of being a system of record for the Agency's telecommunication service, device and license inventory, with integrated ordering and inventory modules.
- How the Vendor master inventory and asset database will integrate with all Agency databases
- How the Vendor management, ordering and billing/financial portals will integrate with relevant Agency databases
- How Agency data will be kept consistent with Vendor databases through automated processes
- How the Vendor TEMS service will be integrated with other mobility management services (e.g. MDM, wireline voice, wireline data)
- Some examples of the types of data flow are:
    - New completed orders will create inventory and needs to flow to the asset management system
    - Charges and payments need to be updated in both the asset management and financial systems
    - Budgeting and purchase order information needs to be set up in the financial system, provided to the TEMS capability to be used in ordering and spend reporting
    - Real time notifications need to flow to users of both systems

Agencies may also require that the TEMS solution be integrated with Mobile Device Management (MDM) solutions & Mobile Application Stores (MAS). When MDM/MAS integration is needed by Agencies, the Vendor must show how the system will meet all business rationale for each level of integration and the resulting high level definition of the data to be exchanged between systems, provide the ability to use the portal as a means to exchange data with MDM and MAS systems, and set the standard and utilize this same specification across MDM and MAS systems.

- The portal shall ensure that move, add, change and disconnect information is entered once into the web portal and the information is forwarded to the MDM and MAS systems.
- The Vendor's web portal shall maintain both role segmentation and agency maintained security policies, device assignments, and specifications.
- The Vendor's system shall demonstrate web portal's role-based ordering ensures governance / policy compliance of approved devices, plans, and MDM/MAS environments.

3 Support for User Activities

3.1.1.1 Order Management

The solution shall provide ordering and procurement services through its portal solution. Ordering and procurement services shall include the ability to provide order status, order and change request tracking, and ensure adequate controls exist to prevent fraud waste and abuse.

The solution shall provide:

- An ordering process that uses workflow management with multiple approval hierarchies for multiple functional or business units. Individual component level requirements will be specified by the ordering agency.
- An ordering interface that ensures that only government approved devices and accessories can be ordered through the portal.
- Ability to reconfigure the portal / systems to accommodate different standard equipment sets as they change and as they are approved by the government COR over time.
- Ability to control device type by Special Designation, Cost Center, System Role, or other Agency-defined category.

3.1.1.1.1 Catalog

The solution shall demonstrate the ability to perform an initial contract optimization analysis of existing wireless service agreements to identify immediate savings. This includes the ability to perform and report follow-on comprehensive assessments of all existing wireless service contracts and agreements to identify improvements and cost savings opportunities. These capabilities include:

- Asset Acquisition
- Service Plan Acquisition
- Service Plan Management

The vendor catalog solution shall also automatically update as new data is received to continually identify new improvements and cost savings opportunities.

3.1.1.2 Inventory Management

The TEMS solution shall be capable of establishing an accurate inventory database.

- The desired goal is 100% accuracy of all Agency user assets
- Initial inventory to be delivered (Agency to define timeline based on number of assets, physical location of assets, ability of Agency personnel to provide data when desired)
- Vendor to deliver results to the COR for agency verification and acceptance
- Ongoing inventory management to be provided by the Vendor over the life of the contract consistent with the inventory validation cycle and deliverable that has been preapproved by the Government.
- Tracking of phones, devices, and accessories procured by Agency personnel for emergency or temporary-use situations.

Inventory Management also includes maintenance and continual database updates as needed or required. The solution's Inventory Management System shall:

- Describe whether, when, and how designated Agency representatives can access the inventory
- Include the ability and instructions for designated Agency representatives to search, filter, and sort information by type
- Provide the ability for designated Vendor and Government representatives to link (or map) an inventory item to multiple supplier billing accounts
- Describe the manual entry and automated components of inventory updating
- Provide Service Level Agreements associated with the inventory management system
- Ensure all warranty components for all equipment is properly identified, documented, catalogued, registered, and utilized according to the Original Equipment Manufacturers (OEMs) requirements
- Leverage warranty replacements for devices and peripherals such as cellular device holders or cases as to optimize savings for the Agency when replacements are required

The vendor solution shall provide provisions for the following:

- Device/Asset Tracking
- Non-Device Tracking (e.g. accessories, miscellaneous hardware, software, licenses)
- Real-Time Inventory
- Account Reports
- Device Disposal (e.g. disposal of devices on behalf of the Government and tracking inventory change, or simply tracking disposal of devices that the Government returns to the carrier as dictated by Agency workflow processes)
- Reporting ENERGY STAR compliance
- Reporting Electronic Product Environmental Assessment Tool (EPEAT) assessment

3.1.1.3 Expense Management

The respondents must demonstrate how they are capable of providing a reduction of telecommunication costs through dispute recovery, rate plan optimization, contract optimization and elimination or reduction of zero use devices. The respondent's expense management processes shall be compliant with Agency-specific policies and workflows.

3.1.1.4 Invoice Consolidation

The solution shall provide invoice consolidation capabilities tailored to the specific Agency business processes, which shall include the following activities at a minimum:

- Collect, process, and validate paper and electronic invoices received from multiple carriers in multiple billing formats against agency information, ordering records, and telecom contract and service agreement terms
- Allocate cost information from the carrier invoices across agency's organizational units and financial accounts to provide increased visibility and accuracy for agency's cost and spend management functions
- Prepare monthly reports identifying billing and invoicing errors for agency claim and dispute submittal

- Integrate invoice data with procurement and inventory management data records to enable and support spend, inventory and usage analysis by the Vendor and Agency telecommunications managers
- Prepare monthly standardized management reports detailing spending levels and trends by carrier, regions, business units, accounts, service lines and service types
- Provide the capability to generate custom-designed and ad hoc spending reports at both a summary and various organizational or financial account levels
- Prepare management reports on budget spend, including projections for current and future fiscal years
- Prepare and provide necessary electronic reports or formatted data feeds to the Agency's bill payment system (or the Vendor's internal payment system if the task order includes the Bill Payment Services option).
- Provide recommendations to the Agency on areas for improvement and savings regarding agency's invoice process (e.g. where invoice consolidation with major carriers would benefit the Government).
- Provide recommendations to the Agency for alternative invoicing options that may benefit the Government (e.g. prepayment of invoices by the vendor with follow-up verification by the Government.
- Provide help desk support as listed in Section 2.1.3.2, Customer Support, to answer billing and invoicing questions from agency financial and telecommunications account managers and to provide and implement recommendations

3.1.1.5 Contract Optimization

The solution shall perform an initial contract optimization analysis and rate-plan and usage optimization analysis of existing wireless service agreements to identify immediate savings. This includes the ability to perform and report follow-on comprehensive assessments of all existing wireless service contracts and agreements to identify improvements and cost savings opportunities. The vendor shall periodically perform these contract and rate optimizations on a regular basis, no less frequently than annually. Contract optimization activities shall include:

- Benchmarking the agency's existing pricing, service terms and conditions with those of other federal and commercial customers and accepted "Best Practices" to identify recommended changes.
- Making specific recommendations for rationalization of rate-plan types, migration of service lines between specific wireless service providers, changing the number of total wireless service providers, changes in contract terms and conditions, and other opportunities that would lower total cost while maintaining or improving the quality of wireless service provided to the agency's users. Provide all necessary metrics (e.g. minutes/capacity purchased, minutes/capacity used, average minutes/capacity used for the specific user/line, internal Agency cost center, and overall Agency.
- Submitting changes for agency approval and assist with the implementation of contract optimization recommendations, changes, and sourcing/competitive bidding among Wireless service providers to lower overall costs.
- Tracking and reporting savings derived from the requisite contract and rate-plan optimization efforts.

- Identifying and reporting on zero use devices.

3.1.1.6 Dispute Resolution

The vendor solution shall collect and prepare information necessary to resolve billing and accounting errors with the wireless service providers and maintain this information in the portal. The vendor shall also manage and track all claims through final resolution. Dispute resolution capabilities include:

- Collect and prepare support material necessary to file and defend claims submitted to the carriers for billing and account corrections.
- Research, review, dispute, and track all potential billing errors and represent the agency as an authorized agent with all carriers and telecommunications suppliers.
- Submit written claims to telecom carriers and suppliers, including reasonable and necessary support documentation, to identify and recover any audit savings for the agency. These are not contract claims as defined in FAR Part 33, which will be handled by a warranted Contracting Officer.
- When errors are found and credits are due to the government, apply those credits to the service line level to ensure they are correctly applied to the component, individual, and/ or project chargeback codes. Additionally, credits may also reference a telecom carrier invoice and line item number.
- Collect, prepare, and submit any information necessary to identify and recover any audit savings from the wireless service providers.
- Manage and track all disputes through final resolution. These are not contract claims as defined in FAR Part 33, which will be handled by a warranted Contracting Officer.
- Prepare and provide the agency with monthly reports detailing the status of claims filed with the carriers, billing accuracy rates for individual carriers, and the amount of any savings (or additional cost) recovered as a result of the audit and dispute recovery efforts
- Apply recovered funds to the specific wireless service being credited.

3.1.1.7 Expense Analysis

The vendor solution shall support allocation of fixed and mobile costs to specific codes, enabling reporting of costs by department, location, employee, and other relevant scenarios. The vendor shall ensure that automated cost allocations can be overridden on a single-case basis, provide appropriate level of detail for cost allocation/chargeback, and accommodate varying allocation and chargeback rules based on the billing media (EDI, FTP, paper, etc...), and whether these rules include fixed percentages from some expenses and allocations based on consumption. The vendor shall support EDI 810/820 standards for invoice payment/cost allocation and payment advice files.

3.1.1.8 Expense Reporting

The vendor solution shall be capable of reporting on all aspects of the TEMS capabilities to support multiple goals, including cost reduction for carrier-provided service plans, elimination of wasteful spending trends, detecting fraud by any party, and any other aspect of full lifecycle management.

The reporting capability will allow the Government to categorize and track lifecycle issues, including:

- Identification of actual usage patterns by carrier, device type, program office, and end user
- Identification of usage patterns and classification into regular usage, minimal usage, zero usage and mis-aligned usage (where actual usage does not match the plan, or international roaming)
- Identification of alternate carriers or contracts to obtain optimized pricing
- Identification of cost savings to date, and strategies for continued spend optimization
- Identification of contract restructuring to obtain additional volume-based discounts

Mission-critical metrics should be available to the entire enterprise – on demand – to allow the Government to make informed decisions from real time reports such as analysis of usage patterns, spend trending, and inventory expense by location. Reporting capabilities shall include configurable summary dashboards and detailed reports, ad-hoc reports, the ability to drill down into every level and aspect of data, and comprehensive data analytics and visualization tools.

3.1.1.9 Rate Optimizer

- The vendor shall perform an initial rate plan analysis of existing wireless service agreements to identify immediate savings. Subsequent to the initial review, the vendor shall conduct follow-on reviews to ensure cost savings and price reductions for products and services pursuant to the contract.
- The vendor shall provide recommendations to rationalize rate plan types, the number of service lines with each wireless service provider, the total number of wireless service providers, and other opportunities that might lower total cost while maintaining or improving the quality of wireless service provided to Agency users.
- The vendor shall calculate costs to the Agency based on actual monthly usage patterns of users and determine where individual account and rate plan changes should be made to lower future costs. The analysis shall be based on a three-month usage period. This applies primarily to voice and data usage. All other featured usage shall be monitored and addressed on current month usage. This information shall be contained in the monthly Performance Status Report.
- The vendor shall provide optimization recommendations to the Agency designated representatives, and upon approval, implement the optimization recommendations and changes as specified by the Government. Where permitted by Agency-specific policies and workflows, the vendor will immediately implement optimizations, and then notify the Government of changes and make further changes as directed.
- Standard service optimizations of each vendor's priced offerings shall be performed on a regular basis, no less frequently than quarterly. Contract optimization (e.g. optimizing across multiple vendors) shall be also be performed on a regular basis, no less frequently than annually, to assist the Government with implementing major contract changes.

3.1.1.10 Bill Payment

- As needed by Agency-specific policies and workflows, the vendor shall accept, pay out, manage, and report on bills from carriers utilizing the web portal, backend analytics and integration services as is appropriate for the Agency.
- The vendor shall provide an effective workflow process from invoice receipt through payment, incorporating details such as average times from receipt, to approval, to payment.

- The vendor shall provide a consolidated invoice capability incorporating multiple carriers. Service shall support funding streams that consolidates wireless service, equipment, miscellaneous managed services and fees.
- Service shall include payment for shipping, equipment and accessories provided by carriers, and miscellaneous equipment and accessoriesneeded for wireless packages that are not provided by the wireless carriers meeting FAR-51.

3.1.1.11 Documentation Management

The vendor's TEMS solution will include a document repository which allows the Government to store, update, and perform configuration on a variety of documents to include policy documents, carrier contract info, and user guides. The content, and structure of the repository, shall be fully under the control of the Government.

Access to this repository will be provided using role-based access, and multiple types of roles shall be supported.

4 Management Services

4.1.1.1 Program Management

A Program/Project Manager with responsibilities for managing contract, schedule, costs and deliverables is required. The respondent must identify their PM POC for all customer interface, and who clearly demonstrates past experience in developing and implementing a Project Management Plan directly related to wireless TEMS, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

The Vendor shall designate a Project Manager as a Key Personnel representative and the Lead for this effort.

This individual will be primarily responsible for managing all areas of contract performance, deliverables, and reporting; including but not limited to: staffing; managing, tracking, and reporting contract performance, deliverables, and training, quality control, schedule (planning and managing), costs, customer service, identifying risk and risk mitigation, communicate and interface with the COR and Government leads.

Guidelines for Agency requirements include:

- Have at least 24 months recent project management experience successfully leading at least two (2) IT customer focused projects directly relating to wireless TEMS using Project Management Institute (PMI) project management standards; or at least 12 months project management experience successfully completing at least one major IT customer project relating to wireless TEMS that is same or similar in size, scope, and complexity for this effort using PMI project management standards
- Be knowledgeable, and demonstrate the ability to remain current, on all aspects regarding wireless TEMS services, carrier plans, and offerings available to the Government through existing contract vehicles
- Provide the ability to work effectively with the Government and wireless TEMS carrier representatives
- Serve as the primary interface with the Contracting Officer's Representative and Government technical leads
- Anticipate appropriate Government customer and account needs and provide reliable customer relations to a diverse set of customers with a wide array of different wireless cellular service needs
- Successfully manage time and resources
- Be thoroughly knowledgeable and be able to discuss or explain all aspects of the Vendor's wireless TEMS services and related customer operations
- Ensure deliverables are provided on-time with minimal need for revisions or corrections
- Effectively lead or participate in oral and written communications with the COR and Government leads
- Effectively investigate, mitigate, and resolve contract performance issues or concerns.

The Project Manager shall also ensure that the Program Management Plan that has been reviewed and accepted by the Government is properly implemented, executed, and remains

current to ensure consistent, quality service delivery through standardized performance metrics and reporting.

As part of the overall duties for the Program Manager, the Vendor shall create and maintain a Program Management Plan to ensure consistent, quality service delivery through standardized performance metrics and reporting. The plan shall include at a minimum:

- Documented standard processes and procedures
- Defined controls and metrics
- Processes to ensure standardized reporting on all service delivery performance
- Staffing Plan
- Training Plan

Once accepted by the Government, revisions to the Vendor's Program Management Plan must be reviewed and preapproved by the COR in writing.

Contract Transition-In: The Vendor shall provide a Transition Plan that details how devices previously supported by the government will transition from existing service in a quick, reliable, and accurate manner to the offered solution. This action begins at contract award and includes downloading relevant service contracts, user profiles, device data and usage into database or solution systems, and the performance of initial optimization for the agency. Staffing requirements (vendor and government) for this Transition Plan must also be identified. The proposed solution will receive additional consideration if example transition plans from previous MDM deployments are supplied. The Vendor's transition-in plan shall be based on lessons-learned from successful on-boarding of hundreds to many thousands of devices. The example must include a high-level timeline, staffing required, and a summary walk-through of the process.

The program management plan shall clearly describe how initial deployment support and integration services will be provided. These services are expected for installing, configuring, and certifying the initial deployment of the TEMS solution, as well as the ability to support specific agency related integrations or customizations. The program management plan shall also detail all activities associated with assisting the Agency with quickly and efficiently achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.

Contract Transition-Out: The Vendor shall provide a transition-out plan that describes how all data associated with this TEMS solution shall be delivered to the Government, and the contract close-out processes that the Vendor will follow.

4.1.1.2 Customer Support

The Vendor shall provide a high degree of professional customer services to various Agency users that collectively have a wide array of different wireless cellular service and reporting needs. For example, Agency staff that regularly travel domestically and abroad require access to wireless data in-route to, from, and while at their temporary duty stations. In these instances the Agency relies heavily on its TEMS provider to ensure that the needs of its traveling staff during travel are managed effectively and cost-efficiently.

Note to Agency Representatives: Help Desk / Customer Service desk support is anticipated to be one of the key cost drivers for TEMS service support. The help desk / service desk support requirements were obtained from other agencies, but your specific Agency needs will likely differ. Please assess Agency-specific needs to ensure minimal head count is provided by the TEMS provider but will meet your needs.

In addition, the customer support desk shall include:

- A trouble-ticketing system where each request has a unique identifier for tracking purposes
- Help Desk interaction that supports online requests / resolution, supported with email
- Telephone (voice) Help Desk support must be available, but can be limited to business hours
- Ability to generate and receive automated customer surveys, process and report the results to Agency management, and incorporate lessons-learned into ongoing service improvement.

Customer Service Plan: The Vendor shall develop and implement a Customer Service Plan, for government review and acceptance, which describes in detail how they will provide High-Touch and Low-Touch Customer Service. The Vendor's Customer Service Plan shall include a combination of High-Touch and Low-Touch Services – depending on the required service, customer experience, and customer preference.

1. *High-Touch Customer Service:* High-Touch Customer Support shall include a high degree of customer service and interaction to resolve customer issues in a timely, proactive manner; i.e. understand and anticipate each unique customer situation and take appropriate actions to respond and resolve customer issues as they occur/in real-time. Depending on the customer location and situation support shall be provided in by telephone (human interaction) and/or face-to-face interaction. High-Touch Customer Service shall be available 24x7x365/6 (including all federal holidays);.
2. *Low-Touch Customer Service:* Support will be provided by automated telephone systems and online, self-service web-based portals to process business transactions. Low-Touch Customer Service shall be available 24x7x365/6 (including all federal holidays).

Mitigate Charges: The Vendor shall monitor, report, and with written COR preapproval take actions to temporarily (or permanently) mitigate charges for users with unusually high international or local voice and data usage that may negatively impact service to other users or costs to the agency.

Help Desk Support and Customer Service Management Plan. The Vendor's Customer Service Plan shall also include how they will provide Help Desk Support Services for approved TEMS solutions, and identify Vendor personnel (by position title) and any required Agency support that will be included in the Agency customer service chain and Administrative Help Desk Services as described below.

Customer Help Desk Support team shall be available to coordinate and assist the Agency IT Help Desk in identifying, documenting, and tracking all customer help desk requests until satisfactorily resolved.

Customer help desk interactions and functions shall also:

- Utilize a trouble-ticketing system where each call/request has a time-stamp and unique identifier for tracking purposes
- Include telephone (voice) support available during the CORE contract business hours
- Support online requests and resolution supported by email
- Record, archive, and be retrievable upon written request from the COR
- Include automated tracking and verification of each customer contact until resolved and archived
- Track the duration of each call, similar calls from the same or multiple users
- Track dropped, abandoned, and disconnected calls
- Optionally, integrate support with other mobile managed services (e.g. MDM deployment, kitting, etc.)
- Optionally, integrate support with pre-existing Agency Help Desk Support personnel and systems
- Facilitate routine customer satisfaction surveys and matrix upon CORs request
- Administrative Help Desk Support includes, but is not limited to, invoicing, billing, or other account related services, and must be available from Monday through Friday, 8:30 AM to 5:30 PM EST,), excluding federal holidays where the government (or Agency Headquarters) is officially closed for business.

4.1.1.3 Training

The government requires that all users of the TEMS system, which includes end users, administrators and developers, be trained to correctly utilize the system. The Vendor shall be responsible for developing and updating the TEMS Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan. Online training shall be hosted by the vendor, and the vendor must provide the required content.

4.1.1.4 TEMS Data Management

Transition-In (Use Case #1 – from prior TEMS provider): The Vendor shall ingest current and historical data from the prior TEMS support vendor, and/or government databases as necessary in order to implement service. The Vendor will initiate ongoing data ingest from the carriers on behalf of the Agency, and notify the Agency of any discrepancies to allow the Government to address with the carriers. The Vendor shall provide any necessary data cleanup to implement service.

Transition-In (Use Case #2 – without prior TEMS provider, without historical analysis): The Vendor shall initiate regular data ingest from the Government databases and wireless carriers as necessary in order to implement service. The Vendor shall provide any necessary data cleanup to implement service. The vendor will notify the Agency of any discrepancies to assist the Government to address with the carriers. Historical tracking, data cleanup, and analysis will be performed on carrier data dated as of or later than the date of contract award.

Transition-In (Use Case #3 – without prior TEMS provider, with historical analysis): The Vendor shall initiate regular data ingest from the government databases and wireless carriers as necessary in order to implement service. The Vendor shall provide any necessary data cleanup to implement service. The vendor will notify the Agency of any discrepancies to assist the government in addressing discrepancies with the carriers. Historical tracking, data cleanup, and analysis will be performed on carrier data dated as of [*TBD – Agency to specify*].

Transition-Out: The Vendor shall export all managed TEMS data to the next TEMS support vendor and/or government databases using commercially standard format(s) as requested by the government to effect smooth transition of services.

4.1.1.5 Audit Capabilities

The Vendor shall be capable of applying risk mitigation strategies and implementing cost controls to assist the Agency to comply with with OMB Circular A-123 and Presidential Executive Order 13589.

The vendor shall provide all necessary audit support to the Agency. At a minimum, auditing should include:

- Validation of account ownership and service existence
- Verification of rates, charges, and discounts
- Verification of correct account numbers and phone numbers associated with accounts
- Identification and Recovery of missing carrier invoices
- Analysis of invoices for abuse, misuse and fraud

4.1.1.6 Management Reporting

The Vendor shall provide a robust menu of standard, preconfigured reports facilitated by a web-based "download and save" capability through the portal. The respondent shall provide sample reports that are available as standard reports and shall indicate the degree of customization of these reports that is possible. The Vendor shall provide data analytics capabilities and display techniques that represent data in graphical or tabular format(s) that foster clear understanding by Agencies.

All reporting shall provide the capability for authorized users to generate new reports and ad hoc reports at both a summary level as well as down to organizational and financial account levels. Reports shall be provided in 508 compliant electronic formats with read/write capability using applications that are compatible with agency programs (such as Microsoft Office).

For vendors to participate in this program, GSA requires that they submit a semi-annual report that can capture programmatic traction and savings that agencies benefit from by using a TEMS provider. This semi-annual report will be due after, and reflect activities through Q2 (after March 31st) and Q4 (after September 30th) of the federal FY (October-September).

Information that will be requested is only that information that can be publically releasable. At a minimum the government will require the agency, task order number, total amount of the award, and attributable savings to date. Respondents must indicate that they are willing and able to

provide the publicly available information to the GSA Managed Mobility PMO in the following format:

Agency	Task Order #	Total Award Amount	Attributable Savings to Date

This report will be available in both Excel format and in formats suitable for processing with mobile devices. This report is not for distribution for anyone other than the PMO and is meant to track programmatic impact as well as attributable savings. It is protectable under FOIA Exemption #4 and cannot and will not be distributed, internally within GSA or externally with other parties, without the expressed written and documented consent of the TEMS provider.

5 Compliance with Government Policies

5.1.1.1 Security

The TEMS solution must be certifiable at a FISMA Moderate Impact level (NIST SP 800-53 Moderate or DoD 8500.2 MAC II) or higher. The response may include proof of certification, accreditation, or Authorization to Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or Authority-To-Operate (ATO).

5.1.1.2 IPv4/IPv6

IPv6 compliance is a goal for this request. On-premise portions of the solution must support IPv6 for network communications. Controls on network communications must apply to both IPv4 and IPv6 communications. The respondent must provide a description of the IP based components of their solution and the status (compliant or non-compliant) of the proposed solution as applicable. If the proposed solution is not compliant at time of response submission, the respondent shall provide an estimated timeline to achieve IPv6 compliance.

6 FedRAMP

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Therefore:

- If the approved solution is cloud based, the Agency requires a FedRAMP compliant solution listed on www.fedramp.gov under "FedRAMP Ready Cloud Systems" or evidence that the Vendor is actively pursuing FedRAMP compliance or provide evidence acceptable to the Agency that the security controls are equivalent to FedRAMP requirements
- If the approved solution is not cloud based, as a minimum, the vendor shall provide a system security plan and privacy threshold analysis/privacy impact analysis, incident response and contingency plans, and an independent assessment of the security control effectiveness.

6.1 Access to Sensitive Information

In conjunction with contract performance Vendor personnel may require access to Sensitive Agency Information. Sensitive Agency Information includes Personally Identifiable Information (PII). Sensitive Agency information, including systems or records, is protected under the Privacy Act. Sensitive Agency Information may also exist in other types of records, such as databases, log files, e-mail, and correspondence files. Therefore, all Vendor personnel are responsible for recognizing Sensitive Information, avoiding inappropriate or accidental access, use, or disclosure in accordance with Agency IT policies, and proper procedures for incident reporting.

In addition, written preapproval from the COR, or the Chief Information Officer (CIO) or delegate, is required prior to the use or storage of Sensitive Information or sharing of Sensitive Information by the Vendor with any subvendor, person, or entity. The Vendor shall not remove, copy or transfer Sensitive Information from approved location(s), electronic device(s), or other container(s), without prior approval of the CIO, or designate.

6.2 Information Security Incidents

An information security incident is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure or acquisition, or unauthorized access of any Vendor or Government systems or information.

Information Security Incident Reporting Requirements. All Information Security Incidents shall be reported in accordance with the requirements below, even if it is believed the Incident may be limited, small, or insignificant. The Agency will determine when an Incident requires additional focus and attention:

- Vendor personnel shall report all Information Security Incidents to the COR and IT Security, orally and in writing, not later than 30 minutes, after becoming aware of a potential or actual Incident, regardless of day or time
- When notifying the COR and IT Security via email copy the Contracting Officer if possible; when reporting the incident by phone or face-to-face, or if the Contracting

Officer's email is not immediately available; contact the Contracting Officer immediately after reporting the incident to the COR

- When reporting SI incidents in writing (i.e. emails or written incident reports) the Vendor shall not forward, include, or repeat Sensitive Information in the subject or body
- As required and preapproved by the Government Vendor personnel shall transmit Sensitive Information (or attachments containing SI) in accordance with (IAW) FIPS 140-2 compliant encryption methods. Passwords shall not be communicated in the same email as attachments
- As required Vendor shall also provide supplementary information or reports related to a previously reported incident directly to the COR and IT Security using the following email subject line: "Supplementary Information/Report related to previously reported incident ## [insert number]."

Information Security Incident Response Requirements. All determinations related to Information Security Incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by authorized Agency officials at the Agency's discretion;

- The Vendor shall provide full access and cooperation for all activities determined by the Agency to be required to ensure an effective Sensitive Information or Incident Response, including but not limited to, all requested images, log files, and event information to facilitate rapid resolution of Information Security Incidents
- The Vendor shall also cooperate and assist the Agency in Incident Response activities, including but not limited to, inspections, investigations, forensic reviews, data analyses and processing, and final determinations of responsibility for the Incident and/or liability for any additional Response activities
- The Vendor shall cooperate and assist the Agency with responding to and supporting other Federal agencies and/or third parties to aid in Incident Response activities
- The Vendor shall be responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by the Agency, whether incurred by the Agency, agents under contract or on assignment to the Agency, or by third party firms.

The Vendor shall provide and maintain a detailed summary document demonstrating how their SECURE WEB ACCESS POINT (WEB PORTAL) meets each of the above SOW requirements for this section.

7 FIPS/FISMA

In regards to FIPS certification, the government will assess whether the solutions include a FIPS 140-2 certificate number or appears on the NIST "Modules in Process" list. If a respondent's system does not have a FIPS certification, they must provide evidence that their system has been assessed as FIPS compliant through a deployment at a federal agency. This evidence must include the name, agency, and contact information for the authorizing official.

In regards to FISMA, the government will assess whether the respondent offers evidence of FISMA authorization at the Moderate impact level. The respondent will provide evidence of an ATO, contact information for the authorizing official, or provide evidence that their system is currently undergoing a authorization review.

8 Pricing

When requested to evaluate pricing of the solution providers, pricing should be presented on a per device basis – it can be presented in the context of price ranges, pricing tiers based upon volume, pricing based upon pre-defined product configurations or some other scenario or set of scenarios. However, to keep with the purpose of this document and to scale across government, it is strongly suggested that pricing submissions be kept to fairly simple structures so that a cost per device can be easily determined and understood in the context of services delivered.

Pricing may either be customized or may be submitted based upon availability through publicly accessed source. Pricing should be submitted as an integral part of the providers' solution.

Agencies should request that solution providers indicate the range at which their product is sold to their federal customers, inclusive of the discounted rate that is offered to their best federal customer. It is recognized that not every federal customer purchases solutions identically, and often pricing is dependent on specific agency needs and requirements. The intent is to indicate the range of potential pricing, subject to the particular requirements that fall beyond the specifications. Additionally, agencies should request a pricing table, which reflects the price structure and currently listed prices for the solutions on Federal contracts/task orders.

For those solution providers offering their solution under IT Schedule 70, the solutions must be on the vehicle and the pricing must correspond to what is found on the schedule. If the solution is offered via a company's IT Schedule 70 contract, the solution must currently reside on that contract vehicle to be considered. If the solution cannot be identified on the company's IT 70 contract it will not be considered for assessment at this time. For pricing related to other government-wide acquisition vehicles, the rules would be consistent with those of the particular vehicle necessary to reach the solution's solution set.

Appendix A Glossary and Abbreviations

Term	Description
Agency	"Department" or other administrative unit of the federal government, such as the General Services Administration (GSA), which is using this contract vehicle. This also includes quasi-government entities, such as the United States Postal Service.
API	Application Programming Interface
Blacklist	Application or software not deemed acceptable and have been denied approval. This may vary between agencies.
Bureau	A sub-Agency Bureau level organization, which is using this contract vehicle, as defined by OMB (www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf).
BYOD	Bring Your Own Device; Staff brings their personally-owned devices and the Enterprise installs capabilities such as email on them. May also refer to bringing devices from other agencies.
CAC	Common Access Card; a 2-factor electronic identity card used by the Department of Defense to identify individuals. The civilian equivalent is the Personal Identity Verification (PIV) card.
Capability	A technical service requirement that is a component of the base service.
CBP	Customs and Border Protection
CIO	Chief Information Officer
COTS	Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors.
DANIEL	DHS Advanced Network Integration and Experimentation Lab
Data Plan	Includes web browsing, send and receive email, download attachments, downloading applications, and application data usage.
Device	Also called handheld wireless devices, these include handheld devices that are capable of wireless voice or data communications. The devices support cellular or paging technologies augmented by technologies such as WLAN and satellite.
Feature	An enhancement beyond base service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced (NSP). Each feature must be ordered separately even if not separately priced.
FAS	Federal Acquisition Service.
FICAM	Federal Identity, Credential, and Access Management mainly addresses user certificate authentication although it does touch on passwords. FICAM is the guidance document, ICAM is the body that created it.
FIPS	Federal Information Processing Standards.
FSSI	Federal Strategic Sourcing Initiative; FSSI Wireless provides wireless service and device ordering capabilities to Government agencies.
GB	Gigabyte or 1000 MB of data.
GFE	Government Furnished Equipment.
GPS	Global Positioning System; A network of orbiting satellites that enable receivers on the ground

Term	Description
	to report their position, velocity and time. Mobile devices often use Assisted GPS (AGPS) which leverages cell towers to speed reporting time.
Government	All government entities that use or administer this contract vehicle, including state, local and education.
Government Web Store	Concept of web-based acquisition interface and management platform where government stakeholders (employees, citizens, partners) may initiate purchases, manage previous purchases, and manage vendor relationships. Concept is based on enterprise version of a commercial web storefront.
HSPD-12	Homeland Security Presidential Directive 12, which (among other things) directs agencies to deploy 2-factor authentication for information systems.
M2M	Machine to machine technologies that allow both wireless and wired systems to communicate with other devices of the same ability.
MAS/MAM	Mobile Application Services/Mobile Applications Management.
MB	Megabyte, a common term used to describe the amount of data being sent over a wireless network.
Mbps	Megabits per second, a common term used to describe wireless transmission speeds.
Mobile Device	Characteristics include 1) a small form factor, 2) at least one wireless network interface for Internet access or voice communications, 3) built-in (non-removable) data storage, 4) an operating system that is not a full-fledged desktop or laptop operating system, 5) built-in features for synchronizing local data with a remote location (desktop, laptop, organizational servers, etc.) if data capable, 6) generally operates using battery power in a non-fixed location.
Mobile Device Management (MDM)	MDM – Mobile Device Management. MDM is a widely used term describing device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring. The definition of MDM varies and reflects its growth (pre-maturity) status.
NIST	National Institute of Standards and Technology
Ordering Entity	Any Agency, sub-Agency, state or local government that is using this contract vehicle.
Ordering Agency	The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency.
PIV	Personal Identification Verification
Portal	A software (or web) solution that enables instant and effortless exchange of business information (Electronic Data Interchange – EDI) over the Internet. This is accomplished by the use of a common operating framework for accessing data and information from different systems. A typical TEMS portal will pull information from carrier electronic billing systems, which is uploaded into their platform (portal). This allows the administrator/user a single view that provides multiple carrier information in a seamless manner, offering efficiency.
Secure Communications	Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications.
Smartphone	Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance.

Term	Description
Subsystem	A subsystem is a set of elements, which is a system itself, and a component of a larger system (Wikipedia). For instance, a subsystem could include both the encryption software and the related software on the server.
TEMS	Telecommunications Expense Management Services, delivered by third parties, relating to processes for the sourcing, procurement and auditing functions connected with business communications expenses. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure [Gartner].
Text Messaging or SMS	Text Messaging or Short Message Service (SMS) is the exchange of brief written messages between cellular phones, smartphones, and data devices over cellular networks.
Third-Party Direct Billing	The receipt of invoices from parties other than the Vendor for services within or outside the scope of this agreement.
Trade Agreements Act (TAA)	The TAA of 1979 is an Act of Congress that governs trade agreements negotiated between the U.S. and other countries under the Trade Act of 1974. Its stated purpose is to: 1) Approve and implement the trade agreements negotiated under the Trade Act of 1974 [19 U.S.C. 2101 et seq.]; 2) Foster the growth and maintenance of an open world trading system; 3) Expand opportunities for the commerce of the United States in international trade; and 4) Improve the rules of international trade and to provide for the enforcement of such rules, and for other purposes. The TAA designated countries are listed in the following web site: http://gsa.federalschedules.com/Resource-Center/Resources/TAA-Designated-Countries.aspx
Trouble Ticket	Also called a trouble report, this is the documentation of a service or device failure that impacts the service. The ticket enables an organization to track the detection, reporting, and resolution of some type of problem.
WLAN Calling	Wireless Local Area Network: Enables a wireless handset to make and receive calls via an internet-connected WLAN (e.g., Wi-Fi network) instead of the cellular network.
White List	Whitelist: Application or software considered safe to run, and is preapproved.
Wireless Systems and Subsystems	Wireless infrastructure, servers, and software that enable an enterprise to enhance its cellular coverage, increase cellular capacity, and enable enterprise solutions (e.g., BlackBerry Enterprise Server) using services offered by the wireless industry.
24/7 phone support	Technical support and user assistance is provided by telephone and Internet 24 hours a day, 365 days (or 366 during leap years) per year.

Mobile Services Category Team (MSCT)

Advanced Technology Academic Research Center (ATARC)

Mobile Threat Protection
App Vetting and App Security
Working Group Document

1 Introduction

1.1 Purpose and Scope

Mobile devices are an essential tool for modern government, giving people access to email, files, and other key business data anytime, anywhere—on hundreds of devices, with more being introduced every year. Embracing mobile devices in the government enterprise, whether GFE (Government Furnished Equipment) or a personal device, being used for work access, makes us more productive, can save money and keep workers happy. But they can also pose huge security risks to government agencies.

A compromised mobile device can give attackers access to the same networks and data that make the device extremely valuable as a business tool. That opening, in turn, can lead to data loss, data theft, malware-infected networks, password compromises and more. Additionally, attackers can leverage stolen corporate data such as address books, calendars, credentials and network profiles to mount sophisticated attacks through other channels such as email and SMS messages.

1.2 Definitions and Assumptions

There are several concepts that are important to understand when considering how to secure a mobile solution across an organization. Some of those concepts and definitions are described in this section.

Malicious WIFI: Malicious WIFI threats include several types of network threats. Example malicious WIFI threats include SSL Man-In-The-Middle, SSL Stripping, host certificate hijacking, protocol downgrade attacks, and general Content Manipulation. Because mobile devices often allow users to access WIFI hotspots in the clear, it leaves data and network activity vulnerable to anyone monitoring the network, including potential attackers. Even legitimate networks can pose a risk when misconfigured. These attacks, easily performed from a laptop or a $99 WIFI hacking device (https://www.wifipineapple.com/), can intercept app, email, and web communications.

Side Loaded App: A side loaded application is defined as any app loaded from a source other than the official commercial app stores for that platform. There are dozens of alternative app stores for both Android and iOS devices. While official app stores analyze applications for security, most MDM solutions do not analyze apps. That paves the way for malicious apps to compromise device data or load malware onto corporate networks, and to steal user credentials and data.

Risky/Non-Compliant apps: Many applications may not be intentionally malicious, but are potentially risky to an organization because they expose sensitive information such as Contact Lists, GPS Location data and other PII data and may share that data remotely with untrusted cloud services or foreign servers.

Jailbroken or Rooted Devices: A mobile device that has been modified to allow Apps to be downloaded, installed, and run outside of the traditional secure methods. Jailbreaking an iOS device, or rooting an Android device compromises the sandboxing and security mechanisms that the OS provides.

Zero-day threats: Zero-day vulnerabilities are those that are unknown (or known only to the attackers) that expose weaknesses in software that can be exploited for access. https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf

Phishing and Spear-Phishing: Phishing is when attackers use social engineering to try to coerce users to open a path into their system. Spear-phishing is when an attacker tailors the social engineering to a targeted group of users. Mobile devices make it difficult to determine whether an email, iMessage, or SMS attachment or link is malicious or to stop users from clicking on it. Attackers can use these links to download malware or trick users into handing over their account credentials.

App Vetting: Part of the software assurance process that occurs following development of a custom app or selection of an app from an app store and prior to installation on a mobile device or publication to a federal, community, or commercial app store. It consists of analysis of the app and an approval/rejection decision on whether to allow the app.

MDM/EMM: A Mobile Device Manager is typically perceived to provide a basic set of capabilities to manage mobile devices. An Enterprise Mobility Manager is typically used to define a more comprehensive device management solution. Both can be a hosted or on-premise solution to manage Government Owned or BYOD devices. Examples include MobileIron, AirWatch, and IBM MaaS360.

Data Collection and Analysis: Mobile Threat Protection (MTP) solutions typically need to collect some information and telemetry from the device to monitor and assess threats. This information should be limited to only what is necessary for analysis and should not include PII data.

Mobile Device Consideration: Not all mobile devices are created equal. Some mobile devices provide additional software and hardware protections such as containers and roots-of-trust. Consideration should be given to the protection provided by the devices being used.

1.3 Going beyond MDM/EMM and App Vetting

Many organizations have deployed mobile device management (MDM) and enterprise mobility management (EMM) systems. MDM tools are designed to configure and manage mobile devices to protect corporate data if the device is lost or stolen. MDM products can also provide device configuration capabilities such as validating that devices are configured to require passcodes, and not allowing USB debugging to be enabled. While an important first step, MDM/EMM tools are most useful as the underpinnings for managing mobile devices, taking defensive actions when alerted of a threat, and helping remediate compromised devices, users and networks.

Application vetting is another valuable tool that should be employed to help secure the mobile environment. However app vetting is typically done up-front before an application is installed on mobile devices. Because applications update frequently, thereby making app vetting too burdensome to support all the apps installed on work related devices, and to detect non-application based threats, agencies should employ a continuous monitoring solution. For that, you need a Mobile Threat Protection (MTP) solution that integrates with your MDM/EMM deployment. MTP provides the underlying intelligence to detect threats in real time and alert your MDM/EMM system for remediation or quarantine.

Although NIST documents such as 800-53 recommend that mobile devices include malware protection, VPN, and other security solutions, more specific government policy describing how to protect mobile devices could have a positive impact on the deployment and usage of such protections. Consequently, many government orgs don't adequately protect mobile devices and the data they access.

1.4 References

- DHS Study on Mobile Device Security (https://www.dhs.gov/publication/csd-mobile-device-security-study)
- NIST NCCoE *Mobile Threat Catalogue* (https://pages.nist.gov/mobile-threat-catalogue/application.html)
- NIST Special Publication (SP) 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*
- ATT&CK Mobile Profile (https://attack.mitre.org/wiki/Main_Page)
- OWASP Mobile Top 10 2016 (https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)

2 Role of Mobile Threat Protection in Mobile Security

A Mobile Threat Protection (MTP) solution monitors a mobile device in real-time to detect various mobile threats that can compromise device, applications and data on mobile devices. An MTP solution is an important part of a layered Mobile Endpoint Protection Strategy that covers the major areas not addressed by MDM/EMM and App Vetting.

1.5 Network Attacks

MITM attacks via WIFI are not new, and can be just as effective on mobile devices as on laptops. MITM attacks are typically a two-step process. First the attacker has to get "in the middle" of the network connection. This is actually quite easy. One can turn on an open WIFI access point in a hotel or other public place and give it an innocuous name like "Free Public WIFI" and people will connect to it. However since most traffic leverages encryption over HTTPS, the attacker will often try to interrupt the encryption to access the traffic. This can be done through a TLS protocol downgrade, SSL stripping, host certificate hijacking and other methods.

To protect against MITM attacks the MTP solution should provide real-time, actionable data about MITM threats based on an active attempt to intercept traffic, without creating false

positives. Providing a warning about insecure WIFI AP's nearby doesn't provide the organization with actionable data and will often create unnecessary alerts for the admin or help desk.

1.6 Side Loaded Apps

There are dozens of alternative app stores for both Android and iOS devices. These untrusted, alternative app stores like Mojo, Vshare, or TuTu often host paid apps that can be loaded on the device for free without jailbreaking or rooting the mobile devices.

The MTP solution should be able to detect applications loaded from untrusted sources (side loaded) by verifying the enterprise app signing certificate and the app signature. The solution should also allow the organization to whitelist legitimate side loaded apps that were installed from sources such as agency app stores and MDM managed apps.

1.7 Compromised Operating System

Both iOS and Android have inherent security features and controls, including sandboxing, and permission controls. Jailbroken or rooted devices compromise the security controls provided by the device operating system.

The MTP solution should provide alerting for jailbroken and rooted devices. Detection should be robust enough to identify intentional, user-initiated compromise or compromise from an attack such as Pegasus.

1.8 Zero-Day Threats

There is a robust market for zero day threats, where people and organizations spend time identifying vulnerabilities and creating exploits to take advantage of them. Organizations sometimes pay millions of dollars to acquire zero-day vulnerabilities, often for nefarious purposes. Because the organizations using them typically don't want the threat found and patched, they often target high value individuals such as executives with these threats. Many of the OS system updates that are released by Apple and Google are often addressing previous zero-day threats, making it important that organizations update their devices in a timely manner.

Preventing zero-day attacks requires real-time threat intelligence deployed across all devices and networks.

1.9 Risky/Non-compliant applications

Many Applications access Agency sensitive information such as GPS location or contacts and attempt to use that info for monetization or share it with untrusted remote servers, or cloud services such as Dropbox. Applications can also expose sensitive data by not implementing best practices for encrypting data at rest and data in transit.

The MTP solution should provide visibility into application behavior so that orgs can decide if the behavior is acceptable for their environment.

1.10 Malicious Applications

Mobile Applications typically change more frequently than any other software on a mobile phone. Therefore, they require continuous monitoring to ensure new apps and updates to existing apps don't introduce unnecessary risk and threats.

The MTP solution should be capable of detecting app install events and validate the new or updated app against criteria of acceptable app risk.

1.11 Malicious URLS and Attachments in Email, iMessage, and SMS

Email is a known and broadly used threat vector used by bad actors. This vector has been a major threat to enterprises for over a decade. iMessage and SMS threats are growing and expected to become a significant threat vector to organizations.

The MTP solution should be capable of detecting and blocking malicious URL's and Attachments sent to mobile devices via email, iMessage, and SMS messages.

3 Mobile Security Best Practice Recommendations

Establish a layered Mobile Endpoint Protection Strategy that covers the major areas not addressed by MDM/EMM and App Vetting.

4 Implementation Guidance

1.12 Security Requirements Definition

An essential first step when implementing a mobile security solution is for the organization to define its mobile security policies, including what apps are acceptable for use on government-furnished devices, and device configuration management policies. Defining the response policies (both automated or manual) can be one of the more challenging efforts and should be given significant consideration. It is critical that the organization clearly communicate the policies and remediation process to users, including timelines. Organizations may also need to consider reviewing their policies and remediations after mobile OS upgrades because they can sometimes change the response options.

1.13 Measures and Metrics

Evaluating the effectiveness of any security solution requires that you consider how the solution improves the overall security of the organization. It also requires that you can identify specific goals and objectives and can measure the improvements objectively. Below are some security goals and objectives that are appropriate for an MTP solution.

- The security of the mobile device should be monitored in real-time. The MTP solution should 1) evaluate application threat, and compliance against agency policies for acceptable risk, 2) validate OS integrity by detecting if a device is jailbroken or rooted, 3) detect network threats such as MITM attacks, 4) detect device configuration risks such as USB debugging enabled and allowing the use of untrusted app sources.

- The window of time between when a threat exists on a device and when it is discovered and remediated allows an attacker to compromise the device. The MTP solution should allow an organization to limit that window of opportunity.
- The validation of efficacy of the MTP solution should take the form of being possible to attest that there are no known active unacceptable threats on the device. If a threat is detected, it is managed and remediated based on the threat level (high, medium, or low risk) to the organization.

1.14 Deployment and Maintenance

- An MTP solution typically uses an application or client on the device to provide insight into threats on the device. Installing the client and enrolling devices in the MTP solution can typically be accomplished either manually via email or a web service, or as a managed app from the MDM. Pushing the MTP client to the devices automatically from the MDM is a more scalable and reliable approach because it also allows the organization to make the client mandatory, preventing the end user from removing the protection.
- Organizations should consider deploying MTP in phases, with “alert only” type policies at the beginning to ensure that the security team understands what to expect in the environment before enabling automated remediation policies.
- The MTP solution should provide a remediation capability either independently or via integration with EMM solutions.
- Privacy is an important consideration in mobile security. Even GFE devices can have personally sensitive information and potentially sensitive apps installed. For example a user could have a diabetes-monitoring app installed outside the container of the device. The MTP solution should allow the organization to protect itself from threats without compromising user privacy whenever possible. This can be accomplished by limiting the data collected from the device, and creating administrative roles that limit access to sensitive data.

5 Future Directions

- MTP solutions should actively look for new threat vectors and establish product strategies to quickly develop and deploy new defenses.
- Google plans to introduce new security capabilities in Android “O”, scheduled to be released in Fall of 2017. Organizations and solution providers should investigate how those changes are implemented and take advantage of them to provide additional security and more timely security patching of Android devices.

6 Conclusion

Defense in depth is a time tested best practice approach to security, and mobile is no different. Having multiple security solutions in place enhances the likelihood that threats will be detected before a compromise occurs.

Best practice defensive layers for mobile security include:

- App vetting of mobile apps before they are approved/deployed.
- Good security development processes in place during enterprise app development.
- An EMM to manage and enforce policies for mobile devices.
- Firewalls to separate and inspect traffic between sensitivity zones.
- Mobile virtualization or containers to separate government data from personal usage on the device.
- Use of a Mobile Threat Protection solution to provide continuous monitoring of the mobile devices and their respective apps, WIFI, and messages (email, SMS, iMessage).

An MTP solution provides active monitoring of mobile threats which provides the organization the confidence to allow users to take advantage of the convenience and efficiency that mobile offers. Without this real-time visibility, organizations are often hesitant to provide mobile solutions.

7 Acknowledgements

The MSCT and the Advanced Technology Academic Research Center (ATARC) appreciate the contributions of the following individuals and organizations in supporting the efforts of the App Vetting and App Security working group and development of this guidance.

- Marika Robertson — Apcerto
- Tom Suder — ATARC
- Tim Harvey — ATARC
- John Drake — DHS S&T
- Vincent Sritapan — DHS S&T
- Anne Dalton — DHS Office of the Chief Information Officer (OCIO)
- Anthony Glynn — DHS OCIO
- Art Mosley — DHS OCIO
- Brett Pfrommer — DHS Customs and Border Protection
- Bob Clemons — DoD
- Stephen Rossero — DoD
- David Driegert — Department of the Navy
- Cathy Simpson — Government Acquisitions
- Suro Sen — GSA
- Jon Johnson — GSA
- Rick Jones — GSA
- Tom Karygiannis — Kryptowire
- Tim LeMaster — Lookout
- Carlton Northern — MITRE
- Mike Peck — MITRE

- Terri Phillips MITRE
- Sean Frazier MobileIron
- Michael Ogata NIST
- Stephen Ryan Proofpoint, Inc.
- Mark Williams VMWare Airwatch

MOBILE SERVICES CATEGORY TEAM (MSCT)

Mobile Device Management (MDM)

MDM Working Group Document

Introduction

Enterprises traditionally established boundaries to separate their trusted internal IT network(s) from untrusted external networks. When enterprise users consume and generate enterprise data on mobile devices, this traditional boundary erodes. Due to the rapid changes in today's mobile platforms, enterprises have the challenge of ensuring that mobile devices connected to their networks can be trusted to protect sensitive data as it is stored, processed, and transmitted, while still giving users the features they have come to expect from mobile devices. Additionally, some enterprises host enterprise data in a public cloud infrastructure, which also needs to be protected.

Centrally managing mobile devices is the *de facto* solution for controlling mobile device use in the enterprise, regardless of mobile deployment scenario. Although central management is not a security technology by itself, technologies such as EMM and MDM can help to properly configure devices in a secure manner. In addition to managing the configuration and security of mobile devices, these technologies offer other features, such as providing secure access to enterprise computing resources.

Technology Overview

Enterprise mobility management (EMM) is a collection of tools that manage enterprise mobile devices in their entirety. MDM is a platform-dependent mobile management technology that provides the necessary functionality to securely enable workplace functionality in a way that complies with an organization's policy. MDMs allowed for control of basic device functions and capabilities, such as remote lock, device wipe, and device encryption. Managing mobile devices has moved beyond just the device's basic functionality. Applications are prevalent on mobile devices and bring risk of vulnerabilities to the device. As a result, another term within mobile management was developed and is known as Mobile Application Management (MAM). MAMs allow for management of the applications on a mobile device, such as the whitelisting and blacklisting of applications. Along with MDMs and MAMs there are other facets of mobile management such as Mobile Content Management (MCM) and Mobile Identity Management (MIM). Today, these many layers of mobile management are typically wrapped into one solution and that solution is known as an EMM or MDM.

An EMM can consist of multiple mobile management functions, including mobile device management (MDM), mobile application management (MAM), and many other services. EMMs can be used to define a set of policies, and push those policies to a mobile device. The mobile device can then enforce these policies via a device-side mechanisms built into the device by the OS vendor and hardware manufacturer. Before policies can be pushed to

a given device, an enterprise must enroll that device into the management platform. An EMM application may need to be installed on the mobile device before it can be enrolled, which is often referred to as an 'MDM agent'. Once a device is enrolled, security and compliance polices are then pushed to the device. These processes and technologies help keep the device secure, and an enterprise aware of the state of a mobile device, and ultimately enable users to work inside and outside their enterprise boundary. There are multiple types of EMMs, each with varying capabilities. In real-world environments, each EMM, MDM agent, and its corresponding device-side isolation mechanism (e.g., container, process isolation) offer different security benefits, usability tradeoffs, and management capabilities.

EMM Features

The following is a high-level set of features of an EMM platform:

- **Device enrollment:** The ability to create a profile or policy set that can integrate with the native EMM and MDM APIs offered by the mobile operating system.
- **Device management:** Once a policy set is defined by the system administrator and deployed to a device, an enforcement engine on the device ensures the policy set is put into practice.
- **Mobile application management:** strong cryptographic protection of data transmitted over untrusted networks to mitigate unauthorized disclosure or modification
- **Mobile Identity integration:** The ability to store, process, and authenticate using PIV Derived Credentials.
- **Private Application Store:** The creation of a mobile application store only available to those mobile users a devices enrolled into the enterprise mobility solution.
- **Mobile Threat Protection:** Use of a system dedicated to providing intelligence on malicious apps and new attack vectors affecting mobile systems. Often provided via data collected on-device and elsewhere in the mobile ecosystem.
- **Unified Endpoint Management:** A capability allowing a single system to manage mobile devices, laptops, and other enterprise information systems.

The following are device side security features that an EMM may be able to configure:

- **Device encryption:** cryptographic protection of all or portions of a device's data storage locations to prevent unauthorized disclosure of enterprise data
- **Application-level encryption:** an alternative or additional layer of cryptographic protection applied only to application data to prevent unauthorized disclosure when device encryption is either undesirable or has been defeated
- **Protected communications:** strong cryptographic protection of data transmitted over untrusted networks to mitigate unauthorized disclosure or modification
- **Remote wipe:** action that prevents the unauthorized access of data stored on a lost or stolen device by rendering data recovery techniques infeasible
- **Selective wipe:** remote wipe that only affects enterprise data, leaving personal data intact; also occurs automatically as a consequence of a device user un-enrolling their device from enterprise management
- **Application whitelisting/blacklisting:** allowing or disallowing the use of applications based on a pre-specified list to prevent the execution of malicious, vulnerable, or flawed applications
- **Asset management:** identify, configure, and maintain the security configuration of devices, components, software, and services residing on a network to reduce the potential for compromise
- **Compliance checks:** determine a device's level of compliance with mandated security policies to prevent granting access to improperly configured and vulnerable devices
- **Root and jailbreak detection:** verification that the security architecture for a mobile device has not been compromised to prevent granting access to untrustworthy devices
- **Auditing and logging:** capture and store security events for devices including enrollment, failed compliance checks, administrative actions, and un-enrollment
- **Canned reports and ad hoc queries:** use preconfigured reports or active searches or filters on security logs to manage incidents and audit compliance
- **Local authentication of user to device:** require a user to provide a PIN, password, cryptographic token, or other authentication mechanism to prevent granting unauthorized access to sensitive device functionality or accessible data
- **Local user authentication to applications:** as above, but specific to an application

- **Remote user authentication:** as above, but for networked applications that require successful authentication to a remote service before granting full access to its functionality and data
- **Device provisioning and enrollment:** identification and association of specific mobile devices with organizational user accounts to ensure that remote access is granted only to authorized users using approved devices
- **Custom privacy statement:** inform users about the implications to privacy or changes to device functionality as a result of accepting organizational management of their personal device or remotely accessing enterprise resources

Threats to Enterprise Mobility

EMMs and MDMs should be considered part of an organization's attack surface. Attacks against EMMs and other device-side mobile security applications, such as containerization technology, are possible.[1] There's a need to fully understand the EMM and device attack surface. High-level concerns include:

- Software and protocol vulnerabilities resident within the operating systems hosting the EMM are a potential entry point.
- EMMs are often complex web applications, and must be secured against common web attacks, such as various forms of injection. See the CWE / SANS Top 25[2] and OWASP Top 10[3] for additional information.
- Vetting the quality of software and understanding how the application interacts with the operating system and other applications.
- Secure data storage, including permissions and storage locations, is a necessity for secure mobility.
- Communications between the EMM and the device need to be secured, including the EMM policy sets and other communications. The EMM policy should not be able to be modified in transit.
- Infect or inhibit normal operation of EMM system
- Unauthorized wiping of data from device
- Force device misconfigurations to facilitate further attacks

---

[1] Tan, Vincent. *Attacking BYOD Enterprise Mobile Security Solutions*, Blackhat 2017. https://www.blackhat.com/docs/us-16/materials/us-16-Tan-Bad-For- Enterprise-Attacking-BYOD-Enterprise-Mobile-Security-Solutions.pdf

[2] https://cwe.mitre.org/top25

[3] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

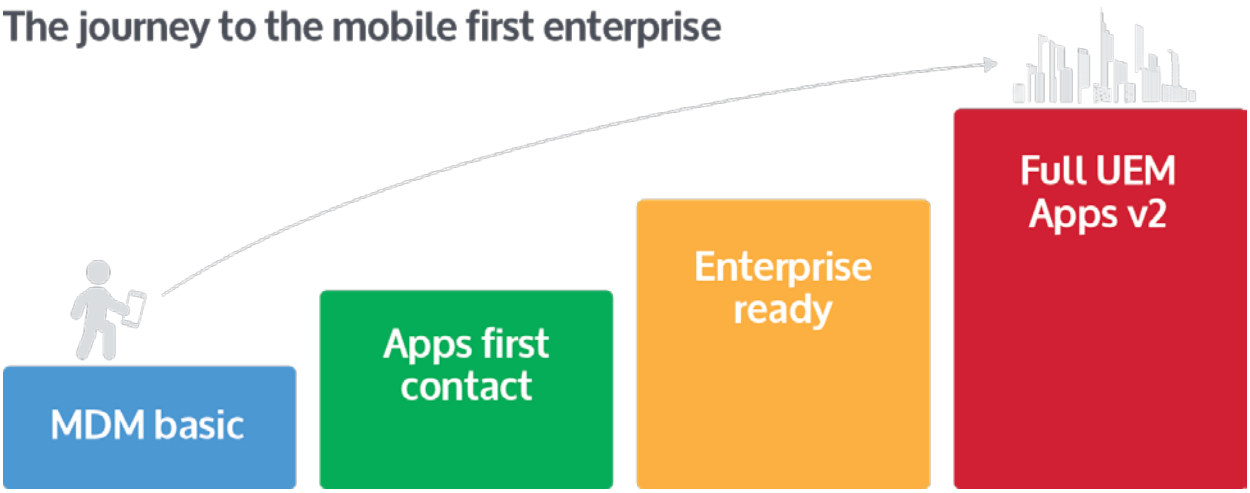
- Force malicious app download to mobile device to facilitate further attacks
- Track user behavior, device location, call logs, text messages, personal contacts, etc

The US Government creates a list of security requirements and objectives for EMMs, via the NIAP protection profiles [12][13][14].

MDM Deployment Phases

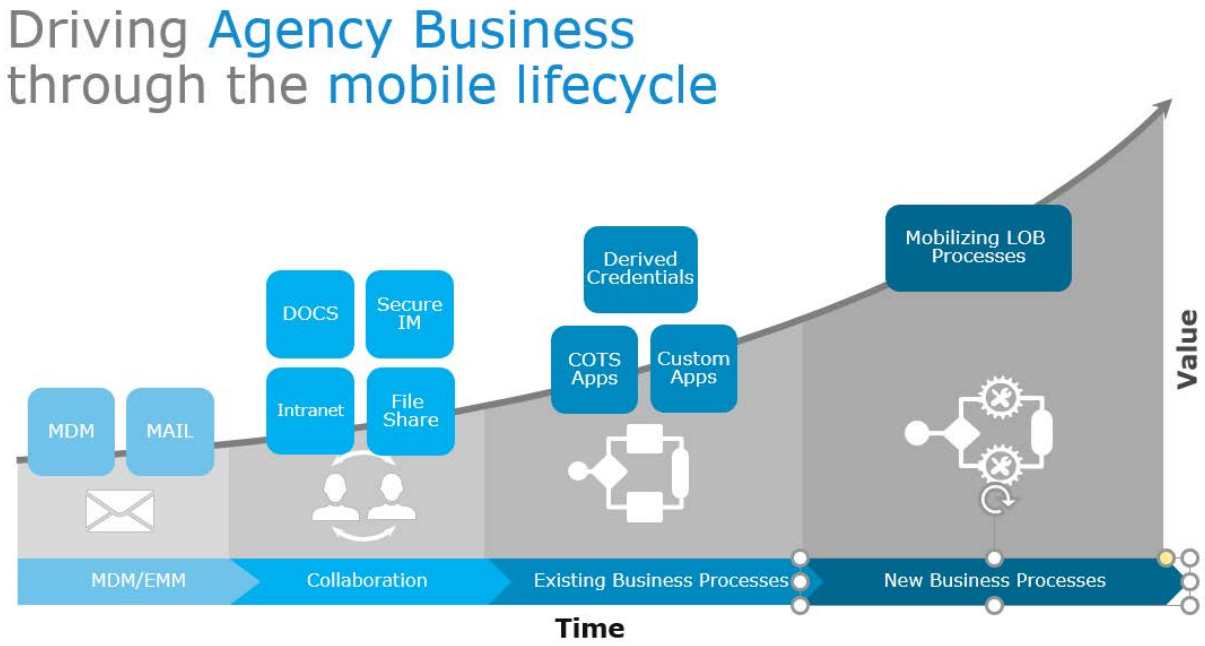
The deployment of mobility capabilities into the enterprise can be categorized into the following tiers:

- Phase I – Basic MDM functionality. Email on device.
- Phase II – Application deployment and development
- Phase III – Comprehensive MDM Solution – Enterprise deployment (PIVD integration, MTP, etc.)
- Phase IV – taking the mobilization of IT to the next level. 2nd gen apps, full UEM (unified endpoint management).

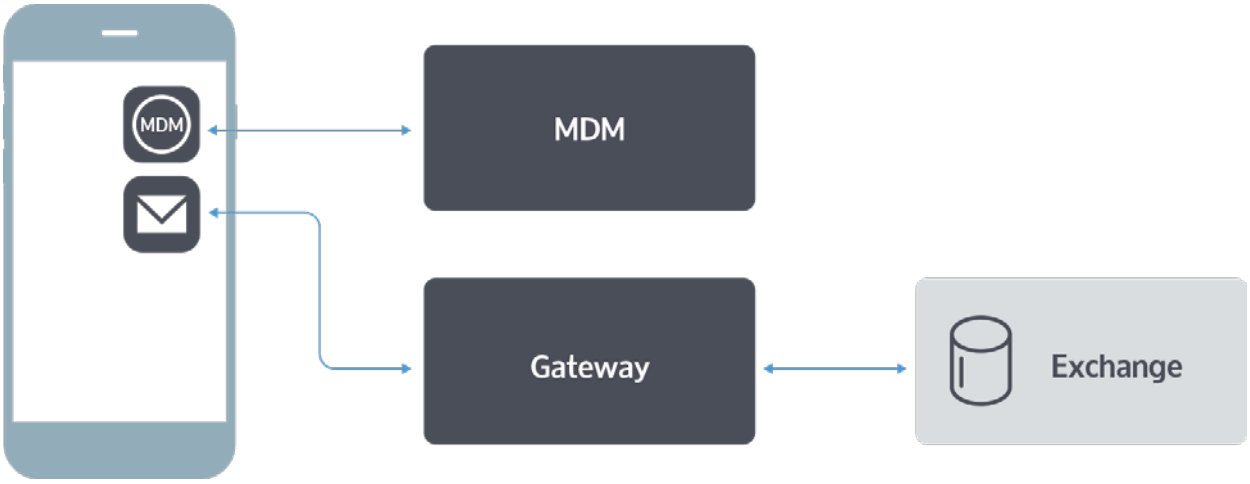


Description:
MDM/EMM can be thought of in the following 4 main phases. The first phase was to get the feature/function parity with generation 1 mobile email devices. Phase 2 was a focus on mobilizing IT and deploying the first phase of useable mobile apps, beyond email but this

was only the 1st phase of mobile application deployment, with a focus on 3rd party apps and some internal app development. Phase 3 was a decided push and focus on bringing MDM/EMM into to play as a critical, enterprise level, management tool, complete with integration into existing IT resources (content, network, identity) and some new ones (MTP, MBAAS, etc.). Phase 4 is the continuation and maturation of the mobile application landscape with the utilization of not only MBAAS, app virtualization but the deployment of cross-platform micro apps and the mobilization of ALL IT available services and applications.



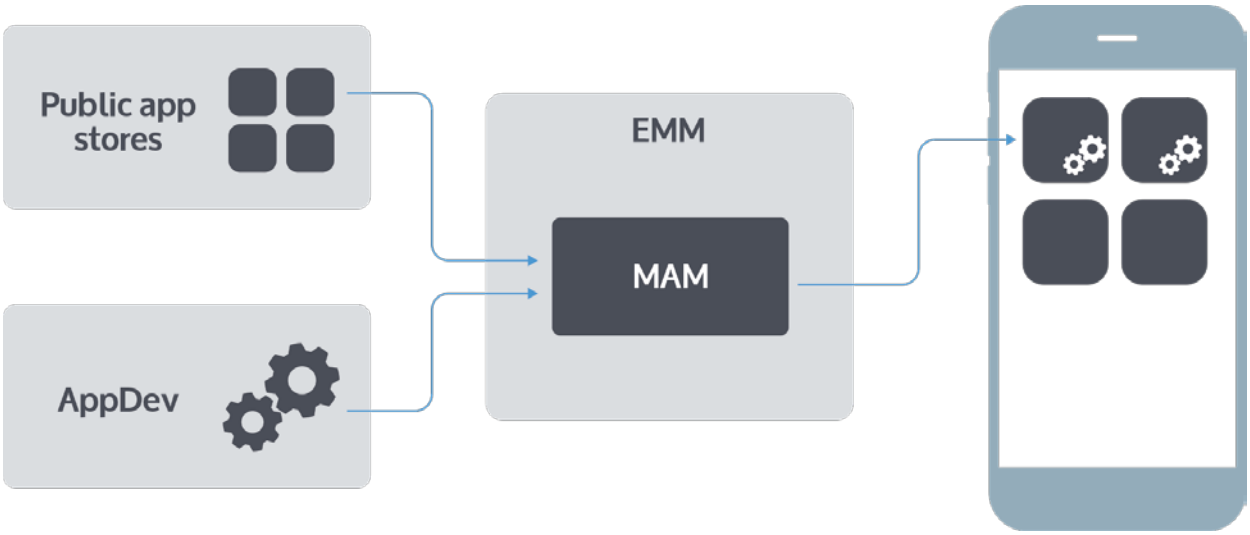
PHASE I – MDM Architectural Diagram



Phase I Basic MDM functionality, Email on device

Description:
The first MDM/EMM deployments were focused on smaller, business unit, level deployments. These deployments were really to service the first highly desirable use case of getting email on the smartphone handset. This was important because the generation 1 public sector mobility solution was blackberry which was inherently an email device. In order to not lose ground in functionality most agencies started with this use case. With current generation of MDM technology, email is not required for Phase I though it is typically associated.

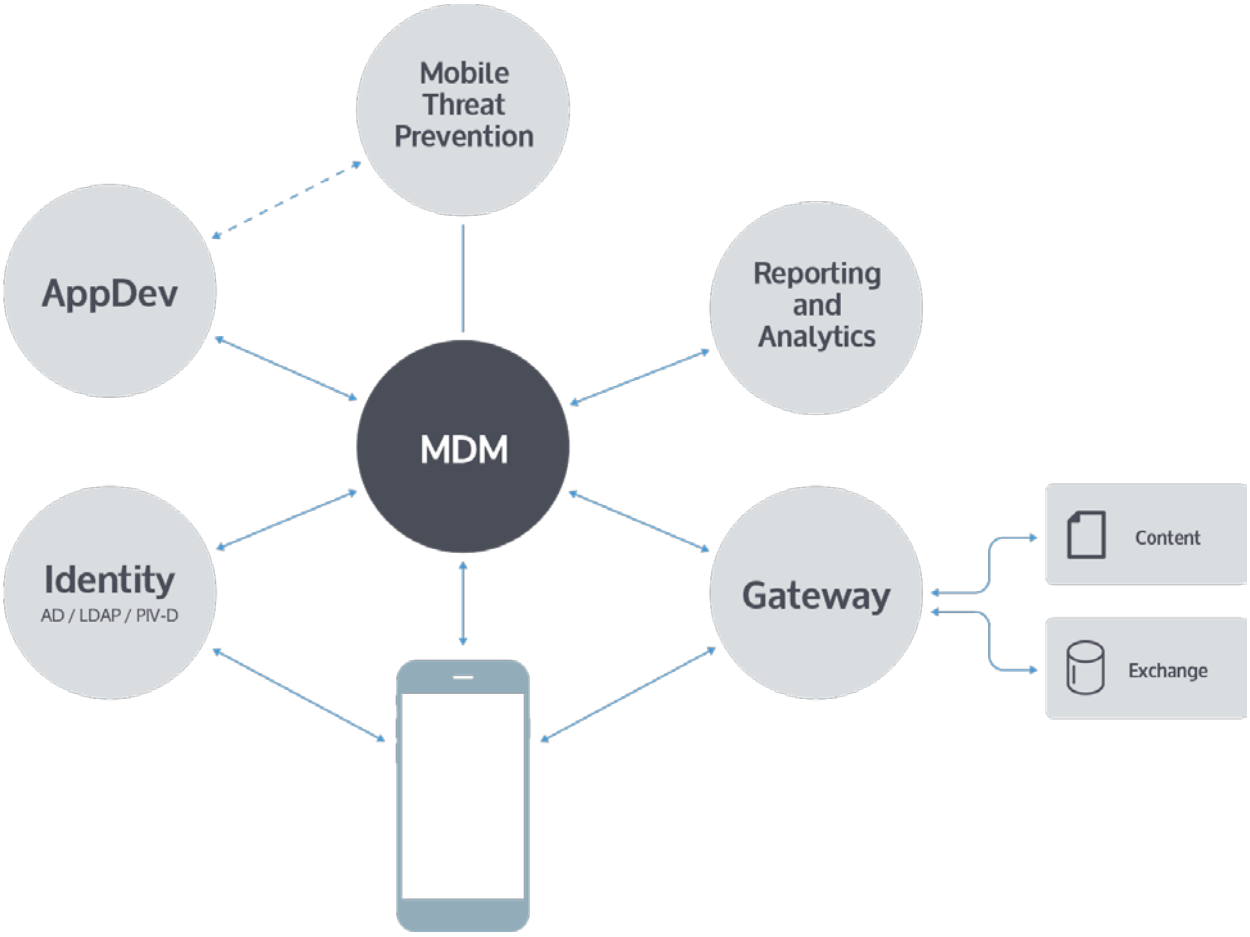
PHASE II – MDM Architectural Diagram



Phase II Application deployment and development

Description:
Phase 2 of most MDM/EMM deployments were extending the basic use case, first application email by providing additional mobile applications to solve business need. The first sets of applications tended to be 3rd party applications, already available from the public app stores for immediate use and deployment. Some agencies started focusing on early stage app development. This first pass tended to be focusing on web apps or hybrid apps that could be developed once and run across the mobile platforms (iOS, Android and in some small cases Windows).

PHASE III – MDM Architectural Diagram



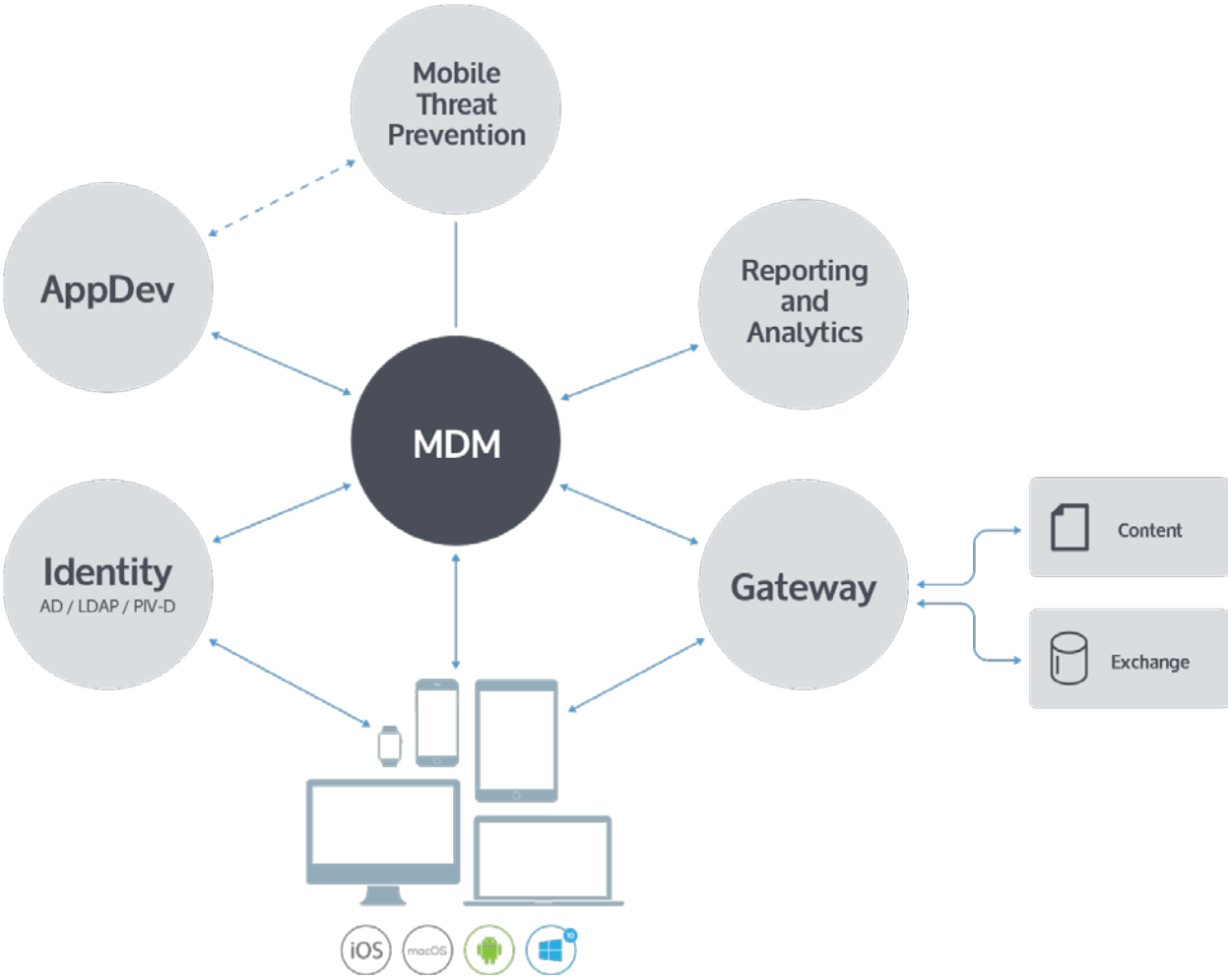
Phase III Comprehensive MDM Solution – Enterprise Deployment

Description:

The natural evolution of MDM/EMM was to become the defector end point management solution as the end-point operating systems become more mobile and coalesced around iOS, Android and Windows 10. The new modern OS architectures provided for management primitives (MDM) to integrate this management into the OS itself. Since this provided a stronger security model this has been adopted across the board. At this phase MDM/EMM became/becomes the primary management model. Since this management paradigm was designed to be hub-spoke, with the MDM/EMM at the center, at this phase integrations with MTP (Mobile Threat Prevention) technologies and existing enterprise IT systems such as identity leveraging PIVD becomes more important, even critical. Tie this to

other systems such as SEIMS (Splunk, Arcsight, etc.,) brings MDM/EMM into the overall enterprise IT ecosystem.

PHASE IV – MDM Architectural Diagram



Phase IV Fully realized UEM (Unified End Point Management) Solution

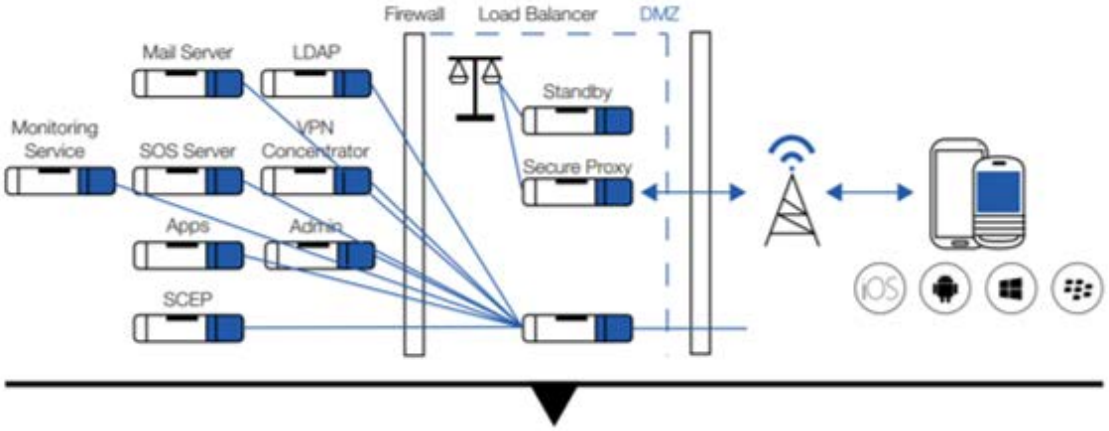
Description:

The natural evolution of MDM/EMM was to become the defector end point management solution as the end-point operating systems become more mobile and coalesced around iOS, Android and Windows 10. The Final phase is to encompass traditional management paradigms for the purpose of a full management lifcyle system. By supporting some legacy

controls in windows (Windows 10 offers both modern and legacy controls whereby the legacy controls will be eliminated over time) and by also supporting MacOS, EMM can be applied to management all modern end points. With it's sophisticated continiuous montoriring and control and with integration into modern threat platforms, this gives agencies a robust system and "single pane of glass" for all their end point needs.

MDM Architecture

A number of architectures were presented in the previous sections. This graphic shows another way of installing and configuring management systems in an enterprise.



MDM Vendors

The following vendors offer mobility management solutions.

MDM - Vendors		
Vendor	**Platform**	**Product**
VMware	Airwatch	Agent (MDM), Container, Catalog, Inbox, App Wrapping, Browser, Content Locker View, VMware Identity manager, Telecom, Content Locker Collaborate
Mobileiron	Mobile Iron EMM Platform	Core, Sentry, Apps@Work, AppConnect, Docs@Work, Web@work, Help@work, Tunnel, Identity@Work (Kerebos Proxy), Dataview, Bridge – Win10 Legacy support, Access – Conditional Controlled Cloud
Microsoft	Intune	Azure portal, AD integration, Office 365, Microsoft enterprise mobile apps
Blackberry	BlackBerry Unified Endpoint Manager (UEM)	BlackBerry Work, Connect, Share, Tasks, Notes, Docs To Go, Access, BlackBerry Dynamics, BlackBerry 2FA, Enterprise Identity, BBM Enterprise, BBM Enterprise SDK, Analytics, SecuSmart, BlackBerry WorkLife,
Samsung	SDS EMM	SDS EMM hosted in EC2 or on premises, KNOX premium app, SDS EMM application
IBM	MaaS360	Mobile Device, App, Content, Threat, Identity Management; Secure Container w eMail, Browser and Content Editor; Unified Endpoint Management; Cognitive Analytics

Standards and Best Practices

The following are relevant standards, best practices, and guidelines in this area.

- NIST SP 800-124 Rev 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise [2]
- NIST SP 800-164 (Draft): Guidelines on Hardware-Rooted Security in Mobile Devices [3]
- NIST SP 800-147: BIOS Protection Guidelines [4]
- NIST SP 800-155: BIOS Integrity Measurement Guidelines [5]
- NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization [6]
- NIST SP 800-163: Vetting the Security of Mobile Applications [7]
- NSA Mobility Capability Package 2.3 [8]
- Department of Defense Commercial Mobile Device Implementation Plan [9]
- CIO Council: Digital Government Strategy Government Mobile and Wireless Security Baseline [10]
- GSA Managed Mobility Program Request for Technical Capabilities [11]
- NIAP Protection Profile for Mobile Device Management Version 1.1 [12]
- NIAP Protection Profile for Mobile Device Fundamentals 2.0 [13]
- NIAP Protection Profile - Extended Package for Mobile Device Management Agents [14]
- Global Platform Specifications for Secure Element and Trusted Execution Environment [15] [16]
- Trusted Computing Group specifications for Trusted Platform Module [17]

Conclusions

To ensure mobile devices conform to the requirements, organizations should develop, communicate, and implement a top-tier EMM/MDM. To mitigate risks most MDMs allow for remediation and communication to devices connected to the enterprise. MDM distribution shall also considered with customer user groups on how they will manage and publish mobile applications. Secondly, procurement of EMM/MDM suites where security is paramount shall also be taken into consideration. Finally, another recommendation is to always discuss your MDM strategy with early with peers and stakeholders to receive feedback from the line of business.

Appendix A – References

[1] NCCoE, *Mobile Device Security for Enterprises*, September 2014. http://nccoe.nist.gov/sites/default/files/nccoe/MobileDeviceBuildingBlock_20140912.pdf [accessed 8/23/15]

[2] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST SP 800-124 Revision 1, NIST, June 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 8/23/15].

[3] L. Chen, J. Franklin, and A. Regenscheid, *Guidelines on Hardware-Rooted Security in Mobile Devices (DRAFT)*, NIST SP 800-164 (DRAFT), NIST, October 2012. http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf [accessed 8/23/15].

[4] D. Cooper et. al., *BIOS Protection Guidelines*, NIST SP 800-147, NIST, April 2011. http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf [accessed 8/23/15].

[5] A. Regenscheid and K. Scarfone, *BIOS Integrity Measurement Guidelines (DRAFT)*, NIST SP 800-155 (DRAFT), NIST, December 2011. http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf [accessed 8/23/15].

[6] R. Kissel et. al., *Guidelines for Media Sanitization*, NIST SP 800-88 Revision 1, NIST, December 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf [accessed 8/23/15].

[7] S. Quirolgico et. al., *Vetting the Security of Mobile Applications*, NIST SP 800-163, NIST, January 2015. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf [accessed 8/23/15].

[8] NSA, *Mobility Capability Package 2.3*, Enterprise Mobility Version 2.3, November 2013. https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_3.pdf [accessed 8/23/15].

[9] Department of Defense (DoD), *DoD Commercial Mobile Device Implementation Plan*, February 15, 2013.

http://archive.defense.gov/news/DoDCMDImplementationPlan.pdf [accessed 9/3/15].

[10] CIO Council, *Government Mobile and Wireless Security Baseline*, May 23, 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf [accessed 8/23/15].

[11] CIO Council, *Government Mobile and Wireless Security Baseline*, May 23, 2013. https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf [accessed 8/23/15].

[12] NIAP, *Protection Profile for Mobile Device Management Version 2.0*, December 2014. https://www.niap-ccevs.org/pp/pp_mdm_v2.0.pdf [accessed 8/23/15].

[13] NIAP, *Protection Profile for Mobile Device Fundamentals Version 2.0*, September 2014. https://www.niap-ccevs.org/pp/pp_md_v2.0.pdf [accessed 8/23/15].

[14] NIAP, *Extended Package for Mobile Device Management Agents Version 2.0*, December 2014. https://www.niap-ccevs.org/pp/pp_mdm_agent_v2.0.pdf [accessed 8/23/15].

[15] Global Platform, GlobalPlatform made simple guide: Secure Element. http://www.globalplatform.org/mediaguideSE.asp [accessed 8/23/15].

[16] Global Platform, GlobalPlatform made simple guide: Trusted Execution Environment (TEE) Guide. https://www.globalplatform.org/mediaguidetee.asp [accessed 8/23/15].

[17] Trusted Computing Group, TPM Main Specification. http://www.trustedcomputinggroup.org/resources/tpm_main_specification [accessed 8/23/15].

[18] The White House, *Bring Your Own Device - A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*, August 23, 2012. https://www.whitehouse.gov/digitalgov/bring-your-own-device [accessed 8/23/15].

[19] National Institute of Standards and Technology, *Managing Information Security*, NIST SP 800-39 Revision 1, NIST, March 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf [accessed 11/14/16].

[20] National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37 Revision 1, NIST, February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf [accessed 11/14/16].

[21] United States Computer Emergency Readiness Team, *Cyber Threats to Mobile Devices*, Technical Information Paper-TIP-10-105-01, US-CERT, April 2010. https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf [accessed 8/27/15].

[22] Delugré, Guillaume, *Reverse engineering a Qualcomm baseband*, Sogeti / ESEC R&D, 2011. https://events.ccc.de/congress/2011/Fahrplan/attachments/2022_11-ccc-qcombbdbg.pdf [accessed 8/27/15].

[23] United States Computer Emergency Readiness Team, *A Glossary of Common Cybersecurity Terminology*, 2015. https://niccs.us-cert.gov/glossary [accessed 8/28/15].

[24] National Institute of Standards and Technology, *National Vulnerability Database*, 2015. http://nvd.nist.gov [accessed 9/2/2015].

[25] L. Badger et. al., *Cloud Computing Synopsis and Recommendations*, NIST SP 800-146, NIST, May 2012. http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf [accessed 9/2/15].

[26] Microsoft, *Protect data using mobile application management policies with Microsoft Intune*, Microsoft Technet, August 13, 2015.https://technet.microsoft.com/en-us/library/dn878026.aspx [accessed 9/2/15]

[27] Microsoft, *Windows Phone 8.1 Security Overview*, Windows Phone, April 2014. http://download.microsoft.com/download/B/9/A/B9A00269-28D5-4ACA-9E8E-E2E722B35A7D/Windows-Phone-8-1-Security-Overview.pdf [accessed 9/2/15].

[28] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Security*, Version 1.0, February 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 9/9/15].

[29] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4,

April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 9/9/15].

[30] International Organization for Standardization and International Electrotechnical Commission, Information technology - Security techniques - Code of practice for information security management., ISO/IEC 27002, 2013.

[31] Council on CyberSecurity, *The Critical Security Controls for Effective Cyber Defense*, Version 5.0, 2013. https://www.sans.org/media/critical-security-controls/CSC-5.pdf [accessed 9/9/15].

[32] Google, *Protect against harmful apps*. https://support.google.com/accounts/answer/2812853?hl=en [accessed 10/20/15]

[33] Lookout, *Change to sideloading apps in iOS 9 is a security win*. https://blog.lookout.com/blog/2015/09/10/ios-9-sideloading/ [accessed 10/20/15]

[34] Microsoft, *Try it out: restrict Windows Phone 8.1 apps*. https://technet.microsoft.com/en-us/windows/dn771706.aspx [accessed 10/20/15]

[35] National Institute of Standards and Technology, *Electronic Authentication Guideline (Public Preview)*, NIST SP 800-63-3, May 2016. https://pages.nist.gov/800-63-3.

[36] National Institute of Standards and Technology, *Best Practices for Privileged User PIV Authentication*, NIST Cybersecurity White Paper, April 2016. http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf. [accessed 5/4/16]

[37] FedRAMP, *Program Overview*. https://www.fedramp.gov/about-us/about. [accessed 5/4/16].

[38] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NISTIR 8062, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2017, 49pp. https://doi.org/10.6028/NIST.IR.8062

Appendix B – Glossary

2FA	Two-Factor Authentication
AD DS	Active Directory Domain Services
AD FS	Active Directory Federation Services
AD	Active Directory
ADAL	Active Directory Authentication Library
BYOD	Bring Your Own Device
CAG	Consensus Audit Guidelines
CIO	Chief Information Officer
CSF	Cybersecurity Framework
DNS	Domain Name System
DoD	Department of Defense
EMM	Enterprise Mobility Management
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IPC	Inter-process Communication
ISO	International Organization for Standardization
IT	Information Technology
MAM	Mobile Application Management
MCM	**Mobile Content Management**
MDM	Mobile Device Management
MDS	Mobile Device Security
MIM	**Mobile Identity Management**
MTP	Mobile Threat Protection
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partnership
NIAP	National Information Assurance Partnership

Mobile device management (MDM)

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OS	Operating System
PIV	Personal Identity Verification
SaaS	Software as a Service
SANS	Sysadmin, Audit, Networking, and Security
SCCM	Systems Center Configuration Manager
SP	Special Publication
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
US-CERT	United States Computer Emergency Readiness Team
WAP	Web Application Proxy

MOBILE SERVICES CATEGORY TEAM (MSCT)

Enterprise Mobility Management

MDM/MAM/MCM

Functional Requirements Document - FRD

1 Introduction

1.1 Background

The Federal Government is becoming increasingly reliant upon mobility, now with approximately 1.5 million mobile devices in service costing the government over $1 billion annually for service alone. Mobility usage across the government has a wide range of diverse profiles from general business use to mission critical, high security. There is an increasing need for the Federal Government's mobile device management processes to be further improved due to increased security risks and broader use of mobile solutions.

The Category Management Leadership Council (CMLC) and the Office of Management and Budget (OMB) established and began the implementation of a Category Management strategy across the federal government identifying 19 Common Government Spending Categories. In 2016, OMB established the Mobile Services Category Team (MSCT), made up of Agency representatives across the Federal Government, to address cross-government requirements for next generation mobility. The MSCT is tasked with, among other responsibilities, establishing requirements for both core and sub-components of mobility. As such, it is the responsibility of the MSCT to establish the minimum baseline Enterprise Mobility Management requirements.

The primary purpose of this document is:

- State the minimum set of requirements across the Federal Government for Mobile Device Management, Mobile Application Management, and Mobile Content Management under the broader umbrella of Enterprise Mobility Management (EMM)

This document establishes minimum EMM requirements government-wide. Individual agencies determine the full extent of requirements for their respective device management, security needs, and mobility software. Within this context, it is also important for the Federal Government to continue to reduce costs and both improve and simplify the acquisition process for mobility and related services.

This requirements document includes documentation from the previous Managed Mobility RFTC solicitation in 2013 as well as a previous Department of Homeland Security 2015 DHS mi-5 Enterprise Mobile Device Management Baseline Initiative Report. The DHS report development included a thorough process of documenting and assessing DHS Component Agency needs and requirements for MDM and app management to establish an Enterprise MDM Baseline.

This FRD differs from the DHS mi-5 Enterprise Mobile Device Management Baseline Initiative Report in that the DHS report has a primary focus upon MDM and security due to its purpose of addressing DHS managed devices. The requirements identified within the FRD included more in the areas of MAM and MCM. The intent of this document is to provide a broad approach and minimum requirements across MDM, MAM and MCM. However, it would be both a redundancy in process and inefficient use of resources not to use findings from the DHS report and the RFTC to establish government-wide EMM requirements. Government agencies that

contributed requirements information to the DHS baseline included CBP (Customs and Border Protection), FEMA (Federal Emergency Management Administration), ICE Immigration and Customs Enforcement, HQ CISO (Headquarters – Chief Information Security Officer), HQ ITSO (Headquarters - Information Technology Services Office), TSA (Transportation Security Administration), USCG (United States Coast Guard), and USCIS (United States Citizenship and Immigration Services).

This document has three primary components as a part of the Enterprise Mobility Management (EMM) across the Federal Government:

1) Mobile Device Management (MDM)
2) Mobile Application Management (MAM)
3) Mobile Content Management (MCM)

This document also specifies a set of optional services contained within each.

The EMM solutions must meet a broad set of requirements that address the following set of criteria:

A. Qualified Secure, Scalable Solutions – Technical solutions that address the existing mobile device, application, and content management needs of government mobile technology including minimum level security and policy management. The solutions shall have the ability to scale to the extremely large and evolving nature of federal government cabinet-level agency organizations.

B. Evolutionary and Flexible – The management needs of the Federal Government Mobility are evolving with increased mobile adoption, new mobile applications, enhanced needs for remote access, and emerging policy and security requirements in an increasingly threatening external environment. As a result, the solutions will continue to assess future requirements to ensure the ongoing Federal Government needs of MDM, MAM, and MCM are adequately met. The MSCT intends to re-assess both the Enterprise Mobility Management requirements and solution providers on a periodic basis in response to mobility evolution. This will provide government agencies with on-going, updated qualified solution providers.

C. Shared Mobility Community – The solution providers are expected to monitor and bring forth new industry developments, identify Managed Mobility best practices in both industry and government, and to present these best practices to government. The Managed Mobility space is in a state of rapid change, making it challenging and resource-intensive for agencies to stay properly informed and to adequately maintain and manage mobility within their respective agencies.

By centralizing requirements gathering, establishing government-wide minimal requirements, and conducting solution assessments; the MSCT intends to reduce the burden on agencies while increasing the quality of their options.

1.2 Objective

The Federal Government must address agency's mission needs in a secure, cost-effective manner. This objective is driven by the MSCT as directed by The Office of Management and Budget (OMB). Enterprise Mobility Management is a core capability for effectively scaling the secure deployment and management of mobile devices, mobile applications, enterprise data on mobile devices, mobile security, and mobile platforms themselves. The optimal balance between security, total costs and functionality will provide the most business value to government agencies.

The MSCT defines the functional framework, and Government agencies should be able to work with all components of the framework seamlessly in an easy to use, secure, integrated solution. For example, if a user reports losing a device, the IT device manager should be able to enter the user name, retrieve the device ID, disable it, and notify the network provider to stop service and billing – all within a single interface. A proposed mobility solution set may incorporate multiple tools due to the complexity of the requirements and the rapid evolution of the managed mobility marketplace.

Since mobile security covers a broad spectrum of requirements and services, this document does not specifically include mobile security as a standalone set of requirements except as it pertains to the securing of devices through MDM and data through MAM and MCM.

1.3 Approach to EMM -- MDM/MAM/MCM Acquisitions

This requirements document identifies EMM (MDM/MAM/MCM) platform(s) capable of satisfying the government's device, applications, and content management needs specified and developed by the Mobility Services Category Team. It is recommended that individual agencies use this set of minimum guidelines, add any additional requirements to meet specific needs of their respective Agency and then, obtain provider information and capabilities to meet the entire set of MDM, MAM, and MCM needs. When agencies obtain information and capabilities from service providers it is also recommended that Agencies request that the providers map their offerings to the government acquisition vehicles to streamline the acquisition process.

1.4 Overview

Enterprise Mobility Management, as previously stated, is a service portfolio of mobile device management, mobile application management, and mobility content management. The baseline requirements of each are shown separately under their respective category headings and subsections.

1.5 Solution Security

While security is not a specific requirement category to itself for the purposes of this requirements document, security is both implied and evident within many of the individually stated technical requirements. Security must be addressed through data at rest encryption, data in transit encryption (VPN), and secure applications, which are included in the requirements for the

EMM: MDM-MAM-MCM solution. The solution requirements may be met through separate products, which are then integrated into the complete EMM: MDM-MAM-MCM solution.

1.6 Solution Requirements

1.6.1 Mobile Device Management (MDM)

1.6.1.1 MDM Detailed Requirements

MDM refers to device management and other mobile management functions that control the mobile device and the activities that may be performed on the device. It is recognized that MDM may be on the device or in some product frameworks may also be in the cloud.

Below is a set of detailed MDM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be evaluated by Agencies in assessing their overall needs.

Table 2.5.1

#	MDM Requirement	Priority
1	The solution shall offer support for the use of Microsoft Active Directory (AD) as its user information repository (This is a specific DHS requirement; There may be different repositories also to be supported for other Agencies)	C
2	The solution shall be capable of connecting to and using multiple AD forests for different user populations.	C
3	The solution shall support a Role-based Access Control (RBAC) model whereby users are assigned roles, which authorize them to perform non-privileged (e.g., user self-service) or privileged (e.g., device enrollment, policy definition, or view usage, logs, and GPS data) actions.	C
4	The solution shall support the automated assignment of roles to users based on group memberships in an enterprise Lightweight Directory Access Protocol (LDAP) directory service.	C
5	The solution shall offer support for policies to control native device screen capture capabilities.	C
6	The solution shall support a “de-centralized” administration model, whereby administrators may be granted administrative privileges within a limited scope or partition of the system (e.g., enabling control of an organizational unit within the organization).	C

#	MDM Requirement	Priority
7	The solution shall support policies to lock or automatically erase all or select enterprise data from the device under the following conditions: • The device is running an unsupported operating system or version • The user has exceeded a threshold of failed authentication attempts • The device has not contacted the MDM server for a configurable time interval • The device OS has been compromised or "jailbroken" • The device is in violation of configuration policies • The device is in violation of configuration policies For container solutions, deletion of the container storage is sufficient. Removable storage must also be wiped, unless the solution provides other safeguards preventing the storage of enterprise data on removable devices.	C
8	Both the MDM server and enrolled mobile devices must display the required system use notification banner to all users attempting to authenticate to the system.	C
9	The solution shall support policies to configure an inactivity lock interval for the device screen (or the container) after which the user will be required to re-authenticate.	C
10	The solution shall support policies to control the display of message/alert notifications on the device lock screen.	C
11	The solution shall allow the user to place emergency calls (e.g., 911) without unlocking the device.	C
12	The solution shall support one or more remote access mechanisms such as a VPN (provided either device-wide or to apps within a container) or an access gateway provided by the MDM server.	C
13	The solution shall support policies requiring the use of VPN for packet data. For whole-device solutions this should apply to all network traffic sent by the device; for container solutions, it should apply only to apps inside the container.	C
14	The solution shall offer support for policies to disable cellular data connections.	C
15	The solution shall offer support for policies to disable Wi-Fi.	C
16	The solution shall offer support for policies to disable Bluetooth.	C
17	The solution shall offer support for policies to disable wireless access point ("hotspot") functionality. *(Note: Security requirement added to baseline)*	C
18	The solution shall offer support for policies to configure Wi-Fi security settings, including specifying known enterprise networks, provisioning network credentials, and selecting supported wireless security protocols.	C
19	The solution shall offer support for policies to restrict the use of Bluetooth profiles and to require the use of encrypted Bluetooth connections.	C
20	The solution shall offer support for the grouping of devices into logical groups, and the application of policies and other security settings to devices based on these groups.	C
21	The solution shall support policies to require specific apps (e.g., anti-malware) to be installed on registered devices.	C

#	MDM Requirement	Priority
22	The solution shall provide at-rest encryption of data stored on enrolled devices either by encrypting all local storage, or through the use of an encrypted container protecting all enterprise applications and data.	C
23	The solution shall provide the ability to monitor and restrict the use of OS-native cloud-based data storage, backup, and synchronization services.	C
24	The solution shall support the configuration of profiles by user group/role and assignment of policies and apps specific to that role.	C
25	The solution shall support configuration of allowed user remote self-service actions including the ability to lock, locate, track, and wipe content on the user's device.	C
26	The solution shall create audit records of security-relevant actions on the device, to include password changes, failed authentication attempts, and connections to enterprise resources.	C
27	The solution shall create audit records of access to the administrative console and all administrator actions such as policy definition and modification, manual requests to wipe devices, and modifications to device and user information.	C
28	Audit records shall contain at a minimum the event ID, timestamp, location information, event source, event description, and identity of the device and, if known, the user.	C
29	To enable event log correlation, the solution shall support synchronizing both the MDM server(s) and managed devices with agency designated Network Time Protocol (NTP) server.	C
30	The solution shall control access to audit records in order to preserve the confidentiality and integrity of audit data.	C
31	The solution shall protect logs against unauthorized modification (e.g., through the use of digital signatures).	C
32	The solution shall protect the confidentiality and integrity of audit records and reporting information transmitted from devices to the MDM server.	C
33	The solution shall meet all security control requirements of the Digital Government Strategy Federal Mobile Computing Security Baseline. While many controls will depend on implementation details and not be provided directly by the solution, the design of the solution must not preclude or impede implementation of any of the baseline controls.	C
34	If the solution is provided as a cloud service offering, it must be granted an Approval to Operate (ATO) through the GSA FedRamp program.	C
35	The solution shall produce hardware and software asset inventory reports for enrolled devices.	C
36	The solution shall monitor devices and report compliant and non-compliant settings to the MDM server. The solution shall automatically configure the defined settings to the extent possible.	C
37	The solution shall support identifying devices that have not reported to the MDM server in a configurable time period.	C

#	MDM Requirement	Priority
38	The solution shall support automated installation of required apps on registered devices, and if possible prevent end-users from removing them. *(Note: Security requirement added to baseline)*	C
39	The solution shall support configuration policies for devices' native web browser to control security settings such as password storage and form auto-fill.	C
40	The solution shall support detailed reporting for enrolled devices to include compliant and non-compliant settings, OS and MDM agent versions, installed apps, and changes to configuration or installed apps.	C
41	The solution shall support policies restricting access to enterprise services based on compliance status.	C
42	The solution shall offer support for policies to disable voice-activated query features such as Apple's Siri, Google Now, and Microsoft Cortana.	C
43	The solution shall offer support for policies to disable location services.	C
44	The solution shall offer support for policies to disable device cameras.	C
45	The solution shall offer support for policies to disable device microphones.	C
46	The solution shall offer support for policies to disable infrared communications.	C
47	The solution shall offer support for policies to disable removable media (e.g., MicroSD) ports.	C
48	The solution shall offer support for policies to disable General Purpose Input/Output (GPIO) pins.	C
49	The solution shall support policies to disable debugging.	C
50	The solution shall be able to report the installation status of required apps on registered devices.	C
51	The solution shall support tracking devices by geolocation.	C
52	The solution shall support policies restricting access to enterprise services based on the device hardware, OS, or MDM agent version.	C
53	The solution shall support restricting enrollment based on device model, OS version, IMEI, Serial Number, or UDID.	C
54	The solution shall support/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, with synchronization of files and data between the device and file servers through an encrypted connection	C
55	The solution shall support configuration policies for devices' native web browsers to restrict access to websites using blacklists/whitelists and content rating.	C
56	The solution shall protect the confidentiality and integrity of device backups.	C
57	The solution shall provide OTA reset and reprovisioning of a locked or compromised mobile device.	C
58	The solution's administration interface shall authenticate MDM administrators through one of the following mechanisms: client Transport Layer Security (TLS) authentication using a Personal Identity Validation (PIV) card, acceptance of a Security Assertion Markup Language (SAML), or Integrated Windows Authentication.	C

#	MDM Requirement	Priority
59	Solutions that manage the entire mobile device must require device users to enter a password or Personal Identification Number (PIN) in order to unlock the device when the screen has been manually locked, after automatic lock due to inactivity, and after initially booting the OS.	C
60	Container solutions must require device users to enter a password or PIN in order to access any apps in the secure container.	C
61	The solution must include support for authentication of users to back-end agency applications and services including SharePoint and other web applications.	C
62	The solution must be integrated with the enterprise PKI for the purposes of Non-Person Entity (NPE) certificate authentication of the mobile device throughout the certificate lifecycle, to include provisioning and revocation.	C
63	The solution shall provide mutually authenticated communications between devices and the MDM services, including during initial device enrollment.	C
64	The solution must enable administrators to remotely reset device passwords/PINs, as well as any profile passwords used to prevent users from removing device profiles.	C
65	The solution shall be capable of managing the cryptographic keys and X.509 certificates on enrolled devices, including the provisioning of keys and certificates to the device and deletion of keys and certificates. Provisioning of client certificates may involve key generation on the device and submission of a Certificate Signing Request (CSR) to a Secure Certificate Enrollment Protocol (SCEP) server or proxy, or the provisioning of keys and certificates to the device in an encrypted file container (e.g., P12 file).	C
66	The solution must support policies governing the length, complexity, age, and reuse of passwords/PINs. For container solutions, these rules should apply to the container password.	C
67	The solution shall support multi-factor authentication of device users to enterprise services such as e-mail and back-end applications through the use of cryptographic credentials. This may be accomplished through a device key and issued certificate unlocked by the user's PIN or password that is used to authenticate to the MDM server, or through PKI credentials issued to the user and provisioned to the mobile device (i.e., derived credentials).	C
68	All solution components including the MDM server and any device agent must perform certificate validation including trusted path validation and revocation checking using Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP). Certificate status information may be cached only until its expiration period.	C
69	The solution must not transmit passwords in plain text.	C
70	The solution must not store passwords in plain text.	C
71	The solution must support policies defining a timeout for cached keystore or smart card passwords between 15 and 120 minutes.	C
72	The solution must mask passwords during entry in the administrative interface, and must also support policies requiring password masking on enrolled mobile devices.	C

#	MDM Requirement	Priority
73	The solution shall ensure that the keystore is password protected. Solutions using the OS native keystore must also support policies to ensure that the device password is set and meets policy requirements. Solutions providing their own keystore implementations must use FIPS 140-2 validated libraries and encrypt the keystore using a key securely derived from the keystore password.	C
74	The solution shall flush encryption keys and decrypted data from device memory when the device or container is locked, except for decrypted data needed by background processes.	C
75	The solution shall support policies to configure the network proxy settings for enrolled devices.	C
76	All solution components creating or validating digital signatures must support the use of Secure Hash Algorithm 2 (SHA-2) digital signatures.	C
77	All components of the solution that perform cryptographic operations must use FIPS 140-2 validated cryptographic libraries.	C
78	The solution shall control the cryptographic algorithms used for e-mail encryption and digital signatures.	C
79	The solution shall be capable of managing the trusted Certificate Authority certificate stores on mobile devices.	C
80	The solution must provide a mechanism to encrypt removable storage devices (e.g., Micro Secure Digital [MicroSD] cards) attached to enrolled mobile devices, unless the solution provides other safeguards preventing the storage of enterprise data on removable devices.	C
81	The solution shall require user authentication to the device before decrypting enterprise data.	C
82	The solution shall be capable of advertising and pushing updates and patches to mobile OSs, MDM agents, and enterprise apps.	C
83	The solution must be able to integrate with the enterprise Security Event and Incident Management (SEIM) systems, including the ability to export audit events in standard formats.	C
84	The solution shall check the integrity of the device to detect whether it has been compromised or “jailbroken.” Detection should include checking for common indicators of rooted devices (e.g., superuser utilities).	C
85	The solution shall check the integrity of the device to detect whether it has been compromised or “jailbroken.” Detection should include periodic validation of key files and processes.	C
86	Container solutions shall provide mechanisms to protect the integrity of the container and detect tampering by compromised OSs and applications operating outside the container.	C
87	The solution shall support policies restricting access to enterprise services based on OS integrity compromise.	C
88	The solution shall employ encryption to protect the confidentiality and integrity of configuration profiles, commands, and software updates transmitted to devices from the MDM server.	C

#	MDM Requirement	Priority
89	The solution shall check the integrity of the device to detect whether it has been compromised or "jailbroken." Detection should include the use of a secure boot process and verification of its integrity.	C
90	The solution shall provide a single, integrated management console to create, update, and manage policies and apps for all managed devices.	C
91	The solution shall provide Document Editing for common file formats (PDF, MS Word, MS Excel, etc.) for managed applications and services.	C
92	The solution shall provide data loss prevention capabilities	C
93	The solution shall provide Over The Air (OTA) device provisioning	C
94	The solution shall provide Over The Air (OTA) registration and enrollment of devices to the MDM.	C
95	The solution shall support mobile devices with the following operating systems: MS Windows Phone 8.x and later, Apple iOS 8.0 and later, Google Android 4.0 and later	C
96	The solution shall interoperate with Agency EaaS	C
97	The solution shall provide OTA re-provisioning of mobile devices for issuance to a different user.	C
98	The container solution shall support policies that limit collection of personal information and app data stored outside the managed container.	C
99	The solution shall support user-initiated password reset requests for managed apps and services.	C
100	The solution shall support the Department's hierarchical organizational structure within the solution, and support multiple configurations for each MDM requirement	C
101	The solution shall provide configurable notification alerts to report organization-defined security and non-security events, problems, or issues, and compliance violations to the MDM administrator or Agency management.	C
102	The solution shall provide configurable reports on alerts, usage, and compliance status.	C
103	The solution shall capture, track, and retain pertinent device information, including UID, Serial Number, phone number, and Device Group Assignment.	C
104	The solution shall support scheduled and ad hoc system performance reports. System performance reports include: Concurrent Connections, Number and size of updates, Peak Time Usage, Active/inactive user and device counts, Bandwidth utilization, Authentication processing times, Email/Calendar/Contact sync durations, Connection failure rate to/from device for the MDM system	C
105	The solution shall provide management dashboards for real-time viewing of organization-defined information on devices, usage, device assignments, location, etc.	C

#	MDM Requirement	Priority
106	The solution shall support 10,000 or higher devices per server	C
107	The solution shall support 10,000 concurrent users	C
108	The solution shall support concurrent XX,XXX policy updates	C
109	The solutions shall support concurrent XX,XXX enrollments	C
110	The solution shall support multiple cost models based on use case and rapid addition and removal of devices and users.	C
111	The solution *should* send alerts via e-mail or Short Message Service (SMS) to a configurable set of recipients if the auditing system experiences a failure preventing the generation of audit records.	I
112	The MDM *should* support the reporting in SCAP format [specifically: CPE, CVE, CCE]	I
113	The solution *should* offer support for policies to disable SMS and Multimedia Messaging Service (MMS) messaging. *(Note: Added deferred security requirement.)*	I
114	The solution *should* offer support for policies to disable Universal Serial Bus (USB) tethering. *(Note: Added deferred security requirement.)*	I
115	The solution *should* support configuration policies to control access to media content by content rating.	I
116	The solution *should* create backups of all user and system information on enrolled devices, and provide a mechanism for restoring backed-up data to devices. At minimum, the solution should create backups of all managed apps and information. These backups are limited to device information, and not including PII, email, or application data.	I
117	The solution *should* include support for the retrieval of other enterprise users' S/MIME certificates via LDAP to enable sending encrypted messages to them. *(Note: Added deferred security requirement.)*	I
118	The solution *should* provide configuration profile templates.	I
119	The solution *should* support multiple email/calendar/contact configurations per profile.	I
120	The solution *should* support setting profile start and end dates, and notification to administrator when a profile is expiring and no other profile has been defined to replace it.	I
121	The solution *should* support multiple profiles being applied to a single device.	I
122	The solution *should* support applying multiple policies to a device; when multiple security policies conflict, the most restrictive policy takes precedence.	I
123	The solution *should* support data synchronization between managed devices and allowed file shares and content repositories.	I
124	The file sharing and content repository solution *should* support document viewing functions including search, bookmarks and hyperlinks for common file formats.	I
125	The solution *should* provide the ability to manage select enterprise data for government-owned and non government-owned devices	I
126	The solution *should* allow for a store and forward approach to data access to allow local content to be manipulated and stored in a secure way for automatic upload when network connection is restored.	I

#	MDM Requirement	Priority
127	The solution should provide usage rate information associated with apps hosted in the enterprise App Store.	I
128	The solution *should* support app management workflow to enable Business Units to delegate and authorize the installation of select restricted applications.	I
129	The solution *should* provide tool-tips in app/device to provide on the fly device/app/solution training to users unfamiliar with the solution. *(Note: May be device- or app-specific, not MDM configurable)*	I
130	The solution should allow the enrollment of a device before applying any policy (null policy)	
131	The solution should allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or groups under the MDM	
132	The solution should allow the implementation of controls at either the device or application / content level	
133	The solution should use an existing MDM user attribute repository for enrollment to the new MDM system	
134	The solution shall lock, erase, or reset the device - ('erase' (wipe) pertains to ONLY the managed data on a device under the following conditions: o Blacklisted operating system or version (policy) o Exceeding a set number of failed access attempts to the device or MDM application (policy) o Exceeding defined interval for contacting MDM (policy) o Detection of OS jailbreaking or application tampering (policy) o Any other policy violation o Remote / over the air instruction from MDM (manual)	
135	The solution should provide detailed Inventory tracking capabilities	
136	The solution should provide for the ability to restrict or control local data storage	
137	The solution should enable viewing the current GPS location of a device or logical grouping of devices on a map or to provide other location identification services achieving the same or more.	
138	The solution should Enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities	

#	MDM Requirement	Priority
139	The solution should allow a device to be assigned to more than one user group	
140	The solution should allow viewing of the required applications from the Mobile Application Store (MAS)	
141	View required applications from the Mobile Application Store (MAS)	
142	Support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications	
143	Integrate certificates from the solution's internal PKI system to mobile devices as well as third party public PKI providers.	
144	MDM to perform its functions from within a secure VPN used to transport all enterprise data (i.e.: no MDM control data transported unencrypted across the open internet).	
145	The Solution shall support the following WiFi settings and requirements: - Multiple Wi-Fi configurations for multiple profile's - Manage device Wi-Fi settings via a MDM policy - For a profile: Control Wi-Fi Security Type: None, WEP, WPA/WPA2, Enterprise (any)	
146	The Solution shall support the following VPN settings and requirements: - For a profile: Ability to support multiple VPN configurations for a profile. - For a profile: Support VPN Connection (or Policy) Type: IPSec (Cisco), Juniper SSL, FS SSL, and Custom SSL, etc. - For a profile: Ability to support a VPN connection Proxy for a VPN configuration	

1.6.1.2 Additional MDM Requirement Descriptions

1.6.1.2.1 *FISMA Requirements*

The MDM solution shall be certifiable at a FISMA (Federal Information Security Management Act) Moderate Impact level (NIST SP 800-53 Moderate or DoD 8500.2 MAC II) or higher. The solution may include proof of certification such as NIAP, Accreditation, or Authorization to

Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or Authority-To-Operate (ATO). Agencies should be aware that a service provider might offer two solutions – one that is NIAP compliant, and one that is not NIAP compliant. Each Agency must determine its level of requirements regarding NIAP compliance due to the likely cost differentiation.

1.6.1.2.2 *FIPS Requirements*

Solutions shall protect control and management data in transit between the MDM and the device using FIPS 140 certified cryptographic modules.

It is recommended that agencies request from any potential service provider proof of the solution's FIPS 140-2 certification for cryptographic modules. All encrypted communications must use a cryptographic module certified in accordance with a NIST Certified Cryptographic Module Validation Program under FIPS 140-2, level 1, certification. All solutions must provide evidence of NIST Certified Cryptographic Module Validation Program compliance, or that cryptographic operations in the solution rely on FIPS certified modules in the environment or operating system.

1.6.1.2.3 *Containerization*

Solutions shall have containerization functionality and must describe how the container meets the following requirements:

1. FIPS 140-2 encryption of data at rest
2. Remote and local (action-triggered) secure erasure of container data without impact the rest of the device
3. Protection of container from other applications; because of varying platform capabilities, this must be described on a platform-by-platform basis

Some solutions address data control through the use of containers on the mobile device that serve to separate enterprise and personal data, and protect data from access by uncontrolled applications. This is particularly helpful for Bring Your Own Device (BYOD) scenarios, where the enterprise intends to limit interaction between agency and personal data. This approach is also used to protect data at rest if the underlying platform does not encrypt all data on the device.

1.6.1.2.4 *IPv6 Support*

IPv6 compliance is important for this request. On-premise portions of the MDM solution shall support IPv6 for network communications. Controls on network communications at the device must apply to both IPv4 and IPv6 communications, including VPNs, logging/auditing and network black/white-listing. The solution must provide a description of the IP based components of their solution and the status (compliant or non-compliant) of Solution providers.

1.6.1.2.5 *User Authentication / Web Management*

Solutions for the device must support multi-factor authentication. Solution providers must describe each of the different types of authentication supported by the solution as well as new authentication types in development with rollout over the next 18-24 months. Policy should also be able to enforce a device PIN.

Solution providers must include a web management portal as part of Solution providers, and the web management portal shall be capable of PIV / CAC (or acceptance of a Security Assertion Markup Language (SAML) for primary authentication as indicated in HSPD-12 standards and guidance. Password fallback for specific accounts may be configurable; however they must employ a second factor (SMS, voice response, etc.) to authenticate.
Solution providers shall state how their proposed solution is capable of offering or supporting multi-factor authentication. Multifactor authentication involves authentication with any two of the following three authentication types:

- Shared Secret – PIN or password
- Token – something a user possesses such as a cryptographic key such as an RSA token (soft or hard), a challenge / response token, a PIV or CAC, or a key generator device like UbiKey
- Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, voice, iris or facial image

Additionally, the solution shall provide for installation and configuration (update, revocation checking, revocation) of individual and group soft authentication certificates for the following purposes:

- Email (S/MIME) signing and encryption
- WiFi Configuration
- VPN Configuration

1.6.1.2.6 *User Compliance*

Solution providers must demonstrate the following capabilities. The requirements below are Critical to the solution to enable the:

1. Set up compliance rules to include custom compliance rules for profiles, devices, groups, and whitelist/blacklist
2. Activate / deactivate a compliance rule
3. Specify user and group rules for application compliance, such as required or prohibited applications on a device.
4. Provide enterprise level compliance reports, including lost/wiped/inactive devices, the number of devices total, the number of devices active, how much data is sent/received by devices, connection type

1.6.1.2.7 *Alerts and Notifications*

The following alert and notification capabilities are required to notify agency operations staff about devices under management. Solution providers are to provide a description of each type of alert for which the solution is capable. The solution must demonstrate the following capabilities:

1. Set up custom alerts to users and management based upon various parameters
2. Send custom alerts to one or more user roles including administrators
3. Specify a creation policy for custom alerts to include having various alert severity levels
4. Have automated alerts for security issues such as compromised devices
5. Create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
6. View alerts pending acknowledgement
7. Acknowledge alerts and track acknowledgement
8. Search and run reports on alerts

1.6.1.2.8 *Data Collection*

The solution shall be able to collect and report on the following data:

1. Roaming status
2. Last policy update time
3. Last synchronization time
4. Jailbreak / root status
5. Available program memory
6. Available storage memory

1.6.1.2.9 *Inventory Management*

The solution must include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information. At a minimum the solution should be able to record, track and manage the following information:

1. Device Manufacturer/Model
2. Government Furnished (GFE) or personal (BYOD) device
3. Carrier
4. Wireless Number
5. MAC Addresses
6. International Mobile Equipment Identity (IMEI)
7. SIM module data
8. Storage capacity
9. OS and Version
10. Device up time
11. Encryption Capability
12. User Name
13. Email
14. Phone number
15. Agency information

16. Supervisor contact information

The solution must also have the ability to extend or expand the schema.

1.6.2 Mobile Application Management

1.6.2.1 MAM Detailed Requirements

MAM describes software and services required for the provision and control of mobile applications, which are commercially available through app stores or are available through custom private app stores. These applications must be managed on either government owned or employee owned devices.

Below is a set of detailed MAM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be addressed in the capabilities response.

Table 2.5.2

	MAM Requirements	Priority
1	The solution shall support policies controlling inter-app communication to restrict which apps can share data with each other. In a container-based solution, this may simply entail preventing apps inside the container from communicating with those outside the container and vice versa.	C
2	The solution shall support policies to restrict enhanced location services access to details such as Wi-Fi SSIDs in range.	C
3	The solution shall support policies preventing the installation of apps that do not have a valid cryptographic signature, including the ability to limit installation to apps signed by specific developer keys.	C
4	The solution shall support restricting the use of default apps included with the native mobile OS (e.g., preventing use of the native browser or e-mail client).	C
5	The solution shall support application “blacklist” policies prohibiting the installation of specific apps.	C
6	The solution shall support application “whitelist” policies that identify specific apps that may be installed and prohibiting the installation of all other apps.	C
7	Container-based solutions shall support the use of both whitelist and blacklist policies, such that only whitelisted apps may be installed inside the container and blacklisted apps may not be installed on the device (inside or outside the container).	C
8	The solution shall support policies disabling the use of commercial app stores, permitting devices to install apps from the enterprise app store only.	C
9	If the solution supports PKI credentials, it must provide or incorporate a PKI-enabled web browser.	C

	MAM Requirements	Priority
10	The solution shall provide a mechanism for third-party mobile applications to integrate with MDM capabilities such as authentication, remote access mechanisms, or policy distribution and management. This may be accomplished by providing a Software Development Kit (SDK) or through an app wrapping mechanism. *(Note: Security requirement added to baseline)*	C
11	The solution shall provide an enterprise app store for users to search, access, download, and install authorized iOS, Android, and Windows Phone applications on managed devices.	C
12	The solution shall support single sign on for Agency-developed apps	C
13	The solution shall support role-based access control to the Agency or Government app store.	C
14	The solution shall support management, distribution and update of custom (Agency developed) and commercial apps.	C
15	The solution shall support integration with Apple's Volume Purchase Program	C
16	The solution shall support delegated administration to allow authorized users the ability to view usage, logs and GPS data.	C
17	The solution *should* support policies to restrict enhanced location services access to details such as Wi-Fi SSIDs in range.	I
18	The solution *should* support enterprise single sign on (e.g., SAML, Kerberos, OpenID, SiteMinder)	I
19	The solution *should* include support for the use of S/MIME for e-mail signatures and encryption using a cryptographic smart card or keys and certificates stored in a software keystore. *(Note: Added deferred security requirement.)*	I
20	The solution *should* support integration and secure connections to Agency internal file shares and content repositories (e.g., SharePoint)	I
21	The solution shall support connecting to Agency-approved Secure Instant Messaging application.	I
22	The solution *should* support app development workflow and app management workflow to enable business units to delegate and authorize installation of select applications.	I
23	The solution *should* provide a test environment to assess new applications and new versions of existing applications prior to authorizing applications for use in an Agency production environment.	I
24	The MAM solution *should* support application life cycle management by providing the capability to evaluate, analyze, and manage submitted applications for approval to release to the application store.	I
25	The solution *should* support federated authentication to Agency or Government app store(s) (e.g., to allow access from State & Local partners).	I
26	The MAM solution shall have the ability to manage individual applications without the requirement of having to manage or control the device (e.g. ability to maintain control of applications on employee owned or contractor devices)	TBD
27	The solution shall Identify and detect a compromised application or one that has been threatened with possible or attempted compromise	TBD

	MAM Requirements	Priority
28	The solution shall clearly specify data loss prevention capabilities and enterprise level implementation options of those capabilities	TBD
29	The solution shall provide Application tunneling capabilities – ability for an enterprise to selectively determine which applications have authorization to access enterprise data behind the Agency firewall	TBD
30	The solution *should* allow for User Authentication on a per application basis	TBD

1.6.2.2 Additional Descriptive Mobile Application Management Requirements

1.6.2.2.1 *(Optional) MAM Software Integration Services*

Some Managed Mobility users may require the need for the delivery of new or existing enterprise applications to mobile devices. One example could be making a data entry system accessible to field workers. If your solution supports these capabilities, please describe how this is accomplished.

1.6.2.2.2 *Application Deployment*

The solution shall support the following controls and capabilities for application deployment:

1. Commercial Application Store (iOS App Store, Google Play, etc.) (enable / disable)
2. Reporting of installed applications
3. Blocking application purchase
4. Application whitelisting / blacklisting
5. Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)

1.6.2.2.3 *Mobile Application Store (MAS)*

The solution shall include a Mobile Application Store to allow users to select private enterprise applications for installation on managed devices. This capability must be integrated into the Managed Mobility MDM portal, and allow application provisioning by group policy, and mandatory application deployment.

The MAS should support the following capabilities:

1. Ability to add an application from a Commercial Application Store to the MAS
2. Ability to add an enterprise application to the MAS via a web GUI
3. Ability to add additional metadata to and report on metadata on any application added to the MAS (etc. name, description, version, OS, keywords, etc.)
4. Ability to specify the effective date for an internal application
5. Ability to specify the expiration date for an internal application
6. Ability to specify the minimum operating system and model for an internal application

7. Ability to download internal and public applications from MAS
8. Ability to categorize, group or tag applications (e.g., business applications, scientific applications, etc.)

1.6.2.2.4 *Mutual Authentication*

MDM applications on the device and services must mutually authenticate to ensure the communications channel is not intercepted. The mutual authentication should be certificate-based, with installation-specific certificates deployed to the server during deployment and to the device during provisioning.

1.6.2.2.5 *Application Installation Control*

The solution shall demonstrate the solution's process to support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.

1.6.2.2.6 *Blacklisting / Whitelisting*

The solution shall provide the capability to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting). This capability should be managed through user and group policies.

1.6.2.2.7 *Application Environment Requirements*

The solution shall be able to detect and enforce device environment conditions such as:

1. Minimum or specific operating system versions
2. Required presence or absence of other applications
3. Absence of privilege escalation ("rooting" or "jailbreaking")

1.6.2.2.8 *Application Signing*

The solution should support requiring digital signatures for application installation, from both commercial and private application stores and direct application push / deployment. It is permissible to meet this requirement through OS capabilities.

1.6.2.2.9 *(Optional) Third-Party Application Mutual Authentication*

The MDM solution may offer the ability provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.

1.6.3 Mobile Content Management

1.6.3.1 MCM Detailed Requirements

MCM refers to content management capable of securing, storing, delivering, controlling, and preventing data loss on the mobile device and any transmission of data to or from the mobile device.

Below is a set of detailed MCM requirements, each marked as either Critical (C) – the solution *shall* meet this requirement or Important (I) – the solution *should* meet this requirement or be a future feature of the solution. The detailed requirements are then followed by a series of additional descriptive requirements (indicated as either optional or required), which should also be addressed in the capabilities response.

Table 2.5.3

	MCM Requirement	Priority
1	The solution shall provide Document Editing for common file formats (PDF, MS Word, MS Excel, etc.) for managed applications and services.	C
2	The solution shall provide data loss prevention capabilities	C
3	The solution shall provide for the restriction of downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for agency data and applications from personal data	TBD
4	The solution shall send/receive (Encrypt and Sign, decrypt and verify) messages that use PKI or S/MIME encryption, where email functionality is delivered by the solution	TBD

1.6.3.2 Additional Descriptive MCM Requirements

1.6.3.2.1 *Privacy*

Solution providers shall not display advertisements to end users of the Information System as part of its business model (i.e. not an advertising-based model).

Solution providers shall safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)” and in accordance with M-06-16: Protection of Sensitive Agency Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf and M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf. An Ordering

Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy. An Ordering Activity may request that PII be kept within U.S. Data Centers.

The solution must disclose privacy-impacting features that cannot be disabled.

1.6.3.2.2 *Continuity of Operations and Disaster Recovery*

The solution shall describe how the solution performs Continuity of Operations (COOP) and Disaster Recovery (DR).

1.6.3.2.3 *File Management*

The Government seeks solutions that have the capability to secure data, files, and applications (for example PDF files or word docs) on a mobile device. Devices may be Government Furnished (GFE) or BYOD. The solution must demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a secured space, whether that is within a secured container or secured within the device OS. The solution must also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and file servers.

1.6.3.2.4 *Personal Information Management*

The solution shall demonstrate the solution's ability to support a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities. To ensure that the information is available to other mobile and desktop devices the user may have, as well as for business continuity, backup/restore, and e-discovery purposes, solution providers must be able integrate functionality with a variety of Email, Calendaring and Contact applications, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection. The solution should also demonstrate the solution's PIM capability to support multiple types of Federal Enterprise Email Systems from different vendors. Please identify which on-premise and cloud-based mail systems are supported, such as Microsoft Exchange, Lotus Notes, Gmail, MS 360, Lotus Domino, MS Exchange or Zimbra.

1.6.3.2.5 *Security Content Automation Protocol (SCAP) Support*

SCAP provides the ability to automate security checks and configuration. Solution providers must describe the SCAP support for the server-side components in the solution, including asset management, configuration management, patch management and remediation capabilities. The requirement is only addressing server SCAP support at this time. SCAP for devices is not currently a requirement.

2.5.8 Audit and Reporting Requirements

The solution shall demonstrate the following detailed Audit and Reporting capabilities:

1.6.3.3 Audit and Reporting Detailed Requirements

	Audit and Reporting Requirements	Requirement Category	Priority
1	The solution shall create audit records of security-relevant actions on the device, to include password changes, failed authentication attempts, and connections to enterprise resources.	AUDIT	C
2	The solution shall create audit records of access to the administrative console and all administrator actions such as policy definition and modification, manual requests to wipe devices, and modifications to device and user information.	AUDIT	C
3	Audit records shall contain at a minimum the event ID, timestamp, location information, event source, event description, and identity of the device and, if known, the user.	AUDIT	C
4	To enable event log correlation, the solution shall support synchronizing both the MDM server(s) and managed devices with agency designated Network Time Protocol (NTP) server.	AUDIT	C
5	The solution shall control access to audit records in order to preserve the confidentiality and integrity of audit data.	AUDIT	C
6	The solution shall protect logs against unauthorized modification (e.g., through the use of digital signatures).	AUDIT	C
7	The solution shall protect the confidentiality and integrity of audit records and reporting information transmitted from devices to the MDM server.	AUDIT	C
8	The solution shall produce hardware and software asset inventory reports for enrolled devices.	REPORTING	C
9	The solution shall be able to report the installation status of required apps on registered devices.	REPORTING	C
10	The solution must be able to integrate with the enterprise Security Event and Incident Management (SEIM) systems, including the ability to export audit events in standard formats.	AUDIT	C
11	The solution shall provide configurable notification alerts to report organization-defined security and non-security events, problems, or issues, and compliance violations to the MDM administrator or DHS management.	REPORTING	C
12	The solution shall provide configurable reports on alerts, usage, and compliance status.	REPORTING	C

	Audit and Reporting Requirements	Requirement Category	Priority
13	The solution shall capture, track, and retain pertinent device information, including UID, Serial Number, phone number, and Device Group Assignment.	REPORTING	C
14	The solution shall support scheduled and ad hoc system performance reports. System performance reports include: Concurrent Connections, Number and size of updates, Peak Time Usage, Active/inactive user and device counts, Bandwidth utilization, Authentication processing times, Email/Calendar/Contact sync durations, Connection failure rate to/from device for the MDM system	REPORTING	C
15	The solution shall provide management dashboards for real-time viewing of organization-defined information on devices, usage, device assignments, location, etc.	REPORTING	C

1.6.3.4 Additional Descriptive Audit and Reporting Requirements

1.6.3.4.1 *Device Inventory Reports*

The solution shall demonstrate the capability to run inventory reports. Device Inventory reports includes all data associated with the device, OS and applications. Device reports will be run and/or exported as needed, and will support the following filters:

1. Device Models
2. Operation System and build level
3. Last Access times (access time not compliance check)
4. Application inventory
5. Last Compliance Check
6. Device Compliance (ability to report on rooted/jailbroken devices, policy, etc.)
7. Carrier
8. Network Card IDs (MAC address)
9. Agency Assignment
10. BYOD or GFE (personal device or government furnished)
11. Security Policy Assignment (policy currently applied to device)

1.6.3.4.2 *System Performance Reports*

The solution shall demonstrate the capability to run system performance reports. System performance reports include key performance data to provide insight into the usage of the

devices, reliability of the solution, and performance of devices. System performance reports will be run as needed and will support the following filters:

1. Concurrent Connections
2. Peak Time Usage
3. Total active user and device counts
4. Bandwidth utilization trends
5. End-to-End testing results
6. Authentication processing times
7. Email/Calendar/Contact sync durations
8. Connection failure rate to/from device for the MDM system

1.6.3.4.3 *MDM Security / Compliance Reports*

The solution shall demonstrate the capability to run security/compliance reports. Security reports include all data relevant to the monitoring and support of the system's vulnerabilities and defenses, including attempts at fraud. Security status reports will be run as needed and will support the following data:

1. Non-compliant devices
2. Device wipe actions
3. Passcode reset actions
4. User/Devices with failed authentication
5. Aggregate data on failed authentications
6. Devices with blacklisted applications
7. Jailbroken devices
8. Device anti-virus versions
9. Mobile Management Agent

1.6.3.5 (Optional) Quality of Service (QoS)

The solution should support QoS capabilities to prioritize real-time or latency-sensitive application data where appropriate (e.g.: VoIP, video, real-time chat). The solution should be able to enforce and exclude QoS priority by application or protocol to prevent non-real-time applications from inappropriately increasing their traffic priority.

1.6.3.5.1 *(Optional) Classified Data*

Some Managed Mobility users may require the ability to access classified data up to the SECRET level via mobile devices. If your solution supports these capabilities, please describe how this is accomplished and indicate the specific impact to pricing for this solution, inclusive of exact dollar amounts.

1.6.3.5.2 *PIV / CAC Support*

Solution providers shall offer solutions that support the management of PIV / CAC cards on mobile devices via the MDM.

1.6.3.5.3 *(Optional) Biometric Support*

Agencies with strong authentication requirements may need biometric support such as fingerprint or face recognition with their mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.

1.6.3.5.4 *(Optional) Network Monitoring*

Network Monitoring is the monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise devices).

The solution should include a device application that performs basic diagnostics, such as:

1. Verify network connection and performance
2. Test authentication settings
3. Verify certificates
4. Verify DNS functionality
5. Verify connection to services (mail, MDM, etc.)

1.6.4 Service Delivery Model

The EMM Solution shall be delivered and (optionally) hosted by the Contractor as a full solution including all hardware, software, hosting, and installation services, using one or more of the following hosting models:

1. Cloud Based - For the purposes of this request a Cloud Only solution is a solution that has all HW/SW components of the solution running in a non-government hosted cloud data center. The solution must show how they provide all required hardware to the network edge of their cloud data center. The solution is responsible for all aspects of system and software performance for solution components within their cloud data center.
2. On Premise - For the purposes of this request an On-Premise solution is a solution that has all HW/SW components running completely within federal Government controlled data centers and network. After installation, the Federal Government will be responsible for operating the infrastructure and devices, application store and container management.
3. Hybrid - For the purposes of this request a Hybrid solution is a solution where the components are distributed across federal Government data centers and the solution's

cloud data center. It is anticipated that the solution will provide all required hardware to the network edge of their cloud data center. The solution will clearly describe all HW/SW components that will be within federal Government data center and those components within the solution's cloud data center. The solution would be responsible for all aspects of system and software performance for solution components within their cloud data center.

The Help Desks should be operationally located within the Continental United States (CONUS).

1.7 Support Requirements

1.7.1.1 Project Management

The solution must clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

1.7.1.2 Deployment / Migration / Transition

The solution must clearly describe how they provide initial deployment support services. These services are expected for installing, configuring, and certifying the initial deployment of the MDM, MAM and Container solutions, as well as the ability to support specific agency related integrations or customizations. The solution would assist the agency with achieving accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.

The solution must contain a Transition Plan that details how devices previously supported by the solution will transition from existing service in a quick, reliable, and accurate manner to the offered solution. Staffing requirements (contractor and government) for this Transition Plan must also be identified. Solution providers will receive additional consideration if example transition plans from previous MDM deployments are supplied.

The solution must provide an example of a previous successful on-boarding of 10,000 or more devices. The example must include a high-level timeline, staffing required, and a summary walk-through of the process (1 page maximum for summary walk-through).

The Contractor must also provide an example of an exit transition plan that describes how, in case termination for any reason, delivered data conforms to an industry standard format capable of being transported to other systems.

1.7.1.3 Enterprise Systems Integration

The solution must show how they can be responsible for providing steps necessary for deploying and integrating their Mobility Solution into the enterprise-wide environment. This includes such systems as enterprise email, directories, trouble-ticketing, etc. The steps included are expected to vary dependent upon whether the solution is on-premise or a cloud solution.

1.7.1.4 Training

The Government requires that all users of the MDM-MAM system, which includes end users, administrators and developers, be trained to correctly utilize the system. The solution must demonstrate how they can be responsible for developing and updating the MDM-MAM Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan. The online training may be hosted by the government or the contractor, and the contractor must provide the required content.

1.7.1.5 Help Desk

The solution must provide access to help desk support for their solutions. Please indicate the location of the operational help desk. They must satisfy the following criteria:

1. End User Help Desk support must be 24/7 including holidays.
2. Administrative / Management Help Desk must be available 8am-5pm in both EST and PST.
3. Help Desks must utilize a trouble-ticketing system where each request has a unique identifier for tracking purposes.
4. Help Desk interaction must support online requests / resolution, supported with email.
5. Telephone (voice) Help Desk support must be available, but can be limited to business hours.

1.7.1.6 Demonstration Platform

The solution must possess a demonstration platform to educate potential customers on the use, benefits and technical specification of the solution. Solution providers shall provide access to the portal for the purpose of sampling and demonstrations that will be connected to the solution's site through the OCSIT Innovation Center.

1.7.1.7 (Optional) Enterprise Configuration

This addresses non-core integration, such as Solution connectivity with non-required components (e.g. custom portal, Telecommunications Expense Management System (TEMS) provider system, etc.). Agencies have applications that may be need to be accessed on mobile devices, but that require configuration services to enable. The solution should describe the services they offer of this type. Each configuration service offered must be accompanied by a successful example from industry or government.

1.7.1.8 (Optional) Integration with FSSI Wireless Portal

The FSSI Wireless Business Portal Interface is a secure standard for agencies to interface with cellular carriers to place orders, manage plan/device inventory, and other carrier provided information. The BPI is not a GUI but merely a secure standard for exchanging data between the customer agency and the carrier. Solution providers should indicate their experience and platform's ability with exchanging information with third party providers for the purpose of providing complementary services such as device ordering, logistics, configuration, replacement/refresh, disposal, and disposition reporting

1.7.1.9 (Optional) Telecommunications Expense Management System (TEMS)

TEMS includes a portfolio of purchasing, expense analysis/optimization, invoice payment, reporting (inventory, usage, zero-use identification) and financial functions associated with business communications expense. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure. The solution may demonstrate how their proposed solution addresses order management, ordering via portal, device provisioning, asset management, device asset tracking, non-device asset tracking, account reports, expense management, service plan management, optimization, and expense tracking/reporting. Further the solution may list additional functions that may be of interested to the Federal Government including the ability to pilot a Mobility Management offering to federal customers.

1.7.1.10 (Optional) Device Replacement / Refresh

Device replacement/refresh refers to complementary logistics services where a Contractor may support Government entities with Device replacement and refresh services based on existing government contracts with device providers, carrier or otherwise. The solution may offer logistical support for device replacement, such as pre-enrolling devices at a depot, etc.

1.7.1.11 (Optional) Device Disposal & Reporting

Device Disposal and Reporting refers to the compliant device wiping, destruction, recycling and reporting of mobile devices per government standards (NIST, R2, others) as required per individual agency requirements. The solution provider should indicate experience, willingness, resources, and ability to provide these services.

2 Pricing

When request or evaluate pricing of the solution providers, pricing should be presented on a per device basis – it can be presented in the context of price ranges, pricing tiers based upon volume, pricing based upon pre-defined product configurations or some other scenario or set of scenarios. However, to keep with the purpose of this document and to scale across government, it is strongly suggested that pricing submissions be kept to fairly simple structures so that a cost per device can be easily determined and understood in the context of services delivered.

Pricing may either be customized or may be submitted based upon availability through publicly accessed source. Pricing should be submitted as an integral part of the providers' solution.

Agencies should request that solution providers indicate the range at which their product is sold to their federal customers, inclusive of the discounted rate that is offered to their best federal customer. It is recognized that not every federal customer purchases solutions identically, and often pricing is dependent specific agency needs and requirements. The intent is to indicate the range of potential pricing, subject to the particular requirements that fall beyond the specifications. Additionally, agencies should request a pricing table, which reflects the price structure and currently listed prices for the solutions on Federal contracts/task orders.

For those solution providers offering their solution under IT Schedule 70 the solutions must be on the vehicle and the pricing must correspond to what is found on the schedule. If the solution is offered via a solution's IT Schedule 70 contracts, the solution must currently reside on that contract vehicle to be considered. If the solution cannot be identified on the solution's IT 70 contract it will not be considered for assessment at this time. For pricing related to other government-wide acquisition vehicles the rules would be consistent with those of that particular vehicle necessary to reach the solution's solution set.

A.1 Glossary and Abbreviations

Term	Description
Agency	"Department" or other administrative unit of the federal government, such as the General Services Administration (GSA), which is using this contract vehicle. This also includes quasi-government entities, such as the United States Postal Service.
API	Application Programming Interface
Blacklist	Application or software not deemed acceptable and have been denied approval. This may vary between agencies.
Bureau	A sub-Agency Bureau level organization, which is using this contract vehicle, as defined by OMB (www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf).
BYOD	Bring Your Own Device; Staff brings their personally-owned devices and the Enterprise installs capabilities such as email on them. May also refer to bringing devices from other agencies.
CAC	Common Access Card; a 2-factor electronic identity card used by the Department of Defense to identify individuals. The civilian equivalent is the Personal Identity Verification (PIV) card.
Capability	A technical service requirement that is a component of the base service.
CBP	Customs and Border Protection
CIO	Chief Information Officer
COTS	Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors.
DANIEL	DHS Advanced Network Integration and Experimentation Lab
Data Plan	Includes web browsing, send and receive email, download attachments, downloading applications, and application data usage.
Device	Also called handheld wireless devices, these include handheld devices that are capable of wireless voice or data communications. The devices support cellular or paging technologies augmented by technologies such as WLAN and satellite.
Feature	An enhancement beyond base service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced (NSP). Each feature must be ordered separately even if not separately priced.
FAS	Federal Acquisition Service.
FICAM	Federal Identity, Credential, and Access Management mainly addresses user certificate authentication although it does touch on passwords. FICAM is the guidance document, ICAM is the body that created it.
FIPS	Federal Information Processing Standards.
FSSI	Federal Strategic Sourcing Initiative; FSSI Wireless provides wireless service and device ordering capabilities to Government agencies.
GB	Gigabyte or 1000 MB of data.
GFE	Government Furnished Equipment.
GPS	Global Positioning System; A network of orbiting satellites that enable receivers on the ground to report their position, velocity and time. Mobile devices often use Assisted GPS (AGPS)

Term	Description
	which leverages cell towers to speed reporting time.
Government	All government entities that use or administer this contract vehicle, including state, local and education.
Government Web Store	Concept of web-based acquisition interface and management platform where government stakeholders (employees, citizens, partners) may initiate purchases, manage previous purchases, and manage contractor relationships. Concept is based on enterprise version of a commercial web storefront.
HSPD-12	Homeland Security Presidential Directive 12, which (among other things) directs agencies to deploy 2-factor authentication for information systems.
M2M	Machine to machine technologies that allow both wireless and wired systems to communicate with other devices of the same ability.
MAS/MAM	Mobile Application Services/Mobile Applications Management.
MB	Megabyte, a common term used to describe the amount of data being sent over a wireless network.
Mbps	Megabits per second, a common term used to describe wireless transmission speeds.
Mobile Device	Characteristics include 1) a small form factor, 2) at least one wireless network interface for Internet access or voice communications, 3) built-in (non-removable) data storage, 4) an operating system that is not a full-fledged desktop or laptop operating system, 5) built-in features for synchronizing local data with a remote location (desktop, laptop, organizational servers, etc.) if data capable, 6) generally operates using battery power in a non-fixed location.
Mobile Device Management (MDM)	MDM – Mobile Device Management. MDM is a widely used term describing device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring. The definition of MDM varies and reflects its growth (pre-maturity) status.
NIST	National Institute of Standards and Technology
Ordering Entity	Any Agency, sub-Agency, state or local government that is using this contract vehicle.
Ordering Agency	The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency.
PIV	Personal Identification Verification
Portal	A software (or web) solution that enables instant and effortless exchange of business information (Electronic Data Interchange – EDI) over the Internet. This is accomplished by the use of a common operating framework for accessing data and information from different systems. A typical TEMS portal will pull information from carrier electronic billing systems, which is uploaded into their platform (portal). This allows the administrator/user a single view that provides multiple carrier information in a seamless manner, offering efficiency.
Secure Communications	Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications.
Smartphone	Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance.

Term	Description
Subsystem	A subsystem is a set of elements, which is a system itself, and a component of a larger system (Wikipedia). For instance, a subsystem could include both the encryption software and the related software on the server.
TEMS	Telecommunications Expense Management Services, delivered by third parties, relating to processes for the sourcing, procurement and auditing functions connected with business communications expenses. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure [Gartner].
Text Messaging or SMS	Text Messaging or Short Message Service (SMS) is the exchange of brief written messages between cellular phones, smartphones, and data devices over cellular networks.
Third-Party Direct Billing	The receipt of invoices from parties other than the Contractor for services within or outside the scope of this agreement.
Trade Agreements Act (TAA)	The TAA of 1979 is an Act of Congress that governs trade agreements negotiated between the U.S. and other countries under the Trade Act of 1974. Its stated purpose is to: 1) Approve and implement the trade agreements negotiated under the Trade Act of 1974 [19 U.S.C. 2101 et seq.]; 2) Foster the growth and maintenance of an open world trading system; 3) Expand opportunities for the commerce of the United States in international trade; and 4) Improve the rules of international trade and to provide for the enforcement of such rules, and for other purposes. The TAA designated countries are listed in the following web site: http://gsa.federalschedules.com/Resource-Center/Resources/TAA-Designated-Countries.aspx
Trouble Ticket	Also called a trouble report, this is the documentation of a service or device failure that impacts the service. The ticket enables an organization to track the detection, reporting, and resolution of some type of problem.
WLAN Calling	Wireless Local Area Network: Enables a wireless handset to make and receive calls via an internet-connected WLAN (e.g., Wi-Fi network) instead of the cellular network.
White List	Whitelist: Application or software considered safe to run, and is preapproved.
Wireless Systems and Subsystems	Wireless infrastructure, servers, and software that enable an enterprise to enhance its cellular coverage, increase cellular capacity, and enable enterprise solutions (e.g., BlackBerry Enterprise Server) using services offered by the wireless industry.
24/7 phone support	Technical support and user assistance is provided by telephone and Internet 24 hours a day, 365 days (or 366 during leap years) per year.

Mobile Services Category Team (MSCT)
Advanced Technology Academic Research Center (ATARC)

Mobility Strategy Development Guidelines

Working Group Document

Developing Federal Agency Mobility Strategy

1 Federal Agency Mobility

The Federal Government is becoming increasingly reliant upon mobility, now with approximately 1.5 million mobile devices in service costing the government over $1 billion annually for service alone. Mobility usage across the government has a wide range of diverse profiles including general business use, vertical applications, and custom mission critical, high security applications. There is an increasing need for the Federal Government's mobile strategy and mobile device management processes to be further improved and integrated into each Agency's overall strategy due to the broader use of mobile solutions as well as increased data security threats.

Mobility has become increasingly important in recent years within the Federal Government to deliver enhanced communication, productivity, and efficiency and is playing a critical role in the accomplishment of most organizations' missions. Given both the government's reliance upon mobility, the cost of mobility services to taxpayers, and the continued rapid advancement of mobile technologies and devices; agencies will want to have a clear and intentional strategy for mobility integration, implementation, and management within Agency operations.

1.1 Federal Agency Mobility Strategy

Developing an Agency Mobility Strategy is a complex task and requires involvement across many functional areas of an Agency. The very large Federal Agencies such as Department of Defense have ample resources to develop a mobile strategy and their complex mobile requirements have unique, customized solutions. However, many other agencies do not have adequate internal resources for strategy development. This document is primarily aligned with providing guidance to those agencies needing to follow a fairly standard strategy development process.

Furthermore, there are resources available to Agencies in the development of their mobile strategy to include GSA – Enterprise Mobility, which serves as the executive agent for the Government-wide acquisition solutions to connect agencies to mobile service providers; the Mobile Services Category Team (MSCT), which serves as the Category Lead for mobile devices and services under the Category Management Leadership Council; and the Advanced Technology Academic Research Center (ATARC), a non-profit organization which seeks to provide collaboration on emerging technologies by working closely with government, industry, and academia.

This paper addresses three primary steps in developing an Agency's Mobile Strategy, which are:

- **Agency Context**
  - The Agency Context describes the Agency mission, goals, use cases, internal communications, and external communication processes and requirements.
- **Mobility Business Drivers**
  - The Business Drivers outline an Agency's management and technical capabilities, resources, and requirements for development and execution of the mobility plan.
- **Mobility Components**
  - The Mobility Components are the day-to-day operational and support activities necessary for the use and management of mobility services.

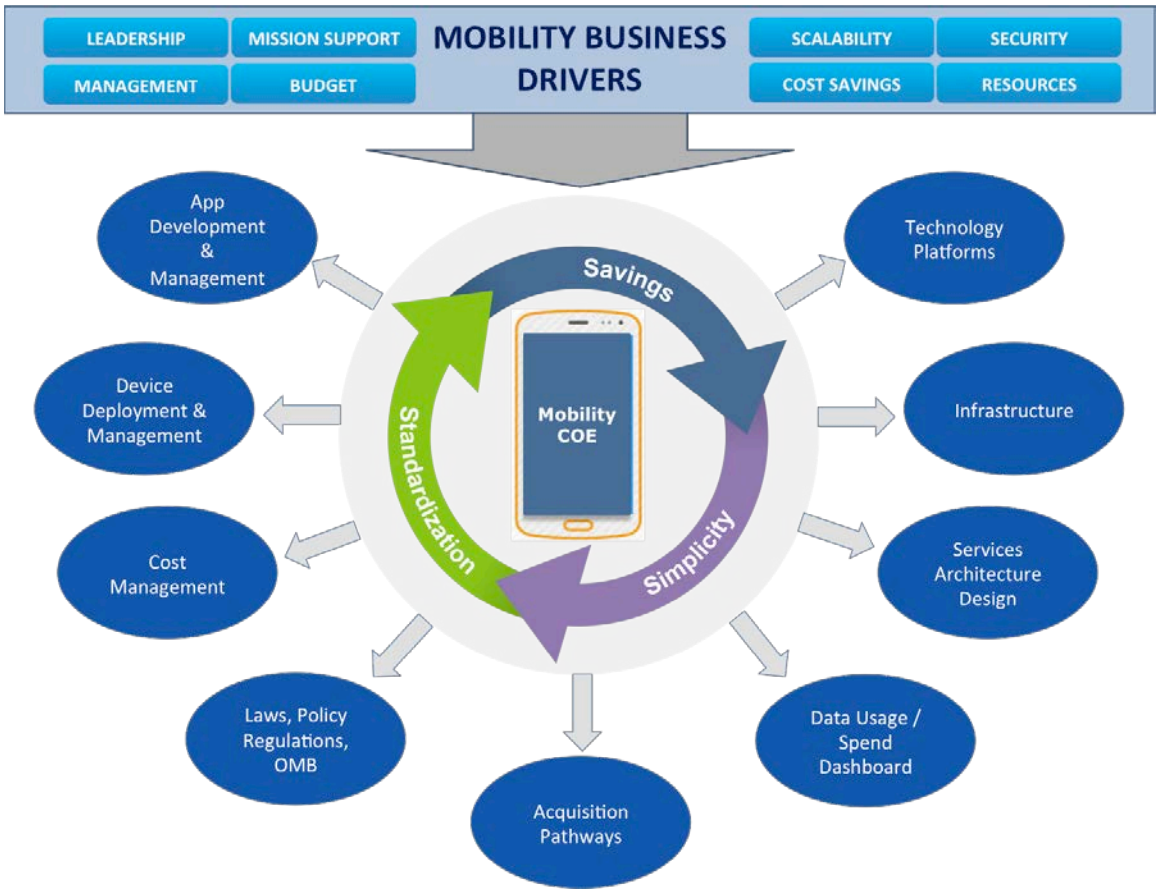
For a mobile strategy to be effective, it will need to be integrated into the overall Agency strategy and not be viewed as a standalone or separate initiative. However, the mobility strategy has specific guidelines and requirements pertaining to planning and execution. But, mobility is to be a means to an end and an element of the infrastructure, albeit a critical one, to help an Agency deliver upon its mission.

The three primary outcomes of the Mobility Strategy are:

- **Standardization** – Standardization of service plans, reporting, and agreements across the Agency will result in improved operational efficiency and reduced management time.
- **Simplicity** – communication processes are simpler and easier to use when they are properly designed around specific use cases. Productivity gains are also recognized, as fewer resources are required for managing mobility services and support processes are streamlined for supporting Agency employees.
- **Savings** – cost savings is a result of lowering direct and indirect costs through mobility integration, active mobility management, and optimization.

The figure below shows the Mobility Strategy structure and the relationship between the Mobility Business Drivers, Mobility Components, and Outcomes.

Figure: Mobility Center of Excellence: Business Drivers, Components, and Outcomes



The remainder of the document provides guidance in following the three steps to building Mobility Strategy – Agency Context, Mobility Business Drivers and the Mobility Components. Each Agency developing a mobility strategy will benefit from going through each of these three steps to build, introduce, and manage the appropriate mobile strategy.

2 Agency Context

The Agency Context provides a description of the environment in which the mobile strategy is to be established. The collective result determines the depth of mobile integration necessary to meet the Agency's mobility goals and objectives. Additionally, enables an understanding of how mobility may help mitigate or overcome some key challenges.

Describe the Agency Context to include the following factors:

1. Agency goals and objectives
2. Challenges the Agency is facing (e.g. budget, resources, etc.)
3. Mission deliverables dependent upon improved communication, productivity, and efficiencies
4. Primary internal communication and data sharing requirements
5. Mobile use case scenarios of the primary work teams – office and remote teams
6. If applicable, interaction between the Agency and US citizens
    - Primary points of interaction between Agency and US citizens
    - Communication and data requirements for service delivery to US citizens
    - How US citizens want to engage and communicate with the Agency

The Agency Context forms the foundation for developing the remaining two steps of the mobility strategy, the Agency's Mobility Business Drivers and the Mobility Components.

3 Mobility Business Drivers

The following are the Mobility Business Drivers to be reviewed and assessed to develop, manage and support the Mobility Strategy:

- Leadership
- Management
- Mission Support
- Budget
- Cost Savings
- Resources
- Security
- Scalability

3.1 Agency Leadership and Mission Support

Assess Leadership and Mission Support: An Agency's leadership, their respective mobility vision, and comfort level with emerging technologies within the organization will determine the degree of mobility integration and the breadth of applications initiated. Agency leadership will need to assign a management team highly capable of supporting and operationalizing the mobility strategy. Internal communication of the mobility vision is important to successful implementation as well as achieving the expected outcomes.

Recommendations:

1. Assign a team responsible for defining, developing and integrating the mobile strategy.
2. After the vision and strategy is drafted, communicate it to the broader employee base, especially those work teams most impacted by changing communication processes and workflows.
3. Include those expected to use any new mobile applications or communication processes should be included in development sessions held by the development team to ensure the best user experience.

3.2 Management

Assess current mobility management characteristics: Federal agencies have varying levels of management expertise and skill in procuring, implementing, and managing mobility resources. Agencies successful in mobility management share certain characteristics including:

1. Maintenance and management control(s) of their mobility assets (devices and service lines);
2. Proactive management of mobility costs;
3. Near-seamless transition for end-users;
4. Appropriate matching of requisite mobile technology to the end-user's work environment and needs, and;
5. Ensuring that the carrier(s) are providing required levels of services, including coverage, voice and data quality, and wireless management reporting.

Recommended management practices of Agencies that employ strategic sourcing principles at the planning phase of their mobility acquisition(s):

- Understand how mobility is procured and used across the organization, the resources required to support a mobile workforce, and the average spend per user each month.
- Reduce the number of separate wireless contracts by consolidating the volume of business for the largest procurement possible.
- Standardize service plans across different contracts to better manage and control their wireless spend.
- Compare their average cost of service per device type to those of other agencies, attempt to renegotiate prices, and review alternative contract vehicles.

3.3 Scalability

Evaluate the ability for solutions to scale beyond initial use if applications expand across user groups or externally. Guiding questions:

- Are the mobile solutions being considered for deployment relied upon for mission critical activities?
- What is the scalability and flexibility of the solutions being considered for deployment?
- What are the contingencies for higher adoption levels and bandwidth requirements to expand beyond the initial plan?
- What is the projected variability in the size of the user groups over time?
- Are there alternative solutions that will allow for greater scalability, if required?
- What are the associated incremental costs of increased scalability if needed?

3.4 Device Management and Security

Evaluate respective device management and security needs to select appropriate security solutions and management software.

Enterprise Mobility Management (EMM) is a collective set of tools used to centralize management and maintenance of mobile devices such as smartphones and tablets and is inclusive of mobile device management (MDM), mobile application management (MAM), and mobility content management (MCM) software. EMM addresses the combination of security and management solutions for devices, applications, data, and content.

Enterprise Mobility Management refers to any of the following mobile management solutions:

- **Mobile Device Management (MDM).** Enables enterprises to manage and secure data on a device and often provides enterprise email access. Management includes configuring settings, taking remote actions (e.g., device wipe), and device tracking.
- **Mobile Application Management (MAM).** Manages and controls access to applications ("apps"), including application deployment, Mobile Application Store (MAS), and application security.
- **Mobile Content Management (MCM)**. Secures and shares content (e.g., Dropbox).

Selecting an EMM provider: Depending upon the provider selected, below is a list of capabilities Agencies should consider when evaluating an EMM provider:

- Deployment, support, locking, configuration, and deactivation of devices – some solutions allow for remote / over the air access
- Monitor and control device, applications, email, connectivity, troubleshooting, and data security
- Manage mobile applications
- Enforce policy compliance
- Share data and documents securely
- Allow secure access to websites and intranets
- MAM solutions may include a custom app store

3.5 Budget and Cost Savings

Establish cost savings objectives and process improvements for mobility solutions: A central component and outcome of the mobility strategy is cost savings. There are several approaches to budgeting and reducing mobility costs. When proactively managing costs, many agencies strive to minimize overage charges as the primary goal. They place users either on unlimited plans or very high-minute plans, then monitor the monthly usage charges or fees and take action as necessary. This practices is rarely optimal for managing mobility spending and reducing costs.

Recommended approach for Agencies to manage their mobility spend:

- Optimize the service plan mix regularly (e.g., at least bi-annually) to more closely match the broad set of actual usage patterns and avoid overpaying for overcapacity.
- Utilize pooling on data plans, not just voice service plans.
- Structure billing account plans to broaden the universe of pooled minutes for both voice and data services.

- Conduct studies to better understand the actual usage per different device types, including minutes and text usage on mobile devices, voice and data usage on smartphones, and MBs used on data services.
- Know their average monthly recurring charges for different device types and areas of their business (e.g., headquarters versus field operations).
- Understand the agency's business cycle and make allowances for increased or decreased usage (e.g., teleworking may increase in winter months due to the greater likelihood of snow days).

3.6 Resources

Evaluate internal resources and the need for additional assistance available through government sources: As stated in other sections of this document, it is critical to a successful strategy development and implementation process to involve multiple areas within an Agency – especially those that will be most impacted by mobility changes.

Agencies needing additional resources and guidance in the development of their mobile strategy have sufficient resources available including GSA – Enterprise Mobility, the Mobile Services Category Team (MSCT), and the Advanced Technology Academic Research Center (ATARC), Both GSA and ATARC websites have many mobility related Working Group documents and papers addressing mobility, which are available to agencies, providing detailed reviews, guidelines, and requirements for all aspects of mobility within the Federal Government.

4 Mobile Strategy Components

The Mobility Business Drivers directly determine how the Mobile Strategy Components will be planned, supported, and executed. It is recommended that Agencies consider each of the Mobile Strategy Components to determine relevance and application to their respective strategies.

Mobility Components are the day-to-day operational and support elements necessary to deliver the on the Mobility Strategy. The extent to which these elements are required will be based upon the scope of mobility integration and strategic objectives.

- Technology Platforms
- Infrastructure
- Services Architecture Design
- Data Usage / Spending
- Acquisition Pathways
- Laws, Policy Regulations, OMB
- Cost Management
- Device Deployment and Management
- App Development and Management

4.1 Technology Platforms

Agencies must ensure that the mobile strategy reflects the selection of the technology, which fits the organizational needs. Technology solutions to consider in the development of the mobile strategy include the following:

- Mobile Devices
  - Standard, commercially available devices
  - Customized devices
  - Device as a Service (DaaS)
  - Virtual Mobile Infrastructure
- Mobile Security
  - EMM – MDM, MCM, MAM

    - Application vetting
    - Mobile Threat Protection
- Application Development
    - Commercial applications
    - Customized applications
- Service Coverage
- Mobile Backend as a Service (MBaaS)
- Mobile Identity Management
- Telecom Expense Management Services (TEMS)

Obtain feedback from end-users:

- Determine the quality of current mobility solutions
- Evaluate coverage across Agency work locations
- Assess current technology related policies and impacts on end-users
- Gather input on perceived gaps in the mobile capabilities and applications
- Identify perceived security risks and requirements
- Understand data access needs for remote and mobile users

4.2 App Development and Management

Assess the need for mobile application development to support Agency mission: The Federal Government increasingly relies on commercial and custom-built mobile apps to increase productivity by:

- Providing government employees real-time information sharing
- Providing "anytime, anywhere" access to perform enterprise or mission-specific tasks
- Delivering government information efficiently to the public

Mobile apps may be developed by one of the following groups:

- Trusted in-house developers
- Contract developers familiar with the agency
- Third parties (commercial developers) having no relationship with the agencies

As Agencies determine their needs for mobile applications to support their mobile strategy, they will select either commercially available apps or develop customized applications for specific Agency functions. When developing new mobile apps, mitigate risk through in-house development and or through app vetting processes.

Unlike desktop applications, precise location information, contact details, sensor data, photos, and messages can be exposed through mobile apps, and personal information. As mobile applications rely on cloud services to store enterprise data, mobile apps that do not use secure programming practices can expose the cloud infrastructure to new risks also.

The mobile application vetting process follows the development of a custom app or identification of a commercial app to be used for government business and prior to the app's installation on a mobile device or publication of a custom app to a federal, community, or commercial app store. Application Vetting is a sequence of activities that aims to determine if a mobile application (app) conforms to security and privacy regulations (e.g., HIPAA, NIAP, PCI) and to organization-specific requirements and policies.

App vetting is part of the software assurance process that occurs after app development: it evaluates mobile apps against a set of security requirements to identify weaknesses, vulnerabilities, poor programming practices, improper use of cryptographic functions, insecure authentication to cloud services, and malicious or privacy invasive behaviors. Its objective is to provide Federal Agencies with a level of assurance that commercial and custom-developed mobile apps used to conduct government business will not compromise Federal systems or information, operate as described, do not request more permissions than needed, and do not expose information that could harm the privacy, security, or safety of employees or the public.

4.3 Device Selection and Deployment

The process for aligning business needs with mobile device selection and deployment requires detailed insights and understanding of the employee base and their work assignments:

4.3.1 Device Selection

- Expected Device Use
    - Develop use case scenarios and determine which of the three user profiles or combination of profiles best address mobility use within the Agency:
        - General use – standard wireless use of voice, text, and mobile data
        - Vertical application – specialized use of mobility device and services
        - Custom solution – combined service, device, and software by an integrator or other service provider, which requires custom software or app development and enhanced devices
- Usage environment and frequency of use
- Connectivity requirements
    - Voice and data, voice only, or data only services
    - Coverage – urban, rural, or highly remote, CONUS, OCONUS
    - WiFi calling
    - Tethered services or hotspot capability
    - Simultaneous use of both voice and data
    - Customized connectivity solutions
- Device cost parameters
- Device requirements: Type, data storage capacity, OS, security, screen size, applications, camera quality, battery life, and external features such as color and available accessories
- Usage requirements critical to mission success
- Projected device life and required refresh cycle
- Validate device alternatives compared to the National Information Assurance Partnership (NIAP) and Protection Profile for Mobile Devices Fundamentals

4.3.2 Device as a Service (DaaS)

Device as a Service (DaaS) is a valid alternative consideration to a la carte procurement in the mobile sector. It is a subscription model for devices such as smartphones, tablets, wearables, and other mobile hardware. The DaaS model may offer a Federal Agency increased flexibility and cost control and reduce internal mobility management resource requirements. Mobile DaaS will continue to evolve to meet changing customer requirements. It includes end-to-end device supply, service, and management to include:

- Planning and Management of Agency DaaS Solutions

- Device Provisioning, Kitting, and Delivery
- Mobile Device Management and Device Refresh
- Ongoing Helpdesk Support
- Logistics for end-of-life disposal / recycling
- Wireless Carrier Network Services (may or may not be included)

DaaS service plans can vary based upon the overall set of Agency needs and the agreement terms with the DaaS service provider. Typically, DaaS service is determined by detailed mobility needs including identifying network coverage requirements; device technology, features, and benefits; determining the initial time period for the length of service; and agreeing on a monthly fee per device for the provider to deliver specific devices and related management services.

The primary reasons Agencies and enterprises may evaluate and consider DaaS for devices, hardware, or equipment instead of purchasing and managing are:

1. **Ability to Scale** - Flexibility in scaling the needed devices to changing workforce levels provides efficiency
2. **Limited Internal Resources** – Third party planning and management of mobile devices eliminates the internal strain on staff resources.
3. **Budget Structure and Flexibility** – DaaS allows an enterprise to move the outright purchase of devices from capital budget to an operating expense, which for government purposes is an annual spending allocation.
4. **Asset Obsolescence** – Ability to refresh devices more quickly and to easily dispose of and recycle older devices gives an Agency newer technology on a regular basis and eliminates the labor-intensive process of device disposal.

4.3.3 Virtual Mobile Infrastructure

Virtual mobile infrastructure (VMI) is an emerging mobile technology that may be considered by those agencies with high security risks and in need of higher-level protection of mobile data. It is a delivery model in which a mobile device runs the OS, authentication, applications, mobile security, and data access from a centralized data center or cloud instead of being stored on the device. The mobile applications and functionality can be run on any mobile device including smartphones, tablets, wearables, or sensors and data collection devices. Since all data is stored centrally and is not stored on an individual device, the user can move from one device to another seamlessly with out losing any data or functionality.

Key benefits for consideration of VMI within the mobile strategy:

- Central control of authentication, access, applications, and capabilities – including GPS, Bluetooth and other device sensors
- Data encryption and centrally managed security
- IT management simplified with single platform
- App development – one version across all devices
- Organizational data accessible remotely enabling mobile business processes
- Allows access and control via BYOD devices
- Both iOS and Android are supported in this structure

4.3.4 Device Transition

Another component of Device Deployment is Device Transition that occurs when Agencies move from one Wireless Carrier Service provider to another or from one TEMs provider to another and

all or a portion of mobile devices must be replaced. Agencies most effective in transitioning to a new vendor or migrating from one service contract to another do the following:

- Develop a detailed project plan or a baseline transition plan with input from the vendor.
- For larger projects, develop a communications plan and separate guidelines for service ordering, including a user guide for end-users.
- Utilize GSA's FSSI Transition Guide as a checklist for future projects.

4.4 Cost Management

Agencies will want to build into their mobile strategy sound cost management and control principles:

- Utilize a variety of consolidated reports to monitor costs and usage on a monthly basis. Cost Management is accomplished by using vendor-provided reports, developing custom reports, or outsourcing this function to a third-party solutions provider (e.g., a systems integrator, TEMS provider, or contractor), with the goal of optimizing rate plans and device inventory.
- Develop a database of current and detailed list of all cellular telephone numbers within the Agency (voice and data lines) per employee across the enterprise.
- Track the number of unused service lines each month and delete lines with three consecutive months of inactive usage.
- Have a well-defined operational model establishing, for example, who is allowed to order, change and delete services; refresh policies for devices; device options for end-users; and procedures for device disposal.
- Develop clear policies for who receives what type of phone or device, what mobile applications can be placed on it, security levels, appropriate uses for the device, actions to take if the device is lost or stolen, etc. It is recommended that agencies standardize across a limited number device models to reduce helpdesk and management costs.
- Know the direct and indirect costs of managing services and device inventory. This includes the time spent adding or removing software, activation and deactivation of lines, selecting service plans, disposing of devices, answering trouble tickets, etc.
- Evaluate third-party alternatives, such as TEMS providers and integrators, if in-house resources are unavailable or outsourcing is more cost effective. The GSA Telecommunications & Mobile Lifecycle Management Program, available at www.gsa.gov/portal/category/100362, provides excellent resources and an extensive list of best practices for this category of spending.

4.5 Laws, Policy Regulations, OMB

In procuring and managing mobile products and services, agencies must navigate a broad and complex set of Federal regulations, guidelines, and policies. They must also consider requirements of other government stakeholders, such as Congress, the Office of Management and Budget (OMB), the Government Accountability Office (GAO).

Following are some of the key policy and regulation drivers:

- **Budget Constraints and Cost Controls** - agencies likely will continue to face pressure from Congress and OMB to reduce costs and control their wireless and telecommunications expenditures. Another factor is the Digital Government Strategy, Part 5.3, which requires agencies to evaluate government-wide contract vehicles in the alternatives analysis for all new mobile-related procurements.

- **Improving Management and Control of Mobile Assets** - Significant savings in wireless purchases can be achieved with clear visibility into the agency's device inventory and end-user usage patterns. The *Federal Information Technology Acquisition Reform (FITARA)* Act, enacted in December 2014, is a key piece of legislation (H.R. 1232) that supports agencies' ability to better manage their IT/Telecom investments and enhances the authority of CIOs to manage IT spending.

- **Increased Reporting Requirements and Oversight by OMB** - OMB provides leadership across the Federal Government to ensure that agencies follow-through on executive orders and guidelines. The Office of Federal Procurement Policy has increased its efforts related to federal procurements. It is chartered to:

- Coordinate and review the collection of information

- Promote public access to public information and include the effective use of information technology

4.6 Acquisition Pathways

The challenge facing agencies in procuring and managing mobility services is the large number and complexity of different acquisition pathways that exist across the Federal Government.

Simplifying the steps to acquisition:

Step 1: Determine the type of technology or service required by the organization. As shown in the Figure below, the framework divides the Enterprise Mobility category into four components: Commodity IT Purchases, Commercial Wireless Services, Enterprise Mobility Management, and Back-Office and Customer Support. Each component lists high-level sub-categories of products and services that apply.

Step 2: Determine the acquisition approach. Within each mobility component (e.g., Commodity IT Purchases), agencies have two mutually exclusive programmatic pathways to consider. Select either an existing Government Wide Acquisition Program (GWAP), or select or establish an agency-specific contract or agreement. The latter pathway is referred to as the Independent Approach.

NOTE: As depicted in the diagram, the number and complexity of acquisition pathways for mobility products and services increase if an agency selects a third-party solutions provider to act as an intermediary in purchasing commodity IT Services or commercial wireless services.

4.6.1 Acquisition Solutions for Federal Agencies

An agency must consider the type of technology or service required by its organization. As shown in the two Figures below, a framework provided to the Mobility Services Category Team (MSCT) divides the Enterprise Mobility category into four components:

- Commodity IT Purchases – Hardware with no service contracts
- Commercial Wireless Services – Device and services from wireless carriers
- Enterprise Mobility Management – Support services for mobility
- Back Office and Custom Support – Helpdesk and administrative services

This section briefly covers the primary contracts, programs, and acquisition solutions available for agencies when considering mobility products and services.

Government Wide Acquisition Contracts (GWACs) offer agencies a streamlined acquisition pathway to procure the requisite technologies and services for their organization. GSA has a broad portfolio of GWACs available to the government to address the variety of enterprise mobility requirements.

Figure: Potential Pathways for Obtaining Mobility Services

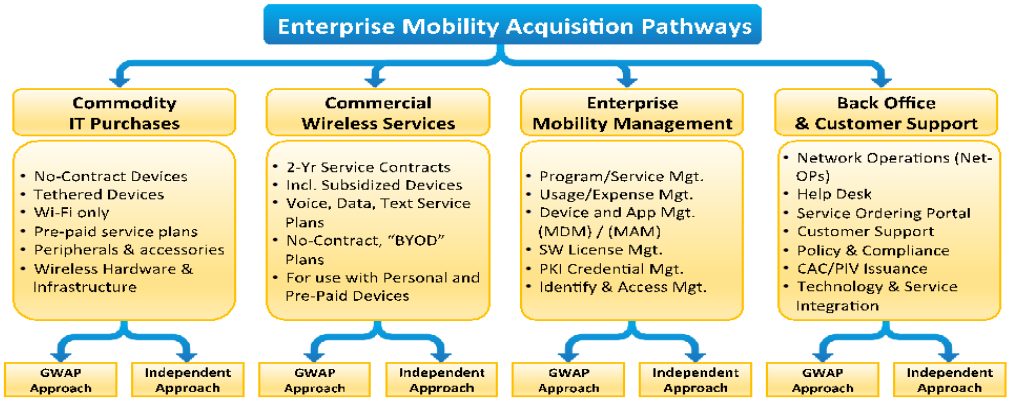
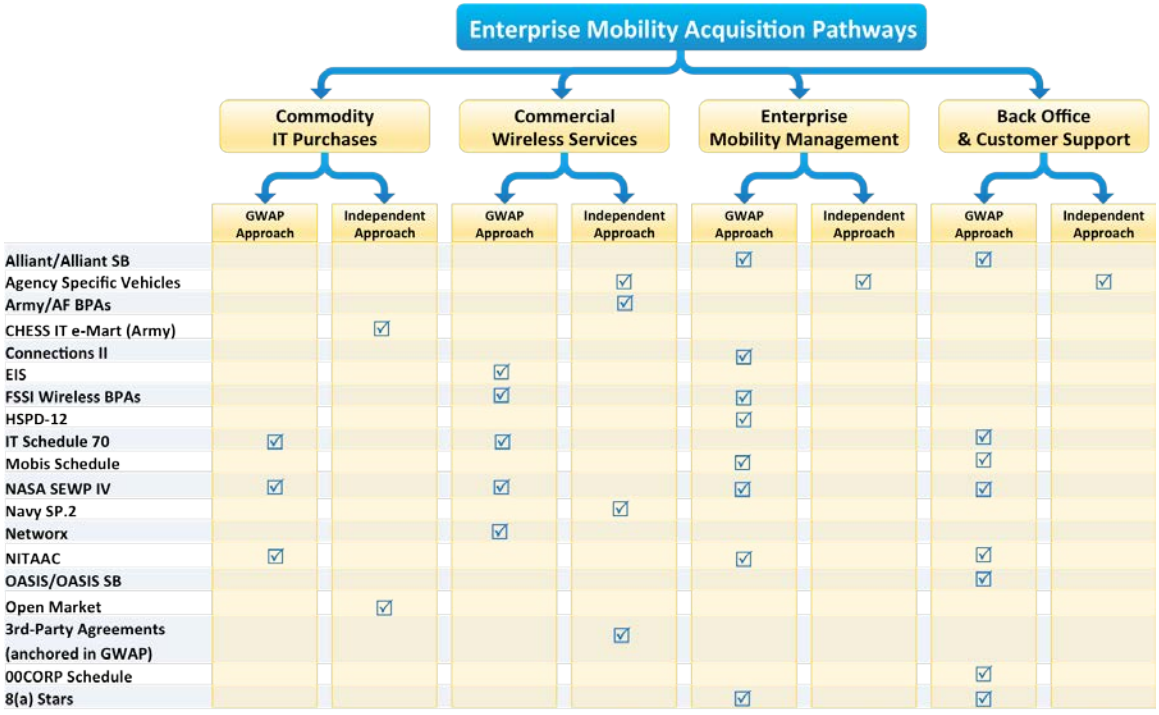


Figure - Mapping of Mobility Acquisition Pathways and Solutions



4.6.2 General Services Administration Contracts

IT Schedule 70

IT Schedule 70 is an evergreen GSA schedule contract IDIQ (Indefinite Delivery, Indefinite Quantity) vehicle, Multiple Award Schedule contract governed by FAR Part 8. The Schedule is arranged by special item numbers (SINs) - the most pertinent to the mobile services category is SIN 132-53. More information available at GSA IT Schedule 70

FSSI-Wireless BPA

The Federal Strategic Sourcing Initiative (FSSI-Wireless BPA) is anchored in SIN 132-53 on IT Schedule 70. FSSI Wireless BPAs primarily include Commercial Wireless Services but also offer some Enterprise Mobility Management solutions (MDM/MAM) and Commodity IT items, such as wireless infrastructure components. More information available at GSA FSSI-Wireless

Networx

Networx is a part 15 IDIQ telecommunications contract, awarded in 2005. Of the $1.62 billion that Federal agencies spent in networks and telecommunications services through the Networx contract in FY15, only $3 million was mobility related. Networx sunsets in 2020, yet its successor comes online in 2017 allowing time for agency transition.

Enterprise Infrastructure Solutions

Enterprise Infrastructure Solutions (EIS) is a part 15 IDIQ telecommunications contract to be awarded in the fall of 2016 and ready to take orders in 2017, with a ceiling of $50 billion. Like its predecessor, EIS will have a mobility component. Using EIS for IT telecommunications, infrastructure requirement, and mobility centralizes the buy for an agency. More information available at Enterprise Infrastructure Solutions

Alliant / Alliant SB Contract

Alliant and Alliant Small Business (SB) is a $50 billion GWAC focused on information technology (IT) services and IT services-based solutions. Alliant contracts have standardized technologies and systems along Federal Enterprise Architecture (FEA). Depending on an agency's mobility requirements, Aliant and Alliant SB contracts address Enterprise Mobility Management and Back-Office and Customer Support functions. Both contracts will expire in 2019, although task orders may live on to 2024.

Connections II

Connections II is a GSA-owned GWAC that focuses on four solution sets:

1. Communications and Networking;
2. Building or Campus Facility Preparation;
3. Operations, Administration, and Management (OA&M); and
4. Customer Service and Technical Support.

Connections II may be used in a variety of Enterprise Mobility Management areas, such as usage and expense management, program/service management, and MDM/MAM solutions. Connections II will expire in 2019, although task orders may live on to 2024.

HSPD-12
GSA's HSPD-12 Shared Services Provider II contract, worth an estimated $66 million, will establish the information technology to provide end-to-end compliant ID credentials and will cover about 42 participating government agencies, boards, and commissions. Areas of mobility addressed by HSPD-12 include PKI Credential Management and Identity and Access Management.

MOBIS and 00Corp Schedule
GSA consolidated its professional services legacy Multiple Award Schedule offerings into one Professional Services Schedule (PSS). Two of these vehicles – Mission Oriented Business Integrated Services (MOBIS) and Corporate Services (00CORP) – offer access to many qualified vendors capable of providing services and solutions for mobility back-office functions and customer support.

OASIS / OASIS SB
The newest GSA GWACs are the OASIS (One Acquisition Solution for Integrated Services) and its Small Business (SB) counterparts that fill the Federal Government's needs for complex, integrated professional service. OASIS (unrestricted) and OASIS Small Business contracts are multiple award IDIQs that are composed of Pools, defined by NAICS codes for the scope of work to be acquired, and span many areas of expertise and mission spaces. The table below "Figure OASIS Pools" highlights several mobility-related back-office functions and the applicable OASIS Pool.

4.6.3 Third-Party Agreements (Anchored in a GWAP), Blanket Purchase Agreements

Blanket Purchase Agreements (BPA) can be established under any GSA Schedule contract. The purpose of a BPA is traditionally focused on addressing recurring needs for supplies and services. When a BPA is based off a schedule, only the vendors on the schedule and designated SINs can compete. When the list on the BPA is narrowed down to a select few, task orders are issued and the vendors compete yet again to win the work. Whatever line items appear in the BPA must also be listed on the vendors' SIN 132-53 schedule.

4.6.4 Other Government-wide Acquisition Vehicles

OMB designated GSA and two other agencies to be stewards of GWACs: the National Aeronautics and Space Administration (NASA), and the Department of Health and Human Services (HHS), National Institutes of Health (NIH). GWACs are information technology contracts that the entire government can access. The following two GWACs address Enterprise Mobility segments:

NASA SEWP IV
Solutions for Enterprise-Wide Procurement (SEWP) is a Fixed Price, IDIQ, multi-award Government-Wide Acquisition Contract (GWAC) vehicle focused on IT products and product-based services. SEWP contract holders offer a wide range of enterprise mobility products and services, including commodity IT, commercial wireless services, Enterprise Mobility Management, and back-office and customer support services. The effective dates for SEWP V contracts are from May 1, 2015, through April 30, 2025. The base contracts were awarded for 5 years with one 5-year option, for a total of 10 years. Each contract has a $20 billion contract limit.

NITACC
The National Institutes of Health Information Technology Acquisition and Assessment Center (NITAAC) within HHS is a holder of three GWACs for information technology procurement: CIO-SP3, CIO-SP3 Small Business, and CIO-CS. These contracts address a range of mobility products and services, including commodity IT purchases, commercial wireless services, and Enterprise Mobility Management.

4.6.5 Department of Defense (DOD) Acquisition Vehicles

The Department of Defense (DOD) has several acquisition vehicles in the enterprise mobility arena. These contracts are considered independent approaches due to their DOD-specific technical requirements, which can be different from civilian agencies.

Army/Air Force BPAs
The NETCOM BPA allow Army, Air Force, and other DOD officials to order commercial cellular wireless voice and data services, as well as related equipment, data analysis, support, and maintenance services.

Navy SP.2
The Navy SP.2 (Solutions and Partners 2) contract is the next generation contract currently under development for commercial wireless services.

CHESS IT eMART (Army)
The Computer Hardware Enterprise Software and Solutions (CHESS) program is the Army's primary source for procuring commercial IT products and services. CHESS (through the ITeMART) allows authorized users to buy commercial off-the-shelf (COTS) IT hardware, software, and services from a variety of contracts through an online e-commerce ordering system. Two other enterprise mobility-related contracts are available through CHESS:

- Army Desktop and Mobile Computing-2 Contract (ADMC-2).
- Wi-Fi Device Contract - All devices are Wi-Fi only and have no cellular data plans or capabilities.

4.6.6 Other Independent Approaches

Agency Specific Vehicles
Some agencies operate outside of the FAR (Federal Acquisition Regulations) or have their own supplement to the regulations. For example, the DOD has the Defense FAR (DFAR), and the FAA and USPS follow their own variations of the FAR. Agencies that take this route believe they have the acquisition resources, technical expertise, specialized requirements, or buying power to negotiate better terms and conditions than any existing GWAP that is available to them.

Open Market Process
For many vendors, it is not practical to carry on their GSA Schedule or other contract all the items that could be a part of a purchase. The Open Market process is the method allowed by the FAR to procure "incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract."

4.7 Services and Architecture Design and Infrastructure

Evaluate the Service, Architecture Design and Infrastructure requirements.
Guiding Questions:

- What elements of the mobile strategy and communication processes mission critical?
- How are contingencies built into the infrastructure design in case of any point of failure?
- Will the implementation of the mobile strategy likely increase, eliminate, or re-distribute support resources?
- What additional service requirements may arise from an expanded mobility implementation?
- Is the infrastructure of the agency able to implement and support internal mobile applications?
- What process changes will be required to move or integrate processes to mobile solutions?
- Does the Agency have the infrastructure to support the traffic of your mobile app if supporting external communications?

5 Resource Summary

To discuss further or obtain assistance in developing a mobile strategy, the resources available are:

- GSA – Enterprise Mobility Team
- Mobile Services Category Team (MSCT)
- Advanced Technology Academic Research Center (ATARC)
- Both GSA and ATARC websites have many mobility related Working Group documents and papers addressing mobility; which are available to agencies, providing detailed reviews, guidelines, and requirements for all aspects of mobility within the Federal Government.