DPIV Scenarios for ATARC Lab

1 Executive Summary

The National Institute of Standards and Technology (NIST) Special Publication 800-157 specifies the use of a Derived PIV Credential (DPC) to situations where the use of a physical Personal Identity Verification (PIV) card is impractical. While the issuance and use of DPCs have existed within the Federal Government since 2015, the Advanced Technology Academic Research Center Identity Management Working Group (ATARC IdM WG) in coordination with the Derived-PIV Working Group (a sub-group under the Federal Mobility Group) has identified four real-world scenarios that have yet to be solved. The ATARC IdM WG is requesting demonstrations to show potential solutions for these four scenarios. By participating, vendors will show the feasibility of available DPC solutions to enable the Federal Government to continue the adoption and usage of phishing resistant multi-factor authentication.

Overview: Because of the complexity to implement Derived PIV Credential systems, it is recognized that no single vendor will address all aspects of a Derived PIV system. When addressing the scenarios provided below, clearly state the following:

- Identify the aspects of Derived PIV implementations (as previously defined by the government) that your solution addresses
- Identity the specific protections your solution provides aligned to the scenario
- Identify any standing partnerships you have with other vendors for meeting other aspects of Derived PIV implementations
- Identify any operational deployments of your solution in either a government setting or private industry, providing specifics on the operational setting (size of agency, etc.)

Unless otherwise stated, assume an unclassified (or SBU) setting.

Below are the scenarios:

<u>Scenario 1 - Remote User BYOD</u>

An agency employee or contracted personnel working remotely, using personally owned mobile devices (phone or tablet), must regularly access a cloud based, agency application. The employee routinely accesses the system as a standard user using a phishing resistant MFA to access that system. The user's physical location changes frequently with personal travel.

Scenario Challenge:

- The government requires solutions to enable DPCs on personally owned mobile devices.

Technical Requirements:

- Unmanaged mobile phone or tablet, that is personally owned (BYOD)
- DPC to be accessible on the phone or tablet
- DPC must follow guidance specified within NIST SP 800-63B for an AAL2 or 3 phishing-resistant authenticator

    - Vendor must specify what AAL is being presented
- Must follow FIPS 201-3

<u>Scenario 2 - Branch Office from TIC 3.0 Document</u>

An agency employee or contracted personnel, working from an agency satellite office and using government furnished equipment (i.e., a laptop), is accessing Internet sites. The sites vary between sites supporting job related research and his/her personal bank. The laptop is not joined to a traditional on-prem domain such as an Active Directory Domain Services environment. The device can be managed by an EMM system. The employee is a standard user and uses a phishing resistant MFA (DPC) to access a local account on that system.

Scenario Challenge:

- The government requires solutions for user enabled MFA login to the non-domain joined workstation
- Web-based authentication to external resource

Technical Requirements:

- DPC must follow guidance specified within NIST SP 800-63B for an AAL2 or 3 phishing-resistant authenticator
    - Vendor must specify what AAL is being presented
- Must follow FIPS 201-3

<u>Scenario 3 - CI/CD Pipeline Dev-Prod Separation</u>

An agency employee or contracted personnel provides ongoing improvements to an agency system as part of a development team and provides administrator and routine maintenance to the operational system. Development is performed from the contracted employee's corporate offices using devices provided by his/her company. Development is performed on a separate network, isolated from the production network. Both operate within a data center located at the agency's facilities. When appropriate, the contracted employee moves systems from the development environment into production. When operating in the Dev environment, they can use an AAL2 or lower authenticator (does not need to be a DPC). In order to move to a production environment, they are required to use an AAL3 authenticator (either PIV or AAL3 derived PIV).

Scenario Challenge:

- Government requires solutions for solving software supply chain management by preventing credential leakage in continuous integration/continuous development (CI/CD) pipelines

Technical Requirements:

- Show usage of a lower assurance credential in the development environment

- Show usage of a higher assurance credential through step up authentication to move code into production (NIST SP 800-63B, AAL3)
- DPC must follow guidance specified within NIST SP 800-63B for AAL3 phishing-resistant authenticators
    - Vendor must specify what AAL is being presented
- Must follow FIPS 201-3

Scenario 4 - Step-up AuthN

An agency employee or contracted personnel using government furnished equipment is accessing an application as a user with an AAL2 authenticator. In order to complete a more sensitive task in the same application (e.g. access PII) the application will require step-up authentication to an AAL3 authenticator for that purpose.

Scenario Challenge:

- Government requires solutions for step up authentication within a single application

Technical Requirements:

- Show usage of a lower assurance credential to access an application environment using GFE (NIST SP 800-63B, AAL2)
- Show usage of a higher assurance credential through step up authentication to access PII using GFE (NIST SP 800-63B, AAL3)
- DPC must follow guidance specified within NIST SP 800-63B for an AAL2 and AAL3 phishing-resistant authenticators
    - Vendor must specify what AAL is being presented
- Must follow FIPS 201-3