Use Case ID:	001-A-PACS		
Use Case Name:	Mobile phone - PKI authentication to physical access control systems providing access to a building.		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/8/22	**Date Last Updated:**	7/13/22

Actor:	Agency Personnel
Description:	Agency personnel uses mobile phone with PKI credentials in a PIV wallet to authenticate and gain access (entrance) to their agency facility via PACS.
Preconditions:	1. User has an existing PIV card/account that is active 2. Authentication methods aligns with NIST Security Control Overlay of SP 800-53 REV 5.
Postconditions:	1. User successfully authenticates their mobile phone/tablet against the building PACS and gains access to the building.
Priority:	High
Frequency of Use:	Average: Twice daily, 5 days a week, 48 weeks a year
Normal Course of Events:	1. User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader 2. The reader validates the PIV PKI certificate on the phone and validates the credential is authorized for access. 3. Access is granted. 4. END.
Alternative Courses:	001-A-PACS.AC.01 - Agency personnel uses mobile phone with PIV PKI credentials to authenticate exit their agency facility via PACS.
Exceptions:	001-A-PACS.EX.01 - User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader. The reader cannot process the information provided from the wallet/container on the mobile phone/tablet. Turnstile gate does not open. END 001-A-PACS.EX.02 - User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader. Validation of the user's PIV PKI certificate cannot be achieved. This validation failure should address certificates that are expired, revoked, or have not been granted access rights. Turnstile gate does not open. END.
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements
Assumptions:	1. PACS hardware, devices, and configuration align to the APL on idmanagement.gov and can read required attributes on the mobile phone/tablet 2. Readers can ONLY read the required PKI certificates on the mobile phone/tablet and all other data on the phone is ignored 3. mobile phone/tablet provides access to the PKI certificates in the wallet/container, and all other data on the phone is inaccessible
Notes and Issues:	

Use Case ID:	002-A-APP&SYS		
Use Case Name:	Mobile phone authentication to workstation or web applications using the x509 authentication certificate.		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/8/22	**Date Last Updated:**	7/13/22

Actor:	Agency Personnel
Description:	Agency personnel uses mobile phone/tablet to access workstation or federated single sign-on (SSO) for web applications.
Preconditions:	1. User has an existing PIV card/account that is active 2. PIV PKI certificates have been provisioned to the wallet/container on the users mobile phone 3. Workstation and web applications are PKI enabled.
Postconditions:	1. User successfully authenticates on to their workstation and/or web applications.
Priority:	High
Frequency of Use:	Average: Twice daily, 5 days a week, 48 weeks a year
Normal Course of Events:	1. User attempts to access an workstation or web application. Workstation or web application allows for multi credentials for authentication and presents user with choice of credentials inside user's digital wallet on their mobile phone/tablet. 2. The workstation or web application validates the user's PIV PKI certificate on the phone/tablet. 3. The workstation and/or web application successfully validates the certificate, user is granted access 4. END.
Alternative Courses:	
Exceptions:	002-A-APP&SYS.EX.01 - User attempts to access a web application. The web application is not PKI enabled. User is not granted access to application or system. END 002-A-APP&SYS.EX.02 - User attempts to access workstation or web application. The workstation or web application only allows for authentication via credential not contained in user's digital wallet. User is not granted access to application or system. END 002-A-APP&SYS.EX.03 - User attempts to access workstation or web application. The workstation or web application cannot authenticate the PIV certificate because it has been revoked or is expired. User is not granted access to application or system. END
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements
Assumptions:	1. Workstation or web application can ONLY read the required PKI certificates on the mobile phone/tablet and all other data on the phone is ignored 2. Workstation or web application provides access to the PKI certificates in the wallet/container, and all other data on the phone is inaccessible.
Notes and Issues:	

Use Case ID:	002-B-APP&SYS		
Use Case Name:	Mobile phone authentication to workstation or web applications using FIDO2 credentials.		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/8/22	**Date Last Updated:**	7/13/22

Actor:	Agency Personnel
Description:	Agency personnel uses mobile phone/tablet to access workstation or federated single sign-on (SSO) for web applications.
Preconditions:	1. User has an existing PIV card/account that is active 2. FIDO2 credentials have been provisioned to the wallet/container on the users mobile phone 3. Workstation and web applications are FIDO2 enabled.
Postconditions:	1. User successfully authenticates on to their workstation and/or web applications.
Priority:	High
Frequency of Use:	Average: Twice daily, 5 days a week, 48 weeks a year
Normal Course of Events:	1. User attempts to access an workstation or web application. Workstation or web application allows for multi credentials for authentication and presents user with choice of credentials inside user's digital wallet on their mobile phone/tablet. 2. The workstation or web application validates the FIDO2 credentials on the phone/tablet. 3. Once the workstation or web application successfully validates the credential, user is granted access 4. END.
Alternative Courses:	
Exceptions:	002-B-APP&SYS.EX.01 - User attempts to access a web application. The web application is not FIDO2 enabled. User is not granted access to application or system. END 002-B-APP&SYS.EX.02 - User attempts to access workstation or web application. The workstation or web application only allows for authentication via credential not contained in user's digital wallet. User is not granted access to application or system. END 002-B-APP&SYS.EX.03 - User attempts to access workstation or web application. The workstation or web application cannot authenticate the FIDO2 credential because it has been revoked or the credential has not been granted access rights. User is not granted access to application or system. END
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements
Assumptions:	1. Readers can ONLY interact with the FIDO2 credential on the mobile phone/tablet and all other data on the phone is ignored
Notes and Issues:	

Use Case ID:	003-A-TEMP (PIV-I)		
Use Case Name:	Mobile phone/tablet authentication for temporary personnel utilizing x509 authentication certificate. (PIV-I)		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/8/22	**Date Last Updated:**	7/13/22

Actor:	Agency Personnel
Description:	Agency personnel who are inelligible for PIV (IAL3) uses mobile phone/tablet with suitable PIV-I credentials to authenticate and gain access to their agency workstation and/or web application.
Preconditions:	1. User has an existing PIV-I card/account that is active 2. PIV-I PKI certificates have been provisioned to the wallet/container on the users mobile phone 3. Workstation and web applications are PKI enabled.
Postconditions:	1. User successfully authenticates their mobile phone/tablet against the their agency's workstation or web application.
Priority:	High
Frequency of Use:	Average: Twice daily, 5 days a week, 48 weeks a year
Normal Course of Events:	1. User attempts to access an workstation or web application. Workstation or web application allows for multi credentials for authentication and presents user with choice of credentials inside user's digital wallet on their mobile phone/tablet. 2. The workstation or web application validates the user's PIV-I PKI certificate on the phone/tablet. 3. The workstation and/or web application successfully validates the certificate, user is granted access 4. END.
Alternative Courses:	
Exceptions:	003-A-TEMP.EX.01 - User attempts to access a web application. The web application is not PKI enabled. User is not granted access to application or system. END 003-A-TEMP.EX.02 - User attempts to access workstation or web application. The workstation or web application only allows for authentication via credential not contained in user's digital wallet. User is not granted access to application or system. END 003-A-TEMP.EX.03 - User attempts to access workstation or web application. The workstation or web application cannot authenticate the PIV-I certificate because it has been revoked or is expired. User is not granted access to application or system. END
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements.
Assumptions:	1. Workstation or web application can ONLY read the required PKI certificates on the mobile phone/tablet and all other data on the phone is ignored 2. Workstation or web application provides access to the PKI certificates in the wallet/container, and all other data on the phone is inaccessible
Notes and Issues:	

Use Case ID:	004-A-PACSTEMP (PIV-I)		
Use Case Name:	Mobile phone authentication to physical access control systems, providing access to a building using a PIV-I certificate.		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/8/22	**Date Last Updated:**	7/13/22

Actor(s):	Agency Personnel
Description:	Agency personnel is inelligible for PIV (IAL3). Agency personnel uses mobile phone with x509 authentication certificates to authenticate and gain access (entrance) to their agency facility via PACS.
Preconditions:	1. User is not eligible for PIV 2. User is able to meet identity proofing standard for access to workstation or web application assurance levels (AAL2) 3. Authentication methods aligns with NIST Security Control Overlay of SP 800-53 REV 5.
Postconditions:	1. User successfully authenticates their mobile phone/tablet against the building PACS and gains access to the building.
Priority:	Medium
Frequency of Use:	Average: Twice daily, 5 days a week, 2 weeks a year
Normal Course of Events:	1. User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader 2. The reader validates the PIV-I PKI certificate on the phone and validates the credential is authorized for access. 3. Access is granted. 4. END.
Alternative Courses:	
Exceptions:	004-A-PACSTEMP.EX.01 - User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader. The reader cannot process the information provided from the wallet/container on the mobile phone/tablet. Turnstile gate does not open. END 004-A-PACSTEMP.EX.02 - User walks up to the PACS turnstile and holds mobile phone/tablet up to the PACS reader. Validation of the user's PIV PKI certificate cannot be achieved. This validation failure should address certificates that are expired, revoked, or have not been granted access rights. Turnstile gate does not open. END.
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements.
Assumptions:	1. PACS hardware, devices, and configuration align to the APL on idmanagement.gov and can read required attributes on the mobile phone/tablet 2. Readers can ONLY read the required PKI certificates on the mobile phone/tablet and all other data on the phone is ignored 3. Mobile phone provides access to the PKI certificates in the wallet/container, and all other data on the phone is inaccessible.
Notes and Issues:	

Use Case ID:	005-A-PROV		
Use Case Name:	Credentials provisioned to wallet/container on the mobile phone/tablet.		
Created By:	S. Nedd	**Last Updated By:**	S. Nedd
Date Created:	6/15/22	**Date Last Updated:**	7/13/22

Actor(s):	Issuer / Agency Personnel
Description:	Issuer provisions credentials to the PIV wallet on the mobile phone/tablet.
Preconditions:	1. User was determined PIV-eligible 2. PIV wallet (application) was downloaded to the mobile phone/tablet. 3. FIDO2 credentials downloaded to the mobile phone/tablet.
Postconditions:	1. Credentials are provisioned to the mobile wallet.
Priority:	High
Frequency of Use:	As needed
Normal Course of Events:	1. Issuer recieves notification that a user with a PIV account was issued a mobile phone and/or tablet 2. Issuer also receives notification of what credentials to provision to the mobile phone and/or tablet 3. Issuer provisions the requested derived/alternate credentials to the PIV wallet on the mobile phone and/or tablet 4. User's PIV account is updated with information regarding derived/alternate credentials 5. END.
Alternative Courses:	
Exceptions:	
Includes (Non-Functional):	
Special Requirements:	1. Performance requirements.
Assumptions:	1. The PIV wallet/application exists 2. The PIV wallet/application can be downloaded to the mobile/phone by the issuer.
Notes and Issues:	Executing use cases UC 001 and UC 002 can validate that credentials have been provisioned.