

## 5 Mapping

Mapping is the process of taking the functional requirements defined in [FRTC] and allocating them into the FIPS 201 Evaluation Program categories, and then indicating the specific components within your solution that perform the operations for that requirement. For example, if the requirement is for a product to validate signatures as defined in [FRTC] §2.1-Test 2.1.1, the Applicant should follow the example given in Table 1 below.

**Table 1 Example Mapping Table for Time of Individual Registration Signature Verification**

Test	Requirement	Category(ies)	Component(s)	Process
2.1	<b>Signature Verification</b>			
2.1.1	Verify products ability to validate signatures in the certificates found in the certification path for a PIV credential	PACS and Validation Infrastructure	PVA Controllers	EE certificate signature is validated immediately by the PACS and Validation Infrastructure. The CA certificate signatures are evaluated, but may be cached by the path discovery and validation engine if they have been previously seen.

In the example provided in Table 1, the signature verification is performed by the PVI. It involves both PACS and validation functions of the PVA software. The PACS function is providing the registration capability and the validation function is doing the PKI signature verification of the end entity, and the PDVAL engine is evaluating signatures and potentially caching status for the CA certificate path. Clearly there are many potential combinations for how this function could be performed. It is up to the applicant to describe the process of how, when and where [FRTC] requirements are met in their submitted Topology Mapping.

Table 2 below provides the PACS 13.02 topology mapping of functional requirements identified in the [FRTC] to the FIPS 201 Evaluation Program categories as defined in this document. The columns for *Category(ies)*, *Components* and *Process* are intentionally left blank in this table. **These three columns must be completed by the Applicant when submitting a component/solution to the FIPS 201 Evaluation Program for evaluation, testing, and approval.**

**Table 2 Topology Mapping for the PACS 13.02 Topology**

Test	Requirement	Category(ies)	Component(s)	Process
2	<b>Requirements at Time of In-Person Registration In Accordance With [E-PACS] PIA-9</b>			
<b>2.1</b>	<b>Signature Verification</b>			
2.1.1	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV credential.			
2.1.2	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV-I credential.			
2.1.3	Verify product’s ability to recognize invalid signature on an intermediate CA in the certification path.			
2.1.4	Verify product’s ability to recognize invalid signature on the End Entity certificate.			
2.1.5	Verify product’s ability to recognize certificate/private key mismatch.			
<b>2.2</b>	<b>Certificate Validity Periods</b>			

Test	Requirement	Category(ies)	Component(s)	Process
2.2.1	Verify product's ability to reject a credential when <i>notBefore</i> date of the intermediate CA certificate is sometime in the future.			
2.2.2	Verify product's ability to reject a credential when <i>notAfterDate</i> of the End Entity Signing CA is sometime in the past.			
2.2.3	Verify product's ability to reject a credential when <i>notBefore</i> date of the End Entity certificate is sometime in the future.			
2.2.4	Verify product's ability to reject a credential when <i>notAfter</i> date of the intermediate certificate is sometime in the past.			
2.2.5	Verify product's ability to reject a credential when <i>notAfter</i> date of the End Entity certificate is sometime in the past.			
<b>2.3</b>	<b>Name Chaining</b>			
2.3.1	Verify product's ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.			
<b>2.4</b>	<b>Basic Constraints Verification</b>			

Test	Requirement	Category(ies)	Component(s)	Process
2.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing <i>basicConstraints</i> extension.			
2.4.4	Verify product's ability to recognize when the first certificate in the path includes <i>basicConstraints</i> extension with a <i>pathLenConstraint</i> of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.			
2.4.5	Verify product's ability to detect a mismatched SKID with the subject public key in the certificate.			
<b>2.5</b>	<b>Key Usage Verification</b>			
2.5.1	Verify product's ability to recognize when the intermediate certificate includes a <i>keyUsage</i> extension in which <i>keyCertSign</i> is false.			
2.5.3	Verify product's ability to recognize when the intermediate certificate includes a <i>keyUsage</i> extension in which <i>crlSign</i> is false.			
<b>2.6</b>	<b>Certificate Policies</b>			

Test	Requirement	Category(ies)	Component(s)	Process
2.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware by the relying party solution.			
2.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).			
2.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware by the relying party solution. Test Condition: production PIV passes.			

Test	Requirement	Category(ies)	Component(s)	Process
2.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.			
2.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).			
2.6.8	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path that includes a <i>policyConstraints</i> extension with <i>inhibitPolicyMapping</i> set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.			

Test	Requirement	Category(ies)	Component(s)	Process
<b>2.7</b>	<b>Generalized Time</b>			
2.7.1	Verify product's ability to process valid use of generalized time post year 2049 in the path.			
2.7.2	Verify product's ability to process invalid use of generalized time before year 2049 in the path.			
<b>2.8</b>	<b>Name Constraints</b>			
2.8.1	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.			
2.8.2	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.			

Test	Requirement	Category(ies)	Component(s)	Process
2.8.3	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and <i>subjectAltName</i> with a DN that falls outside that subtree.			
<b>2.9</b>	<b>Certificate Revocation Tests (CRL)</b>			
2.9.1	The system recognizes when no revocation information is available for the End Entity certificate			
2.9.2	The system recognizes when a second intermediate CA certificate is revoked.			
2.9.3	The system recognizes when the End Entity certificate is revoked.			
2.9.4	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.			
2.9.5	The system recognizes when a certificate in the path points to a CRL with an expired <i>nextUpdate</i> value (an expired CRL).			
2.9.6	The system recognizes when a certificate in the path points to a CRL with a <i>notBefore</i> Date in the future.			

Test	Requirement	Category(ies)	Component(s)	Process
2.9.7	The system recognizes when a certificate in the path has an incorrect CRL distribution point.			
2.9.8	The system recognizes when the CRL has an invalid signature.			
2.9.9	The system recognizes when an incorrectly formatted CRL is present in the path.			
2.9.10	The system recognizes when an invalid CRL signer is in the path.			
<b>2.10</b>	<b>CHUID Verification</b>			
2.10.1	The system recognizes when the CHUID signature is invalid and does not verify.			
2.10.2	The system recognizes when the CHUID signer certificate is expired.			
2.10.3	The system recognizes when the CHUID is expired.			
2.10.4	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.			
2.10.5	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I Auth Cert.			

Test	Requirement	Category(ies)	Component(s)	Process
2.10.6	The system recognizes when the PKI-AUTH certificate expires after the CHUID expiration date.			
2.10.7	The system recognizes when the CHUID expiration date is after the CHUID signer certificate expiration date.			
2.10.8	The system recognizes when an intermediate certificate in the CHUID signer certificate path is expired.			
2.10.9	The system recognizes when an intermediate certificate in the CHUID signer certificate path is revoked.			
<b>2.11</b>	<b>Facial Image Verification</b>			
2.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.			
<b>2.12</b>	<b>Copied Containers</b>			
2.12.1	The system recognizes when the FASC-N in the PKI-CAK certificate does not equal the FASC-N in the PIV Auth Cert.			
2.12.2	The system recognizes when the UUID in the PKI-CAK certificate does not equal the UUID in the PIV-I Auth Cert.			

Test	Requirement	Category(ies)	Component(s)	Process
2.12.3	The system recognizes when the FASC-N in the Facial Image does not equal the FASC-N in the PIV Auth Cert.			
2.12.4	The system recognizes when the UUID in the Facial Image does not equal the UUID in the PIV-I Auth Cert.			
<b>2.13</b>	<b>FINGERPRINT Verification</b>			
2.13.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).			
2.13.2	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).			
2.13.3	Verify Product's ability to accept a valid credential with a matching fingerprint.			
2.13.4	Verify Product's ability to reject a valid credential with a non-matching fingerprint.			
2.13.5	The system recognizes when the FASC-N in the Fingerprint does not equal the FASC-N in the PIV Auth Cert.			

Test	Requirement	Category(ies)	Component(s)	Process
2.13.6	The system recognizes when the UUID in the Fingerprint does not equal the UUID in the PIV-I Auth Cert			
<b>2.14</b>	<b>Security Object Verification</b>			
2.14.1	The system recognizes when the Security Object signature is invalid and does not verify.			
<b>2.15</b>	<b>OCSP Response Checking</b>			
2.15.1	The system successfully validates a good credential using an OCSP response with a good signature			
2.15.2	Validation fails using an OCSP Responder with an expired signature certificate for a good card.			
2.15.3	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.			
2.15.4	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.			

Test	Requirement	Category(ies)	Component(s)	Process
2.15.5	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.			
<b>2.16</b>	<b>Interoperability Testing</b>			
2.16.1	Various valid PIV (including CAC) and PIV-I cards can be individually registered using PKI-AUTH method.			
<b>2.17</b>	<b>Cryptography Testing</b>			
2.17.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).			
2.17.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).			
2.17.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).			
2.17.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).			
2.17.7	Verify Product's ability to validate signatures using ECDSA (P-256).			

Test	Requirement	Category(ies)	Component(s)	Process
2.17.8	Verify Product's ability to validate signatures using ECDSA (P-384).			
2.17.10	Verify Product's ability to validate signatures using SHA-256.			
2.17.11	Verify Product's ability to validate signatures using SHA-384.			
2.17.12	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.			
2.17.13	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of $2^{256}-1$ .			
2.17.14	Verify product's ability to validate signatures using RSA 4096 in the path.			
<b>2.18</b>	<b>Discovery Object &amp; PIN Usage Policy</b>			
2.18.1	Discovery object not present. Confirm E-PACS is using Application PIN.			
2.18.2	Discovery object not present. Confirm E-PACS is using the Application PIN.			

Test	Requirement	Category(ies)	Component(s)	Process
2.18.3	Discovery object present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.			
2.18.4	Discovery object is present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.			
2.18.5	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.			
2.18.6	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.			
2.18.7	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.			
2.18.8	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.			

Test	Requirement	Category(ies)	Component(s)	Process
2.18.9	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.			
2.18.10	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.			
2.18.11	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.			
<b>3</b>	<b>Dual Chip Card, time of registration</b>			
<b>3.1</b>	<b>CHUID Verification (Contactless chip on a 2 chip card)</b>			
3.1.1	The system recognizes when the CHUID signature is invalid and does not verify.			
3.1.2	The system recognizes when the CHUID signer certificate is expired.			
3.1.3	The system recognizes when the CHUID is expired.			

Test	Requirement	Category(ies)	Component(s)	Process
3.1.4	The system recognizes when the PKI-CAK certificate expires after the CHUID expiration date.			
<b>3.2</b>	<b>Copied Containers</b>			
3.2.1	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV PKI-CAK Cert.			
3.2.2	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV-I PKI-CAK Cert.			
<b>3.3</b>	<b>Signature Verification (Contactless chip on a 2 chip card)</b>			
3.3.1	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.			
3.3.2	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.			
3.3.3	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.			
3.3.4	Verify product's ability to recognize invalid signature on the End Entity certificate.			

Test	Requirement	Category(ies)	Component(s)	Process
3.3.5	Verify product’s ability to recognize certificate/private key mismatch.			
<b>4</b>	<b>Requirements for Automated Provisioning In Accordance With [E-PACS] PIA-8</b>			
<b>4.1</b>	<b>Dual Interface Chip Card</b>			
4.1.1	The E-PACS shall accept automated provisioning from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.			
4.1.2	The E-PACS shall accept automated de-provisioning from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.			
<b>4.2</b>	<b>Dual Chip Card</b>			
4.2.1	The E-PACS shall accept automated provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in the detailed guidance of PIA-8.			

Test	Requirement	Category(ies)	Component(s)	Process
4.2.2	The E-PACS shall accept automated de-provisioning of the contactless CAK from a source it trusts and that complies with the security requirements described in PIA-3.5 and PIA-3.6.			
<b>5</b>	<b>Authentication at Time of Access Test Cases</b>			
<b>5.1</b>	<b>Signature Verification</b>			
5.1.1	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.			
5.1.2	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.			
5.1.3	Verify product's ability to recognize invalid signature on an intermediate CA in the certification path.			
5.1.4	Verify product's ability to recognize invalid signature on the End Entity certificate.			
5.1.5	Verify product's ability to recognize manipulated keys.			

Test	Requirement	Category(ies)	Component(s)	Process
5.1.6	Verify product's ability to recognize public key from card does not match public key previously registered to the system.			
<b>5.2</b>	<b>Certificate Validity Periods</b>			
5.2.1	Verify product's ability to reject a credential when <i>notBefore</i> date of the intermediate CA certificate is sometime in the future.			
5.2.2	Verify product's ability to reject a credential when <i>notBefore</i> date of the End Entity certificate is sometime in the future.			
5.2.3	Verify product's ability to reject a credential when <i>notAfter</i> date of the intermediate certificate is sometime in the past.			
5.2.4	Verify product's ability to reject a credential when <i>notAfter</i> date of the End Entity certificate is sometime in the past.			
<b>5.3</b>	<b>Name Chaining</b>			
5.3.1	Verify product's' ability to reject a credential when common name portion of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.			
<b>5.4</b>	<b>Basic Constraints Verification</b>			

Test	Requirement	Category(ies)	Component(s)	Process
5.4.1	Verify product's ability to recognize when the intermediate CA certificate is missing <i>basicConstraints</i> extension.			
5.4.4	Verify product's ability to recognize when the first certificate in the path includes <i>basicConstraints</i> extension with a <i>pathLenConstraint</i> of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.			
5.4.5	Verify product's ability to detect a mismatched SKID with the subject public key in the certificate.			
<b>5.5</b>	<b>Key Usage Verification</b>			
5.5.1	Verify product's ability to recognize when the intermediate certificate includes a <i>keyUsage</i> extension in which <i>keyCertSign</i> is false			
5.5.3	Verify product's ability to recognize when the intermediate certificate includes a <i>keyUsage</i> extension in which <i>crlSign</i> is false.			
<b>5.6</b>	<b>Certificate Policies</b>			

Test	Requirement	Category(ies)	Component(s)	Process
5.6.1	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV Hardware by the relying party solution.			
5.6.2	With the trust anchor set to Common Policy check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set by the relying party solution to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).			
5.6.3	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to Medium Hardware by the relying party solution. Test Condition: production PIV passes.			

Test	Requirement	Category(ies)	Component(s)	Process
5.6.4	With the trust anchor set so the certificate path requires trust across the Federal Bridge to the CertiPath Root CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4) by the relying party solution.			
5.6.5	With Common Policy anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate - however, is present somewhere in the certificate path. The explicit policy will be set by the relying party solution to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).			
5.6.8	With required policy set to 2.16.840.1.101.3.2.1.48.11 (test id-fpki-common-authentication), verify product's ability to process a path that includes a <i>policyConstraints</i> extension with <i>inhibitPolicyMapping</i> set to 0 which invalidates the ICAM Test Bridge to ICAM Root CA policy mappings.			

Test	Requirement	Category(ies)	Component(s)	Process
<b>5.7</b>	<b>Generalized Time</b>			
5.7.1	Verify product's ability to process valid use of generalized time post year 2049 in the path.			
5.7.2	Verify product's ability to process invalid use of generalized time before year 2049 in the path.			
<b>5.8</b>	<b>Name Constraints</b>			
5.8.1	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.			
5.8.2	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.			

Test	Requirement	Category(ies)	Component(s)	Process
5.8.3	The system recognizes when the intermediate certificate includes a <i>nameConstraints</i> extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and <i>subjectAltName</i> with a DN that falls outside that subtree.			
<b>5.9</b>	<b>Certificate Revocation Tests (CRL)</b>			
5.9.1	The system recognizes when no revocation information is available for the End Entity certificate.			
5.9.2	The system recognizes when a second intermediate CA certificate is revoked.			
5.9.3	The system recognizes when the End Entity certificate is revoked.			
5.9.4	The system recognizes when the CRL has an invalid signature.			
5.9.5	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.			
5.9.6	The system recognizes when a certificate in the path has an expired <i>nextUpdate</i> value (an expired CRL).			

Test	Requirement	Category(ies)	Component(s)	Process
5.9.7	The system recognizes when a certificate in the path points to a CRL with a <i>notBefore</i> Date in the future.			
5.9.8	The system recognizes when a certificate in the path has an incorrect CRL distribution point.			
<b>5.11</b>	<b>Facial Image Verification</b>			
5.11.1	The system recognizes when the Facial Image signature is invalid and does not verify.			
<b>5.12</b>	<b>FINGERPRINT Verification</b>			
5.12.1	The system recognizes when the Fingerprint signature is invalid and does not verify (using CHUID content signer certificate).			
5.12.2	The system recognizes when the Fingerprint signature is invalid and does not verify (using biometric object signer certificate).			
5.12.3	Verify Product's ability to accept a valid credential with a matching fingerprint.			

Test	Requirement	Category(ies)	Component(s)	Process
5.12.4	Verify Product's ability to reject a valid credential with a non-matching fingerprint.			
<b>5.13</b>	<b>Security Object Verification</b>			
5.13.1	The system recognizes when the Security Object signature is invalid and does not verify.			
<b>5.14</b>	<b>OCSP Response Checking</b>			
5.14.1	The system successfully validates a good credential using an OCSP response with a good signature.			
5.14.2	Validation fails using an OCSP Responder with an expired signature certificate for a good card.			
5.14.3	Validation succeeds using an OCSP Responder with a revoked signature certificate for a good card with PKIX_OCSP_NOCHECK present.			
5.14.4	Validation fails using an OCSP Responder with a revoked signature certificate for a good card without PKIX_OCSP_NOCHECK present.			

Test	Requirement	Category(ies)	Component(s)	Process
5.14.5	Validation fails using an OCSP Responder with a signature certificate containing an invalid signature for a good card.			
<b>5.15</b>	<b>Interoperability Testing</b>			
5.15.1	Various valid PIV (including CAC) and PIV-I cards are granted access using PKI-AUTH method.			
<b>5.16</b>	<b>Cryptography testing</b>			
5.16.2	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).			
5.16.3	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).			
5.16.5	Verify Product's ability to validate signatures using RSASSA-PSS (2048).			
5.16.6	Verify Product's ability to validate signatures using RSASSA-PSS (3072).			
5.16.7	Verify Product's ability to validate signatures using ECDSA (P-256).			

Test	Requirement	Category(ies)	Component(s)	Process
5.16.8	Verify Product's ability to validate signatures using ECDSA (P-384).			
5.16.10	Verify Product's ability to validate signatures using SHA-256.			
5.16.11	Verify Product's ability to validate signatures using SHA-384.			
5.16.12	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of 65,537.			
5.16.13	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048) w/exponent of $2^{256}-1$ .			
5.16.14	Verify product's ability to validate signatures using RSA 4096 in the path.			
<b>5.17</b>	<b>Discovery Object &amp; PIN Usage Policy</b>			
5.17.1	Discovery object not present. Confirm E-PACS is using Application PIN.			
5.17.2	Discovery object not present. Confirm E-PACS is using the Application PIN.			
5.17.3	Discovery object present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.			

Test	Requirement	Category(ies)	Component(s)	Process
5.17.4	Discovery object is present and set for PIV App PIN only. Confirm E-PACS is using the Application PIN.			
5.17.5	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.			
5.17.6	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.			
5.17.7	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Application PIN.			
5.17.8	Discovery object is present. PIV App and Global PINs are available. PIV App PIN is primary. Confirm E-PACS is using the Global PIN.			
5.17.9	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.			

Test	Requirement	Category(ies)	Component(s)	Process
5.17.10	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.			
5.17.11	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Application PIN.			
5.17.12	Discovery object is present. PIV App and Global PINs are available. Global PIN is primary. Confirm E-PACS is using the Global PIN.			
5.17.13	Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using Application PIN.			
5.17.14	Discovery object is present and tag 0x5F2F is not populated. Confirm E-PACS is using the Application PIN.			
<b>6</b>	<b>Dual Chip Card, time of access</b>			
<b>6.2</b>	<b>Signature Verification (Contactless chip on a 2 chip card)</b>			
6.2.1	Verify product's ability to validate signatures in the certificates found in the certification path for a PIV credential.			

Test	Requirement	Category(ies)	Component(s)	Process
6.2.2	Verify product’s ability to validate signatures in the certificates found in the certification path for a PIV-I credential.			
6.2.3	Verify product’s ability to recognize invalid signature on an intermediate CA in the certification path.			
6.2.4	Verify product’s ability to recognize invalid signature on the End Entity certificate.			
6.2.5	Verify product’s ability to recognize certificate/private key mismatch.			
<b>7</b>	<b>PACS Design Use Cases</b>			
<b>7.1</b>	<b>Continuity of Operations Testing</b>			
7.1.1	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.			
7.1.2	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for a valid credential.			

Test	Requirement	Category(ies)	Component(s)	Process
7.1.3	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for a valid credential.			
7.1.4	The network connection is dropped to individual components within the solution individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.			
7.1.5	Individual component services within the solution are stopped individually, in sequence. Degraded mode shall honor requirements for authentication factors and authorizations for an invalid credential.			
7.1.6	Power is removed and immediately restored to individual components within the solution, in sequence. Solution shall recover and honor requirements for authentication factors and authorizations for an invalid credential.			
<b>7.2</b>	<b>Security Boundaries</b>			

Test	Requirement	Category(ies)	Component(s)	Process
7.2.1	...all security relevant processing shall be performed inside the secure perimeter. No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.			
7.2.2	...compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself.			
<b>7.3</b>	<b>Registering Physical Access Privileges</b>			
7.3.1	Shall be able to define populations (validities) such as "guest, visitor, and regular access".			
7.3.2	Shall be able to define: Access points for each population.			
7.3.3	Shall be able to define: Temporal access rules for each population.			
7.3.4	Shall be able to define: Authentication mode required to support 7.3.2 and 7.3.3.			
<b>7.4</b>	<b>PKI Configuration</b>			

Test	Requirement	Category(ies)	Component(s)	Process
7.4.1	The solution shall provide the means to select which X.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.			
7.4.2	The solution shall provide the means to select and manage Trust Anchors. This configuration will reflect the customer's PKI relying party policy.			
7.4.3	The solution may provide configuration options to ignore PKI faults in certificates (end-entity up to trust anchor). This configuration will reflect the customer's PKI relying party policy.			
7.4.4	For every event where a PKI fault is identified, the solution shall check configuration options to ignore the identified fault. If configuration allows the solution to ignore the fault, the solution shall ignore the fault and produce a warning in the audit log and store the certificate in a certificate store of failed certificates. The audit log shall indicate what failed and provide sufficient information to link the log entry to the stored certificate.			

Test	Requirement	Category(ies)	Component(s)	Process
7.4.5	If PKI faults are allowed, the solution shall provide a means to generate a report and consolidate failed certificates for transmission to appropriate parties by email. Running the report and sending the email shall be per the customer’s PKI relying party policy.			
7.4.6	The system shall check that the issuing certificate authority has not placed the certificate on its certificate revocation list (CRL) within the previous 6 hours.			
7.4.7	The system shall process revocation progression from OCSP to HTTP CRL. If the system leverages SCVP in lieu of OCSP or HTTP CRL, and SCVP is unavailable, it should support the progression from OCSP to HTTP CRL.			
<b>7.5</b>	<b>Credential Number Specifications</b>			
7.5.1	The solution shall support FICAM conformant 128-bit FASC-N credential numbers as specified in <i>Table 3</i> for Time of Registration, Time of Access, and Automated Provisioning.			

Test	Requirement	Category(ies)	Component(s)	Process
7.5.2	The solution shall support FICAM conformant 128-bit UUID credential numbers as specified in <i>Table 3</i> for Time of Registration, Time of Access, and Automated Provisioning.			
<b>7.6</b>	<b>Validation at Time of Access</b>			
7.6.2	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Interface Chip card.			
7.6.3	Shall support BIO.			
7.6.4	Shall support PIV Authentication Key + PIN (PKI-AUTH).			
7.6.5	Shall support PIV Authentication Key + PIN + BIO (PKI-AUTH+BIO).			
7.6.6	Shall support Card Authentication Key + PIN + BIO (PKI-CAK+BIO).			
7.6.7	Shall support PKI-CAK + BIO to PACS.			
7.6.8	Shall support PKI-AUTH + BIO to PACS.			
7.6.9	Shall support contact Card Authentication Key (PKI-CAK) for Dual Interface Chip card.			

Test	Requirement	Category(ies)	Component(s)	Process
7.6.10	Shall support contactless Card Authentication Key (PKI-CAK) for Dual Chip card.			
7.6.11	E-PACS portal solutions shall not support legacy technologies when configured for approved FICAM modes.			
7.6.12	Shall support PKI-CAK + PIN to PACS.			
7.6.13	E-PACS portal solutions shall not support legacy PIV authentication modes when in approved FICAM configuration.			
<b>7.7</b>	<b>Portal Hardware</b>			
7.7.1	Product shall support Reader to PACS communications using bi-directional technology. This includes a minimum of one of RS-485, Ethernet, and secure wireless.			
7.7.2	For multi-factor readers, applicant's system must allow an administrator to modify an individual reader's authentication mode (authentication factors) from the server or a client/workstation to the server.			

Test	Requirement	Category(ies)	Component(s)	Process
7.7.3	For multi-factor readers, applicant's system must allow an administrator to modify a group of readers' authentication mode (authentication factors) from the server or a client/workstation to the server.			
7.7.4	For multi-factor readers, the site administrator shall not be required to approach and touch each reader to change its authentication mode (authentication factors).			
7.7.5	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) on a time based schedule.			
7.7.6	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) on a time based schedule.			
7.7.7	For multi-factor readers, the system shall support dynamic assignment of an individual reader's authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.			

Test	Requirement	Category(ies)	Component(s)	Process
7.7.8	For multi-factor readers, the system shall support dynamic assignment of a group of readers' authentication mode (authentication factors) based on Threat Condition, Force Protection Condition, Maritime Security Level, or other similar structured emergency response protocol.			
7.7.9	Contact readers shall support ISO/IEC 7816.			
7.7.10	Contactless readers shall support ISO/IEC 14443 Type A.			
7.7.11	ISO/IEC 14443 Type A contactless readers shall not activate and operate with a PIV card beyond 10cm.			
7.7.12	ISO/IEC 14443 Type A contactless readers shall provide sufficient field strength to activate and operate with a PIV card at or below 3.5cm.			
7.7.13	The System shall protect the communications between readers and the PACS using a cryptographically secure protocol.			

Test	Requirement	Category(ies)	Component(s)	Process
7.7.14	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered non-compliant.			
<b>7.8</b>	<b>Auditing and Logging</b>			
7.8.1	Granularity of auditing records shall be to the card and individual transaction. These shall be easily verifiable through a reporting tool or any other log and audit viewing capability.			
7.8.2	The product shall provide auditing/logging of all PKI processing to include: <ul style="list-style-type: none"> <li>• Pass/fail from a Challenge/Response</li> <li>• PDVAL</li> <li>• Disabling credential based on PDVAL, expiration, or revocation status</li> </ul>			
7.8.3	The product shall provide auditing/logging of credential number processing and transmission.			
7.8.4	The product shall provide auditing/logging of all software driven configuration changes.			
7.8.5	The product shall provide auditing/logging of periodic certificate PDVAL and status checking.			

Test	Requirement	Category(ies)	Component(s)	Process
7.8.6	The product shall provide auditing/logging of Card activity (e.g., 3 days of card activity).			
7.8.7	The product shall provide auditing/logging of last known location of a card in system.			
7.8.8	The product shall provide auditing/logging of PKI policies for name constraints, path constraints, and validity checks.			
7.8.9	The product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop).			
7.8.10	The product shall provide auditing/logging of what date individuals were provisioned or de-provisioned and by whom.			
7.8.11	The product shall provide auditing/logging of all readers and their modes.			
7.8.12	The product shall provide auditing/logging of configuration download status to system components.			
<b>7.9</b>	<b>Security Certification and Accreditation</b>			
7.9.1	As required by UL 294, relevant components within the solution shall have a UL 294 listing.			

Test	Requirement	Category(ies)	Component(s)	Process
7.9.2	As required by UL 1076, relevant components within the solution shall have a UL 1076 listing.			
7.9.3	As required by UL 1981, relevant components within the solution shall have a UL 1981 listing.			
7.9.4	When adding a component to an existing system under a given topology, each existing component in the existing system under that topology shall have GSA FIPS-201 Evaluation Program APL status.			
7.9.5	Each component leveraging cryptography in the system shall have FIPS 140-2 certification.			
7.9.6	All components of the solution shall be certified against [BAA] requirements.			
7.9.7	All components of the solution shall be certified against [TAA] requirements.			
<b>7.10</b>	<b>Biometric in PACS</b>			
7.10.1	Shall follow PIA-3.4 Detailed Guidance Case 3 for biometric identifiers leveraged in BIO to PACS.			
<b>7.11</b>	<b>Operational Controls</b>			

Test	Requirement	Category(ies)	Component(s)	Process
7.11.1	The system shall have the ability to enforce administrative privilege for configuration management operations.			
7.11.2	Shall authenticate administrators using a process of equivalent or greater assurance than the authentication modes supported by the system. This may be done using E-Authentication LOA-4 credentials.			
7.11.3	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.			
7.11.4	Each physical component shall be separately defined and addressable within the server user interface.			
7.11.5	The system shall support configuration downloads to relevant components.			
<b>7.12</b>	<b>Accessibility</b>			

Test	Requirement	Category(ies)	Component(s)	Process
7.12.1	All components in the end-to-end solution shall support [Sect508] of the Rehabilitation Act <sup>2</sup> .			
<b>8.</b>	<b>Handheld Requirements</b>			
<b>8.1.</b>	<b>Communications</b>			
8.1.1.	Ensure a secure connection using an encrypted wireless session using a NIST certified encryption method.			
8.1.2.	Must have built-in support for Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2).			
8.1.3.	The system has the ability to communicate using 802.11 a, b, c, g, n.			
8.1.4.	The Handheld must be able to support both 3G and 4G communications for cellular communications.			

<sup>2</sup> The FIPS 201 Evaluation Program has no jurisdiction with respect to installation of the solution in order to meet [Sect508] requirements. This attestation requires the user interface (including visual, audio, and touch) to be [Sect508] compliant for all components within the end-to-end solution.

Test	Requirement	Category(ies)	Component(s)	Process
8.1.5.	Handheld must have the ability to demonstrate the option to select a primary communication source and a secondary communication source.			
8.1.6.	Handheld must be able to failover from primary to secondary mode to maintain an online state with PACS and Validations system.			
8.1.7.	Reader provides a visual indication that the handheld is in an online or offline state.			
<b>8.2.</b>	<b>Operational Requirements</b>			
8.2.1.	The handheld must be capable of supporting contactless, contact, or both modes of authentication. Interfaces can be fully integrated or modular.			
8.2.2.	Contactless modes must support a minimum of: <ul style="list-style-type: none"> <li>• CAK+CHUID</li> </ul>			

Test	Requirement	Category(ies)	Component(s)	Process
8.2.3.	Contact modes must support a minimum of: <ul style="list-style-type: none"> <li>• CAK+CHUID</li> <li>• PIV+PIN</li> <li>• PIV+PIN+BIO</li> </ul>			
<b>8.3.</b>	<b>Docking Station</b>			
8.3.1.	The handheld docking station must utilize a hardwired Ethernet port or wireless communications with the Validation System, PACS, or other trusted source.			
8.3.2.	The handheld docking station provides a mechanism to securely update the handheld while cradled in the device, via hardwired Ethernet or Wireless communications.  Updates can be from online validation system, PACS or other trusted source.			
8.3.3.	Handheld must automatically logout operator when placed in docking station.			
<b>8.4.</b>	<b>FINGERPRINT Verification</b>			

Test	Requirement	Category(ies)	Component(s)	Process
8.4.1.	<ul style="list-style-type: none"> <li>• See Section 2 – Validation at time of Registration</li> <li>• See Section 5 – Validation at time of Access</li> </ul>			
<b>8.5.</b>	<b>Import Function</b>			
8.5.1.	Reader must cache CRL information locally on the handheld  This CRL data must include the Certificate PATH information and be supplied by an online Validation System or other trusted source.			
8.5.2.	Cached information must be protected either by a FIPS140-2 level -1software or Level-2 HSM.			
8.5.3.	The reader must cache authentication and authorization information for all cardholders with access to the Handheld assigned area. This information can be transferred from either an online validations system or other trusted source.			
8.5.4.	The Handheld device must have the ability to provide a visual indication when locally cached information is over 6 hours old.			

Test	Requirement	Category(ies)	Component(s)	Process
<b>8.6.</b>	<b>Operational</b>			
8.6.1.	System must automatically log the operator out of the handheld after a user defined time of non-use.			
<b>8.7.</b>	<b>Online Validation Requirements</b>			
8.7.1.	When the Handheld is online communicating with the Validations System, functional requirements defined within the Validation System category apply.			
<b>8.8.</b>	<b>Online PACS Requirements</b>			
8.8.1.	When the Handheld is online communicating with the PACS. The PACS functional requirements defined in the PACS Infrastructure category apply.			
<b>8.9.</b>	<b>Offline Validation Requirements</b>			
8.9.1.	Handheld must use locally cached authentication and authorization data to authenticate and authorize the operator.			

Test	Requirement	Category(ies)	Component(s)	Process
8.9.2.	Handheld must be able to determine the validity of the cardholder certificates using the locally cached validation data.			
8.9.3.	Handheld must provide the operator with indication that the locally stored data exceeds 6 hour refresh limit.			
8.9.4.	Handheld must cache PKI Validation decisions to be uploaded to the trusted source for archive and reporting.			
<b>8.10.</b>	<b>Offline PACS Requirements</b>			
8.10.1.	The handheld must provide an indication to the operator that the reader is in offline mode.			
8.10.2.	<p>The handheld must be able to use locally cached PACS data to verify cardholders access privileges. For example:</p> <ul style="list-style-type: none"> <li>• Schedule</li> <li>• Shift</li> <li>• Access to areas</li> </ul> <p>The operator must be provided a visual indication of access granted or denied.</p>			

Test	Requirement	Category(ies)	Component(s)	Process
8.10.3.	While in offline mode the handheld must log all access decisions made at the handheld.			
8.10.4.	When transitioning from an offline to an online state the handheld must transfer all locally stored access transaction to the PACS solution or other trusted source.			