Community Interoperability Test Environment (CITE) Participation Guidance

For

Federal PKI Affiliates

Prepared By:
The FPKI Technical Working Group (TWG)

An FPKI Policy Authority Working Group

VERSION 1.0.5

September 7, 2017

REVISION HISTORY

Date	Version	Description	Editor
8/22/14	1.0.3	Added revision history table and new testing OIDs id-fpki-common-pivAuth-derived and id-fpki-common-pivAuth-derived-hardware	Wendy Brown
6/22/16	1.0.4	Add new testing OIDs for new Treasury OIDs: id-treasury-certpcy-pivi-hardware, id-treasury-certpcy-pivi-cardAuth, id-treasury-certpcy-pivi-contentSigning	Wendy Brown
9/7/2017	1.0.5	Added new testing OIDs for "golden PIV-I" card for PACS testing	Wendy Brown

`

TABLE OF CONTENTS

1   OVERVIEW

The Federal Public Key Infrastructure (FPKI) has been the subject of various transitions and evolutions during its years of existence. This includes hardware and software upgrades, configuration and architecture changes, implementation of higher complexity keys and algorithms, and implementation of new application capabilities. The impacts on continued interoperability throughout these transitions have made it apparent that the FPKI community would benefit greatly from an integrated test environment.

The Community Interoperability Test Environment (CITE) has been established to provide the FPKI community with a test environment to: (1) identify and resolve technical issues across Affiliates PKIs, and (2) ensure proper functionality of respective system changes prior to deploying them in a production environment. Specifically, the FPKI Management Authority (FPKIMA), FPKI Affiliates, and Relying Parties (RPs) can use the CITE to evaluate the functionality, interoperability, and potential impacts of deploying software, hardware, upgrades, patches, configuration changes, infrastructure changes, and application capabilities. The use of the CITE minimizes the risk of introducing problems into each respective production environment.

The CITE is comprised of participating Affiliates' test environments cross-certified with a test instantiation of the FPKI Trust Infrastructure, mirroring the production FPKI environment.

Figure 1.1 depicts the CITE architecture, which includes the test FPKI Trust Infrastructure and two fictitious Affiliate test PKIs. It also demonstrates RPs' accessibility to the CITE repositories.
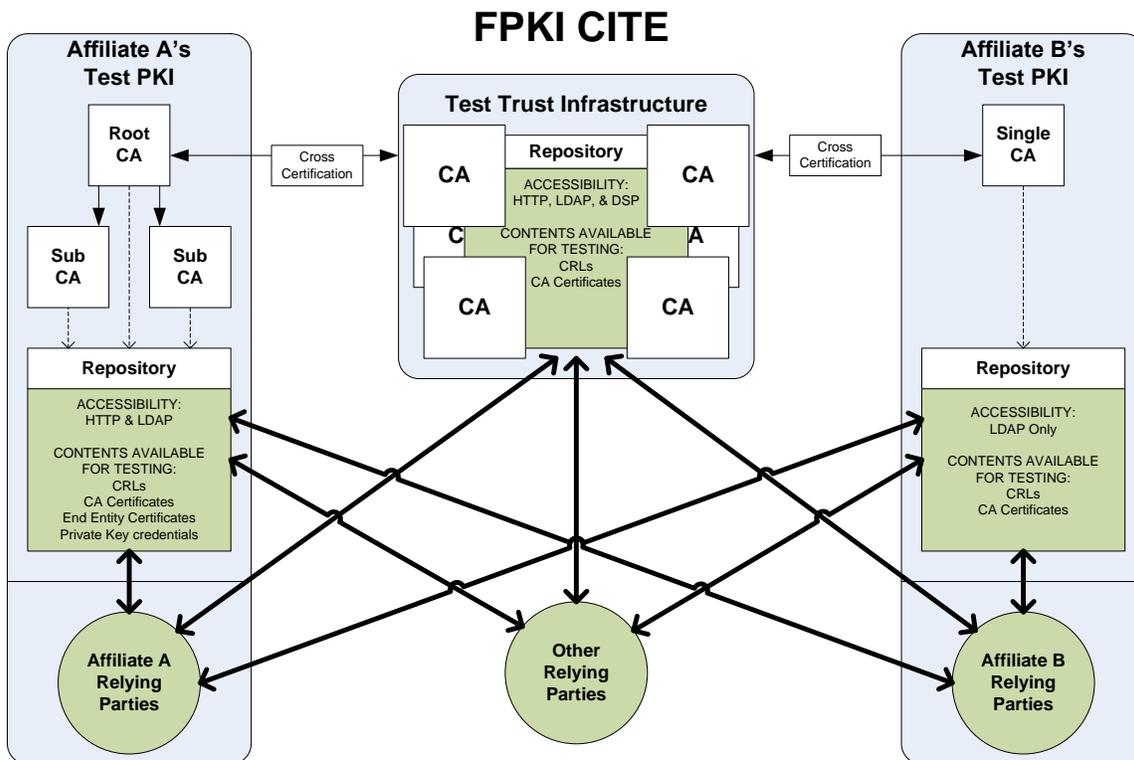
1.1   PARTICIPATION IN CITE

Any organization seeking to become an FPKI Affiliate must undergo the cross-certification process. As part of the cross-certification process, the FPKIMA performs interoperability testing. The FPKI Affiliate has the option of retaining their test environment integration with CITE, to begin their participation in the CITE.

2   SCOPE

This document serves as the CITE participation guidelines, which provides the terms and conditions of CITE participation. Participation in the CITE, for the purposes of this guidance document, refers to the establishment of a continuous test environment integrated with the CITE after becoming an FPKI Affiliate – not the temporary relationship established with the CITE during interoperability testing.

Modifications to this document and any waivers that may ensue are controlled by the FPKI Technical Working Group (TWG).

FIGURE 2.1 – FPKI CITE ARCHITECTURE

FPKI CITE

3   THE CITE VALUE

Participation in CITE is not a condition of retaining cross-certification with the production FPKI. However, the FPKI TWG encourages all FPKI Affiliates to maintain CITE participation, as there are significant benefits to the individual FPKI Affiliate and to the overall FPKI Community:

1. Each FPKI Affiliate minimizes the risk of interoperability issues in their production environment because of their PKI being available for the community to test against.
2. The more PKI environments that are readily available in the CITE, the more the CITE emulates production, which makes testing in the CITE more representative of production FPKI and therefore more valuable.
3. There are many reasons for an FPKI Affiliate to use the CITE after initial interoperability testing. An FPKI Affiliate can use the CITE to test subsequent modifications to its PKI, as well as testing RP applications (or modifications to RP applications) before deployment into production.

4   TYPES OF CITE TESTING

The CITE is available for testing infrastructure components and RP applications. Additional types of testing may be identified and conducted as necessary and to the extent supported by the CITE.

However, testing should be undertaken in a manner that provides maximum resource availability for all parties. The CITE should not be used for system stress testing.

Infrastructure testing ensures that upgrades, patches, policy changes, new products, and any other changes within the FPKI do not adversely affect interoperability.

RP application testing ensures that application modules operate as intended. In addition, the RP application testing ensures that the system as a whole performs adequately on the platform onto which the application will be deployed, and that it interoperates properly within the FPKI environment (i.e., no adverse affect within the FPKI environment).

Some examples of testing conducted in the CITE are:

- Interoperability testing between cross-certified Certification Authorities (CAs);
- Interoperability testing of chaining between directories;
- Transition testing to new algorithms (e.g., SHA-2, ECC);
- PIV-I card interoperability testing;
- Path discovery testing for a particular application; and
- Path validation testing for a particular application.

When testing is successful in the CITE, assurance is gained that the proposed change(s) will operate in a production environment as intended. When tests fail in the CITE, issues are identified and addressed without impacting the FPKI.

5   TERMS AND CONDITIONS

To ensure the CITE provides effective services and comprehensive test results, each participating FPKI Affiliate should emulate its production environment as closely as possible in the CITE. To the extent possible, the test environment should include the same products, logical architecture, and community integration relationships as in the production environment. The more similar the test environment is to the production environment, the more likely issues can be discovered and resolved earlier in the development and testing process; thus reducing operational issues in the production environment. For example, if a FPKI Affiliate includes both HTTP and LDAP URIs in its production certificates, both types of URIs should be included in its CITE test certificates, along with operational repositories corresponding to those URIs. Therefore, both methods available in production can be tested in the CITE.

5.1   REPOSITORY AVAILABILITY

The repository is the key PKI component with respect to system availability, whether in a production environment or test environment. The CITE repository services must be internet accessible, operational, and available 12 hours a day, 5 days a week (Mon – Fri, 8:00am – 8:00pm Eastern Time, except Federal holidays), with the exception of scheduled downtime. Scheduled

downtime of repository services during these 12x5 business hours is limited to sixteen hours per month.

Each participating FPKI Affiliate is strongly encouraged to leave its CITE repository services operational and available 24 hours a day, 7 days a week. However, this is not required and there is no limitation on scheduled downtime during off hours. Table 5.1 depicts the repository availability requirements as they apply to the timeframes.

TABLE 5.1 – REPOSITORY AVAILABILITY

Days and Times	Description	Repository Availability Requirement
Mon – Fri 8:00am – 8:00pm Eastern Time (excluding Federal holidays)	12x5 Business Hours: Potential scheduled testing hours	Repository services are operational and available, except for scheduled downtime. Scheduled downtime is limited to 16 hours per month.
Mon – Fri 8:00pm – 8:00am Eastern Time (+ weekends and Federal holidays)	Off hours	No requirement. However, the FPKI TWG strongly encourages participating FPKI Affiliates to keep repository services operational and available at all times.

Availability requirements for other services provided by participating FPKI Affiliates, to include certificate issuance and management, are subject to the technical support availability requirements in the following section.

5.2   TECHNICAL SUPPORT AVAILABILITY

Participating FPKI Affiliates may be called upon to assist the FPKIMA, other FPKI Affiliates and their RPs, and FPKI Applicants with certificate issuance and management, testing, and troubleshooting. The participating FPKI Affiliate technical support and maintenance staff must be made available on an as scheduled basis. The participating FPKI Affiliates are only obligated to provide such support when certificate management requests or testing involves their PKI environment, and when testing is scheduled during the 12x5 potential scheduled testing hours according to the stipulations in section 5.3.

When unscheduled service disruptions occur, participating FPKI Affiliates shall attempt to resolve issues with their respective PKIs in a timely manner. It is important to note that technical support for production environments take precedence over technical support for the CITE. And as such, flexibility to the CITE response times is anticipated. The participating FPKI Affiliate shall make a good faith effort to initially respond within the severity level timeframes specified in Table 5.2. Severity levels are initially determined by the testing organization

affected by the issue. After initial assessment, the severity level may be adjusted after the impacted organizations discuss the issue in more detail.

TABLE 5.2 – INITIAL CITE PARTICIPANT RESPONSE TIMES

Severity Level	Description	Initial Response Time
1	Critical failure that prevents productive testing (e.g., unavailable directory services, non-operational network)	4 business hours
2	Urgent, high-impact problem where testing is proceeding, but in a significantly impaired fashion	1 business day
3	Important issue that does not have a significant impact on current testing	2 business day
4	Informational/non-critical: Either a request for information or issues not impeding testing for follow-up if needed	3 business days

5.3 SCHEDULE AND COORDINATION

Participating FPKI Affiliates are obligated to provide the FPKI TWG with email and phone information for at least two technical points of contact (POCs) – one primary and one backup – to provide technical support when necessary.   In lieu of providing individual names for technical POCs, participating FPKI Affiliates may establish group or other organizational-based email addresses for communications with the appropriate technical POCs. This information will only be made available (in a controlled manner) to FPKI Affiliates, FPKI Applicants (if applicable), and vendors supporting the FPKI as needed during testing or troubleshooting. POC information shall not be posted on a publicly-accessible website, unless protected using robust authentication technology.

The CITE testing and support requests (to include certificate issuance and management requests) shall be scheduled and coordinated in order to receive technical support from the relevant participating FPKI Affiliates. This coordination shall be done using an online reservation, schedule, and notification mechanism(s), which will be established in the future. Requests shall be scheduled during the 12x5 potential scheduled testing hours. At least five business days advance notice must be provided to all applicable technical POCs. However, the CITE is internet accessible and available for anyone (including vendors and other RPs) to conduct tests against it at any time. Tests that do not comply with the above requirements may be conducted if: 1) all parties involved agree to provide the necessary support; or 2) the testing party does not need support from any other participating FPKI Affiliate (in which case, the testing party is willing to accept that services may or may not be available).

Participating FPKI Affiliates shall also schedule and coordinate downtime associated with the services provided by their test environment. This coordination shall be done using a

reservation, schedule, and notification mechanism(s), which will be specified in the future. At least five business days advance notice should be provided for scheduled downtime, to allow for proper planning around potential testing conflicts. However, downtime may be scheduled with less than five days notice if there are no conflicting tests already scheduled or the respective testing party agrees to reschedule the conflicting scheduled tests.

Participating FPKI Affiliates are obligated to notify the FPKI TWG of significant changes to their test environment, and to verify interoperability when changes have been implemented.

5.4 TECHNICAL SPECIFICATIONS

This section details the CITE technical specifications, which apply to all participating parties.

1. The CITE services must be internet accessible.

2. Operational availability of the CITE repository services must be maintained as detailed in Section 5.1.

3. Technical support to include certificate issuance and management services must be available, as detailed in Section 5.2.

4. Test environments should emulate the corresponding production environment as closely as possible.

    a. Each CA hierarchy must mirror the production environment, but there is no requirement for the same number of physical CAs.

    b. The CITE CAs must not have the same Distinguished Names (DNs) as their production environment counterpart.

    c. The CITE CAs are not required to emulate Hardware Security Modules (HSMs).

    d. The CITE repositories should match those in the corresponding production environment as accurately as possible, including operating system versions and patch levels, protocols, and product version and patch levels.

    e. The CITE directory software must contain the same schema, context prefix, and similar chaining agreements as in the corresponding production environment.

    f. All CITE CA certificates, Certificate Revocation Lists (CRLs), and cross-certificates must be included in the associated CITE repository.

        ▪ If any production repository contains end-entity certificates, so must the corresponding CITE repository.

    g. Certificate revocation information will be made available using the same mechanism(s) as in the production environment (e.g., OCSP, CRLs).

5. Participating FPKI Affiliates must provide expired, revoked, and valid test end-entity certificates, representing each of the certificate policies from the corresponding production environment, for application testing.

   a. Participating FPKI Affiliates are encouraged to post the test certificates in a publicly available location, for other Affiliates and relying parties to easily access and utilize when necessary for testing.

   b. Participating FPKI Affiliates are encouraged to provide the private keys associated with test certificates. Private keys may be publicly posted, or provided as requested.

6. All CITE CA, cross-certificate, and end-entity certificates should match their production counterparts as much as possible.

   a. Test certificates and CRL profiles (including version, key length, extensions, and syntax) must match that of the production environment.

   b. The CITE CRLs may have a significantly-longer validation period than is required in production.

   c. The CITE CA certificates and cross-certificates must depict the same trust relationships as in the production environment.

   d. Participating FPKI Affiliates are strongly encouraged to use certificates that assert test certificate policy Object Identifiers (OIDs), when testing with CITE (see Appendix A for test certificate policy OIDs).

      ▪ If publicly posting private keys for testing purposes, the corresponding certificates are required to assert test certificate policy OIDs (see Appendix A for test certificate policy OIDs).

7. Resource references (such as CRL Distribution Points and Authority Information Access points) in the CITE certificates must correspond to appropriately functional repositories (during the 12x5 potential scheduled testing hours as detailed in Section 3.1).

APPENDIX A – TEST POLICY OBJECT IDENTIFIERS (OIDS)

The table below lists the current Production OIDs used by FPKI Affiliates, and their corresponding test OIDs that should be used in the test environment.

Test OID	Production OID
2.16.840.1.101.3.2.1.48.1	FBCA Rudimentary (2.16.840.1.101.3.2.1.3.1)
2.16.840.1.101.3.2.1.48.2	FBCA Basic (2.16.840.1.101.3.2.1.3.2)
2.16.840.1.101.3.2.1.48.3	FBCA Medium (2.16.840.1.101.3.2.1.3.3)
2.16.840.1.101.3.2.1.48.4	FBCA Medium Hardware (2.16.840.1.101.3.2.1.3.12)
2.16.840.1.101.3.2.1.48.5	FBCA Medium CBP (2.16.840.1.101.3.2.1.3.14)
2.16.840.1.101.3.2.1.48.6	FBCA Medium Hardware CBP (2.16.840.1.101.3.2.1.3.15)
2.16.840.1.101.3.2.1.48.7	FBCA High (2.16.840.1.101.3.2.1.3.4)
2.16.840.1.101.3.2.1.48.99	FBCA devices (2.16.840.1.101.3.2.1.3.37)
2.16.840.1.101.3.2.1.48.100	FBCA devices Hardware (2.16.840.1.101.3.2.1.3.38)
2.16.840.1.101.3.2.1.48.8	id-fpki-common-policy (2.16.840.1.101.3.2.1.3.6)
2.16.840.1.101.3.2.1.48.9	id-fpki-common-hardware (2.16.840.1.101.3.2.1.3.7)
2.16.840.1.101.3.2.1.48.10	id-fpki-common-devices (2.16.840.1.101.3.2.1.3.8)
2.16.840.1.101.3.2.1.48.98	id-fpki-common-devicesHardware (2.16.840.1.101.3.2.1.3.36)
2.16.840.1.101.3.2.1.48.11	id-fpki-common-authentication (2.16.840.1.101.3.2.1.3.13)
2.16.840.1.101.3.2.1.48.12	id-fpki-common-High (2.16.840.1.101.3.2.1.3.16)
2.16.840.1.101.3.2.1.48.13	id-fpki-common-cardAuth (2.16.840.1.101.3.2.1.3.17)
2.16.840.1.101.3.2.1.48.109	id-fpki-common-pivAuth-derived (2.16.840.1.101.3.2.1.3.40)

Test OID	Production OID
2.16.840.1.101.3.2.1.48.110	id-fpki-common-pivAuth-derived-hardware (2.16.840.1.101.3.2.1.3.41)
2.16.840.1.101.3.2.1.48.14	id-eGov-Level1 (2.16.840.1.101.3.2.1.3.9)
2.16.840.1.101.3.2.1.48.15	id-eGov-Level2 (2.16.840.1.101.3.2.1.3.10)
2.16.840.1.101.3.2.1.48.16	id-eGov-Applications (2.16.840.1.101.3.2.1.3.11)
2.16.840.1.101.3.2.1.48.78	id-fpki-certpcy-pivi-hardware (2.16.840.1.101.3.2.1.3.18)
2.16.840.1.101.3.2.1.48.79	id-fpki-certpcy-pivi-cardAuth (2.16.840.1.101.3.2.1.3.19)
2.16.840.1.101.3.2.1.48.80	id-fpki-certpcy-pivi-contentSigning (2.16.840.1.101.3.2.1.3.20)
2.16.840.1.101.3.2.1.48.101	id-sha1-medium-CBP (2.16.840.1.101.3.2.1.3.21)
2.16.840.1.101.3.2.1.48.102	id-sha1-mediumHW-CBP (2.16.840.1.101.3.2.1.3.22)
2.16.840.1.101.3.2.1.48.81	id-sha1-policy (2.16.840.1.101.3.2.1.3.23)
2.16.840.1.101.3.2.1.48.82	id-sha1-hardware (2.16.840.1.101.3.2.1.3.24)
2.16.840.1.101.3.2.1.48.83	id-sha1-devices (2.16.840.1.101.3.2.1.3.25)
2.16.840.1.101.3.2.1.48.84	id-sha1-authentication (2.16.840.1.101.3.2.1.3.26)
2.16.840.1.101.3.2.1.48.85	id-sha1-cardAuth (2.16.840.1.101.3.2.1.3.27)
2.16.840.1.101.3.2.1.48.86	id- fpki-common-piv-contentSigning (2.16.840.1.101.3.2.1.3.39)
2.16.840.1.101.3.2.1.48.17	Citizen & Commerce Provisional (2.16.840.1.101.3.2.1.14.1)
2.16.840.1.101.3.2.1.48.18	Citizen & Commerce Approved (2.16.840.1.101.3.2.1.14.2)
2.16.840.1.101.3.2.1.48.19	doe-basic (2.16.840.1.101.3.2.1.10.1)
2.16.840.1.101.3.2.1.48.20	doe-medium (2.16.840.1.101.3.2.1.10.2)
2.16.840.1.101.3.2.1.48.21	doe-high (2.16.840.1.101.3.2.1.10.3)

Test OID	Production OID
2.16.840.1.101.3.2.1.48.22	doe-medium-v2 (2.16.840.1.101.3.2.1.10.4)
2.16.840.1.101.3.2.1.48.23	id-doj-Class1 (2.16.840.1.101.3.2.1.16.1)
2.16.840.1.101.3.2.1.48.24	id-doj-Class2 (2.16.840.1.101.3.2.1.16.2)
2.16.840.1.101.3.2.1.48.25	id-doj-Class3 (2.16.840.1.101.3.2.1.16.3)
2.16.840.1.101.3.2.1.48.26	id-doj-Class4 (2.16.840.1.101.3.2.1.16.4)
2.16.840.1.101.3.2.1.48.27	id-doj-Class5 (2.16.840.1.101.3.2.1.16.5)
2.16.840.1.101.3.2.1.48.28	id-fbi-mediumAssurance (2.16.840.1.101.3.2.1.16.6.1)
2.16.840.1.101.3.2.1.48.29	id-fbi-highAssurance (2.16.840.1.101.3.2.1.16.6.2)
2.16.840.1.101.3.2.1.48.30	aces-ca (2.16.840.1.101.3.2.1.1.1)
2.16.840.1.101.3.2.1.48.31	aces-identity (2.16.840.1.101.3.2.1.1.2)
2.16.840.1.101.3.2.1.48.32	aces-business-rep (2.16.840.1.101.3.2.1.1.3)
2.16.840.1.101.3.2.1.48.33	aces-relying-party (2.16.840.1.101.3.2.1.1.4)
2.16.840.1.101.3.2.1.48.34	aces-SSL (2.16.840.1.101.3.2.1.1.5)
2.16.840.1.101.3.2.1.48.35	aces-fed-employee (2.16.840.1.101.3.2.1.1.6)
2.16.840.1.101.3.2.1.48.36	aces-fed-employee-hw (2.16.840.1.101.3.2.1.1.7)
2.16.840.1.101.3.2.1.48.37	id-gpo-medium (2.16.840.1.101.3.2.1.17.1)
2.16.840.1.101.3.2.1.48.38	State of Illinois Level I (software) (2.16.840.114273.1.1.1.1)
2.16.840.1.101.3.2.1.48.39	State of Illinois Level I (hardware) (2.16.840.114273.1.1.1.2)
2.16.840.1.101.3.2.1.48.40	State of Illinois Level II (software) (2.16.840.114273.1.1.1.3)
2.16.840.1.101.3.2.1.48.41	State of Illinois Level II (hardware) (2.16.840.114273.1.1.1.4)

Test OID	Production OID
2.16.840.1.101.3.2.1.48.42	State of Illinois Level III (software) (2.16.840.114273.1.1.1.5)
2.16.840.1.101.3.2.1.48.43	State of Illinois Level III (hardware) (2.16.840.114273.1.1.1.6)
2.16.840.1.101.3.2.1.48.44	State of Illinois Level IV (hardware only) (2.16.840.114273.1.1.1.7)
2.16.840.1.101.3.2.1.48.45	State of Illinois MEDI Single-Use Certificate (2.16.840.114273.1.1.2.1)
2.16.840.1.101.3.2.1.48.46	nfc-basicAssurance (2.16.840.1.101.3.2.1.8.1)
2.16.840.1.101.3.2.1.48.47	nfc-mediumAssurance (2.16.840.1.101.3.2.1.8.2)
2.16.840.1.101.3.2.1.48.48	nfc-highAssurance (2.16.840.1.101.3.2.1.8.3)
2.16.840.1.101.3.2.1.48.49	state-basic (2.16.840.1.101.3.2.1.6.1)
2.16.840.1.101.3.2.1.48.50	state-low (2.16.840.1.101.3.2.1.6.2)
2.16.840.1.101.3.2.1.48.51	state-moderate (2.16.840.1.101.3.2.1.6.3)
2.16.840.1.101.3.2.1.48.52	state-high (2.16.840.1.101.3.2.1.6.4)
2.16.840.1.101.3.2.1.48.53	state-mrtd (2.16.840.1.101.3.2.1.6.100)
2.16.840.1.101.3.2.1.48.54	treasury-cp1 (2.16.840.1.101.3.2.1.5.1)
2.16.840.1.101.3.2.1.48.55	treasury-level 1 (2.16.840.1.101.3.2.1.5.2)
2.16.840.1.101.3.2.1.48.56	treasury-level 2 (2.16.840.1.101.3.2.1.5.3)
2.16.840.1.101.3.2.1.48.57	treasury-level 3 (2.16.840.1.101.3.2.1.5.4)
2.16.840.1.101.3.2.1.48.58	treasury-level 4 (2.16.840.1.101.3.2.1.5.5)
2.16.840.1.101.3.2.1.48.111	treasury-pivi-hardware (2.16.840.1.101.3.2.1.5.10)
2.16.840.1.101.3.2.1.48.112	treasury-pivi-cardAuth (2.16.840.1.101.3.2.1.5.11)
2.16.840.1.101.3.2.1.48.113	treasury-pivi-contentSigning (2.16.840.1.101.3.2.1.5.12)

Test OID	Production OID
2.16.840.1.101.3.2.1.48.59	id-US-IRS-Securemail (2.16.840.1.101.3.2.1.5.6)
2.16.840.1.101.3.2.1.48.60	pto-registered-practitioner (2.16.840.1.101.3.2.1.2.1)
2.16.840.1.101.3.2.1.48.61	pto-inventor (2.16.840.1.101.3.2.1.2.2)
2.16.840.1.101.3.2.1.48.62	pto-practitioner-employee (2.16.840.1.101.3.2.1.2.3)
2.16.840.1.101.3.2.1.48.63	pto-basic (2.16.840.1.101.3.2.1.2.4)
2.16.840.1.101.3.2.1.48.64	pto-service-provider (2.16.840.1.101.3.2.1.2.5)
2.16.840.1.101.3.2.1.48.65	pto-service-provider-registrar (2.16.840.1.101.3.2.1.2.6)
2.16.840.1.101.3.2.1.48.66	pto-basic-2003 (2.16.840.1.101.3.2.1.2.7)
2.16.840.1.101.3.2.1.48.67	pto-medium-2003 (2.16.840.1.101.3.2.1.2.8)
2.16.840.1.101.3.2.1.48.68	id-US-dod-basic (2.16.840.1.101.2.1.11.2)
2.16.840.1.101.3.2.1.48.69	id-US-dod-medium-2048 (2.16.840.1.101.2.1.11.18)
2.16.840.1.101.3.2.1.48.70	id-US-dod-mediumhardware-2048 (2.16.840.1.101.2.1.11.19)
2.16.840.1.101.3.2.1.48.71	id-US-dod-FORTEZZA (2.16.840.1.101.2.1.11.4)
2.16.840.1.101.3.2.1.48.72	id-US-dod-type1 (2.16.840.1.101.2.1.11.6)
	id-US-dod-mediumNPE-2048(2.16.840.1.101.2.1.11.17)
	id-US-dod-mediumNPE-112 (2.16.840.1.101.2.1.11.36)
	id-US-dod-mediumNPE-128 (2.16.840.1.101.2.1.11.37)
	id-US-dod-mediumNPE-192 (2.16.840.1.101.2.1.11.38)
	id-US-dod-medium-112 (2.16.840.1.101.2.1.11.39)
	id-US-dod-medium-128 (2.16.840.1.101.2.1.11.40)
	id-US-dod-medium-192 (2.16.840.1.101.2.1.11.41)

Test OID	Production OID
	id-US-dod-mediumHardware-112 (2.16.840.1.101.2.1.11.42)
	id-US-dod- mediumHardware-128 (2.16.840.1.101.2.1.11.43)
	id-US-dod- mediumHardware-192 (2.16.840.1.101.2.1.11.44)
2.16.840.1.101.3.2.1.48.73	Wells Fargo CPS (2.16.840.1.114171.500.0.0)
2.16.840.1.101.3.2.1.48.74	NASA (1.3.6.1.4.1.71.1.1.103)
2.16.840.1.101.3.2.1.48.75	Treasury Medium-Software (2.16.840.1.101.3.2.1.5.7)
2.16.840.1.101.3.2.1.48.76	Treasury Basic Org (2.16.840.1.101.3.2.1.5.8)
2.16.840.1.101.3.2.1.48.77	State Medium Hardware (2.16.840.1.101.3.2.1.6.12)
2.16.840.1.101.3.2.1.48.90	id-eGov-BAE-Broker (2.16.840.1.101.3.2.1.3.32)
2.16.840.1.101.3.2.1.48.91	id-eGov-RelyingParty (2.16.840.1.101.3.2.1.3.33)
2.16.840.1.101.3.2.1.48.92	id-eGov-MetaSigner- (2.16.840.1.101.3.2.1.3.34)
2.16.840.1.101.3.2.1.48.93	id-eGov-MetaSigner-Hardware (2.16.840.1.101.3.2.1.3.35)
2.16.840.1.101.3.2.1.48.94	id-eGov-Level1-IdP (2.16.840.1.101.3.2.1.3.28)
2.16.840.1.101.3.2.1.48.95	id-eGov-Level2-IdP (2.16.840.1.101.3.2.1.3.29)
2.16.840.1.101.3.2.1.48.96	id-eGov-Level3-IdP (2.16.840.1.101.3.2.1.3.30)
2.16.840.1.101.3.2.1.48.97	id-eGov-Level4-IdP (2.16.840.1.101.3.2.1.3.31)
2.16.840.1.101.3.2.1.48.248	APL test lab – Golden PIV-I Authentication
2.16.840.1.101.3.2.1.48.249	APL test lab – Golden PIV-I CardAuth
2.16.840.1.101.3.2.1.48.250	APL test lab – Golden PIV-I Key Management
2.16.840.1.101.3.2.1.48.251	APL test lab – Golden PIV-I Digital Signature
2.16.840.1.101.3.2.1.48.252	APL test lab – Golden PIV-I Content Signing

Test OID	Production OID
id-dhs-certpcy-testRudimentary (2.16.840.1.101.3.2.1.15.31)	id-dhs-certpcy-rudimentary (2.16.840.1.101.3.2.1.15.1)
id-dhs-certpcy-testBasic (2.16.840.1.101.3.2.1.15.32)	id-dhs-certpcy-basic (2.16.840.1.101.3.2.1.15.2)
id-dhs-certpcy-testMedium (2.16.840.1.101.3.2.1.15.33)	id-dhs-certpcy-medium (2.16.840.1.101.3.2.1.15.3)
id-dhs-certpcy-testHigh (2.16.840.1.101.3.2.1.15.34)	id-dhs-certpcy-high (2.16.840.1.101.3.2.1.15.4)
id-dhs-certpcy-testMediumHardware (2.16.840.1.101.3.2.1.15.35)	id-dhs-certpcy-mediumHardware (2.16.840.1.101.3.2.1.15.5)
2.16.840.1.113733.1.7.21.1.1	Class -1-VTN SSP-rudimentary (2.16.840.1.113733.1.7.23.1.1.1)
2.16.840.1.113733.1.7.21.2.1	Class 2-VTN SSP-basic (2.16.840.1.113733.1.7.23.2.1.1)
2.16.840.1.113733.1.7.21.3.6	Class 3-VTN SSP-medium (2.16.840.1.113733.1.7.23.3.1.6)
2.16.840.1.113733.1.7.21.3.7	Class 3-VTN SSP-mediumHardware (2.16.840.1.113733.1.7.23.3.1.7)
2.16.840.1.113733.1.7.21.3.8	Class 3-VTN SSP-Devices (2.16.840.1.113733.1.7.23.3.1.8)
2.16.840.1.113733.1.7.21.3.13	Class 3-VTN SSP-PIV-I Hardware (2.16.840.1.113733.1.7.23.3.1.13)
2.16.840.1.113733.1.7.21.3.14	Class 3-VTN SSP-Medium CBP (2.16.840.1.113733.1.7.23.3.1.14)
2.16.840.1.113733.1.7.21.3.15	Class 3-VTN SSP-Medium Hardware CBP (2.16.840.1.113733.1.7.23.3.1.15)
2.16.840.1.113733.1.7.21.3.17	Class 3-VTN SSP-PIV-I CardAuth (2.16.840.1.113733.1.7.23.3.1.17)
2.16.840.1.113733.1.7.21.3.20	Class 3-VTN SSP-PIV-I ContentSigning (2.16.840.1.113733.1.7.23.3.1.20)
	ECA medium {2.16.840.1.101.3.2.1.12.1}
	ECA Medium Hardware {2.16.840.1.101.3.2.1.12.2}

15

Test OID	Production OID
	ECA Medium Token {2.16.840.1.101.3.2.1.12.3}
2.16.840.1.114027.200.3.10.10.1.8.	id-emspki-nfssp-rudimentary-policy {2.16.840.1 .114027.200.3. 10.7.8}
2.16.840.1.114027.200.3.10.10.1.7	id-emspki-nfssp-basic-policy {2.16.840.1 .114027.200.3. 10.7.7}
2.16.840.1.114027.200.3.10.10.1.3	id-emspki-nfssp-medium-policy {2.16.840.1 .114027.200.3. 10.7.1}
	id-emspki-nfssp-medium-devices {2.16.840.1 .114027.200.3. 10.7.3}
2.16.840.1.114027.200.3.10.10.1.4	id-emspki-nfssp-medium-hardware {2.16.840.1 .114027.200.3. 10.7.2}
2.16.840.1.114027.200.3.10.10.1.6	id-emspki-nfssp-medium-authentication {2.16.840.1 .114027.200.3. 10.7.4}
2.16.840.1.114027.200.3.10.10.1.6	id-emspki-nfssp-pivi-hardware {2.16.840.1 .114027.200.3. 10.7.6}
2.16.840.1.114027.200.3.10.10.1.5	id-emspki-nfssp-medium-cardAuth {2.16.840.1 .114027.200.3. 10.7.5}
2.16.840.1.114027.200.3.10.10.1.9	id-emspki-nfssp-pivi-contentSigning {2.16.840.1 .114027.200.3. 10.7.9}
	Safe basic (1.3.6.1.4.1.23165.1.1)
	Safe med software {1.3.6.1.4.1.23165.1.2)
	Safe med HW {1.3.6.1.4.1.23165.1.3}
1.3.6.1.4.1.24019.1.1.1.101	CertiPath medium Software 1.3.6.1.4.1.24019.1.1.1.1
1.3.6.1.4.1.24019.1.1.1.102	CertiPath medium Hardware 1.3.6.1.4.1.24019.1.1.1.2
1.3.6.1.4.1.24019.1.1.1.103	CertiPath highHardware 1.3.6.1.4.1.24019.1.1.1.3
1.3.6.1.4.1.24019.1.1.1.104	CertiPath medium CBP Software 1.3.6.1.4.1.24019.1.1.1.4
1.3.6.1.4.1.24019.1.1.1.105	CertiPath medium CBP Hardware 1.3.6.1.4.1.24019.1.1.1.5
1.3.6.1.4.1.24019.1.1.1.106	CertiPath highCBPHardware 1.3.6.1.4.1.24019.1.1.1.6

Test OID	Production OID
1.3.6.1.4.1.24019.1.1.1.107	CertiPath IceCAP-hardware 1.3.6.1.4.1.24019.1.1.1.7
1.3.6.1.4.1.24019.1.1.1.108	CertiPath IceCAP-cardAuth 1.3.6.1.4.1.24019.1.1.1.8
1.3.6.1.4.1.24019.1.1.1.109	CertiPath IceCAP-contentSigning 1.3.6.1.4.1.24019.1.1.1.9
1.3.6.1.4.1.24019.1.1.1.110	CertiPath variant medium Software 1.3.6.1.4.1.24019.1.1.1.17
1.3.6.1.4.1.24019.1.1.1.111	CertiPath variant medium Hardware 1.3.6.1.4.1.24019.1.1.1.18
1.3.6.1.4.1.24019.1.1.1.112	CertiPath variant high Hardware 1.3.6.1.4.1.24019.1.1.1.19
1.3.6.1.4.1.24019.1.1.1.113	CertiPath variant medium CBP Software 1.3.6.1.4.1.24019.1.1.1.20
1.3.6.1.4.1.24019.1.1.1.114	CertiPath variant medium CBP Hardware 1.3.6.1.4.1.24019.1.1.1.21
1.3.6.1.4.1.24019.1.1.1.115	CertiPath variant high CBP Hardware 1.3.6.1.4.1.24019.1.1.1.22
2.16.840.1.114412.99.4.1.1	DigiCert Level 1 Client Certificate - Personal 2.16.840.1.114412.4.1.1
2.16.840.1.114412.99.4.1.2	DigiCert Level 1 Client Certificate - Enterprise 2.16.840.1.114412.4.1.2
2.16.840.1.114412.99.4.2	DigiCert Level 2 Client Certificate - Basic 2.16.840.1.114412.4.2
2.16.840.1.114412.99.4.3.1	DigiCert Level 3 Client Certificate – US -Medium 2.16.840.1.114412.4.3.1
2.16.840.1.114412.99.4.3.2	DigiCert Level 3 Client Certificate – CBP -Medium 2.16.840.1.114412.4.3.2
2.16.840.1.114412.99.4.4.1	Digicert Level 4 Client Certificate – US - Hardware 2.16.840.1.114412.4.4.1
2.16.840.1.114412.99.4.4.2	Digicert Level 4 Client Certificate –CBP - Hardware 2.16.840.1.114412.4.4.2
2.16.840.1.114412.99.4.5.1	Level 4 PIV-I - Hardware 2.16.840.1.114412.4.5.1
2.16.840.1.114412.99.4.5.2	DigiCert Level 4 PIV-I – Card Authentication 2.16.840.1.114412.4.5.2

Test OID	Production OID
2.16.840.1.114412.99.4.5.3	DigiCert Level 4 PIV-I – Content Signing 2.16.840.1.114412.4.5.3
2.16.840.1.114412.99.1.11	DigiCert OV SSL 2.16.840.1.114412.1.11
id-test-usps-certpcy-rudimentaryAssurance 2.16.840.1.101.3.2.1.48.103	idusps-certpcy-rudimentaryAssurance TBD
id-test-usps-certpcy-basicAssurance 2.16.840.1.101.3.2.1.48.104	idusps-certpcy-basicAssurance TBD
id-test-usps-certpcy-mediumAssurance 2.16.840.1.101.3.2.1.48.105	idusps-certpcy-mediumAssurance TBD
id-test-usps-certpcy-mediumHardware 2.16.840.1.101.3.2.1.48.106	idusps-certpcy-mediumHardware TBD
id-test-usps-certpcy-mediumDevice 2.16.840.1.101.3.2.1.48.107	idusps-certpcy-mediumDevice TBD
id-test-usps-certpcy-mediumDeviceHardware 2.16.840.1.101.3.2.1.48.108	idusps-certpcy-mediumDeviceHardware TBD