Operational Capabilities Demonstration Criteria for PKI Shared Service Provider Candidates

Federal PKI Policy Authority
Shared Service Provider Working Group

June 28, 2007

1. Introduction

The Federal Public Key Infrastructure (PKI) Shared Service Provider (SSP) Program facilitates outsourcing of PKI services by Federal agencies. The Federal government has established a Certified PKI Shared Service Providers (PKI SSP) List for vendors that have demonstrated the ability to provide managed PKI services that meet government requirements.[1] This document specifies the functionality that an SSP candidate must demonstrate during an Operational Capabilities Demonstration (OCD), which is one of the steps that a candidate must complete in order to be accepted for inclusion on the Certified PKI SSP List [ROADMAP].

2. Demonstration Criteria

This section outlines demonstration requirements associated with the mandatory capabilities that must be provided by all SSPs and with the optional capabilities that may be provided by an SSP. The SSPWG reserves the right to augment the OCD criteria based on the proposed architecture and approach identified by the SSP candidate. This includes validation of specific areas identified in the SSP candidate's CPS submission, as presented in the CP-CPS Analysis Matrix (section 4.2 in [ROADMAP]).

2.1. Demonstration of Mandatory Requirements

This section specifies demonstration criteria associated with mandatory requirements of the SSP program that must be satisfied by all SSP candidates.

1. Demonstrate support for in-person verification of applicant's identity as specified in [COMMON]: Demonstrate the method by which the Registration Authority (RA) and CA communicate applicant identity information, authorization information, etc.
2. Demonstrate support for PIV [SP 800-73] compliant smart card users:
   a. Issue certificates for signature keys generated for a user on PIV compliant smart cards.
   b. Comply with the Certificate and CRL Profile [PROF], including authorityInfoAccess and cRLDistributionPoints extensions.
   c. Provide newly generated user certificate to user and import certificate onto smart card.
3. Demonstrate support for each public key type and signature algorithm that is specified as being supported by the CA. At least one certificate must be generated for each of the supported key types and algorithms. Possible

[1] These requirements have been defined by the Shared Services Provider Working Group, which is a subcommittee of the Federal PKI Policy Authority (FPKIPA). Statutory authority is derived from the E-Government Act, passing from OMB through the Federal CIO Council (http://www.cio.gov) to the FPKIPA, and in turn to the Shared Service Provider Working Group.

combinations include:

- Certificate signed with RSA (PKCS #1 v1.5 padding) and SHA-1
- Certificate signed with RSA (PKCS #1 v1.5 padding) and SHA-256*
- Certificate signed with RSASSA-PSS and SHA-256*
- Certificate signed with ECDSA and SHA-256
- Certificate signed with ECDSA and SHA-384
- Certificate with RSA subject public key
- Certificate with elliptic curve public key (P-256 curve)
- Certificate with elliptic curve public key (P-384 curve)

* Demonstration of RSA signatures with SHA-256 is not required before January 1, 2010.

4. Distribute trust anchor certificate to an RA or a user.
5. Authenticate and process Certificate Revocation Requests.
6. Generate CRLs that comply with Certificate and CRL Profile [PROF].
7. Demonstration support for repository requirements [REP]:
    a. Post CA certificates in LDAP directory as specified in [REP] and matching authorityInfoAccess/subjectInfoAccess extensions.
    b. Post CRLs in LDAP directory as specified in [REP] and matching cRLDistributionPoints extension.
    c. Post CA certificates on HTTP web server as specified in [REP] and matching authorityInfoAccess/subjectInfoAccess extensions.
    d. Post CRLs on HTTP web server as specified in [REP] and matching cRLDistributionPoints extension.
8. Demonstrate paper and electronic archiving in accordance with Archive Requirements document [ARCH].
9. Demonstrate CA key rollover.
10. After key rollover, perform the following actions:
    a. Issue new certificates.
    b. Revoke one “new” certificates and one “old” certificate.
    c. Generate valid X.509 CRL(s) for all currently unexpired certificates.

2.2. Demonstration of Optional Capabilities

This section specifies demonstration criteria associated with optional capabilities of the

SSP program. SSP candidates whose CPSs indicate they intend to offer any of the capabilities listed in this section must satisfy the corresponding demonstration criteria specified in this section for those capabilities.

1. Demonstrate support for trusted agent verification of applicant's identity as specified in CP.
2. Issue certificates to software users.
3. Issue certificates for devices.
4. Issue PIV Authentication certificates.[2]
5. Issue Card Authentication certificates.
6. Issue Key Management (i.e., key transport or key agreement) certificates.
7. Demonstrate support for OCSP.[3]
8. Escrow and recover encryption keys.
9. Demonstrate support for posting user certificates in LDAP directory as specified in [REP].

3. Notification of Results

The SSPWG will notify the SSP candidate of any deficiencies that require further attention. The SSP candidate should expect to resolve any deficiencies through re-evaluation against the OCD criteria. This is initiated by contacting the SSPWG for scheduling.

Upon successful completion of the OCD evaluation process, a formal determination of acceptability will be generated by the SSPWG. Based on these results and where deemed appropriate by the SSPWG, operating limitations may be enforced on the SSP. The Chair of the SSPWG will provide a copy of the determination of acceptability to the SSP candidate and the FPKIPA.

4. References

[ARCH] *Archive Requirements for Certified PKI Shared Service Providers*, January 29, 2007. http://www.cio.gov/fpkipa/documents/ArchiveRqmtsForSSP.pdf

[COMMON] *X.509 Certificate Policy for the Common Policy Framework*, Version 3647 – 1.0, May 8, 2007. http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf

[2] Note: PIV authentication certificates are mandatory to satisfy HSPD-12/FIPS 201 implementation.

[3] Note: OCSP is required for PIV Authentication and Card Authentication certificates.

[PROF] *X.509 Certificate and CRL Extensions Profile for the SSP Program*, February 6, 2006. http://www.cio.gov/fpkipa/documents/CertCRLprofileForCP.pdf

[REP] *Shared Service Provider Repository Service Requirements*, June 28, 2007. http://www.cio.gov/fpkipa/documents/SSPrepositoryRqmts.pdf

[ROADMAP] *Shared Service Provider Roadmap: Navigating the Process to Acceptance*, March 8, 2007. http://www.cio.gov/fpkipa/documents/SSProadmap.pdf

[SP 800-73] *Interfaces for Personal Identity Verification*, NIST Special Publication 800-73-1, March 2006. http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf