Certificate Validation Capability Requirements and Best Practices

8 August 2012

Version 1.1

DOD PKE Team

Revision History

Issue Date	Revision	Change Description
07/29/2010	1.0	Document Developed
8/8/2012	1.1	Updated DoD PKE support email address

Contents

Introduction

The DoD Public Key Enablement (PKE) Reference Guides are developed to help an organization augment their security posture through the use of the Public Key Infrastructure (PKI).

Purpose

The purpose of this document is to provide vendors and other custom application developers with guidelines for designing certificate validation capabilities that meet DoD and federal interoperability requirements and technical constraints for certificate-based authentication.

Scope

This document addresses certificate validation practices, with an emphasis on revocation checking functionality and interoperability support.

Minimum Requirements

Algorithms and Key Sizes

The system must support Rivest, Shamir and Adleman (RSA) keys up to 4096 bits with Secure Hash Algorithm (SHA)-1 and SHA-2 digital signatures as dictated by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-57, SP 800-78 and draft SP 800-131 (see Appendix B).

Basic Validation Steps

The system must implement the basic validation steps outlined in section 6.1.3 of the internet X.509 certificate specification [Request for Comment (RFC) 5280][1].

Revocation Checking

The system must provide the capability to check certificate revocation status as part of the certificate validation process (as defined in RFC 5280). If the revocation status of a certificate cannot be determined, the system must be configurable to fail closed, meaning that access is denied to the possessor of the end entity (EE) certificate for which revocation status cannot be determined.

Best Practices

Algorithms and Key Sizes

The DoD and its coalition partners currently use RSA keys up to 4096 bits with SHA-1 digital signatures. Within the next few years, the DoD and federal communities will move to Elliptic Curve Cryptography (ECC) keys as well. SHA-256 digital signatures are mandated for use starting January 1, 2011. The system should support all of these algorithms and key sizes for validating digital signatures on signed objects including certificates (in compliance with NIST SP 800-78), and for native application digital signature generation (in compliance with NIST SP 800-57 and draft SP 800-131). More detailed information on required algorithms and timelines can be found in NIST SP 800-57, SP 800-78 and draft SP 800-131.

Basic Validation Steps

Section 6.1.3 of the internet X.509 certificate specification [RFC 5280][2] defines the basic certificate processing steps that any implementation should follow. A more condensed, practical version of this specification's requirements can be found in the draft NIST

[1] http://www.ietf.org/rfc/rfc5280.txt
[2] http://www.ietf.org/rfc/rfc5280.txt

Recommendation for X.509 Path Validation[3]; requirements in the Bridge-Enabled section of this document (Section 4) should be included to meet federal interoperability requirements. Note that the draft recommendation references RFC 3280[4], which has been superseded by RFC 5280.

Revocation Checking

Methods and Failover Configuration

The best practice for certificate revocation checking mechanisms is to provide multiple methods with failover capabilities. In general, DoD's preferred order of revocation checking methods (where the first method is primary, with failover to the subsequent methods in listed order) is:

1) Online Certificate Status Protocol (OCSP)
2) Local Certificate Revocation List (CRL) cache
3) CRL distribution points (CRL DP)

The logic behind this configuration that the OCSP is preferred for use when available. When OCSP is unavailable, local CRL caches are preferred over CRL DPs due to the size of DoD CRLs and performance/possible denial of service implications for users who must wait for CRLs to download in real time from their distribution points in order for the user's certificate to be checked for revocation. In scenarios where the CRL may not exist in the local cache, dynamic CRL retrieval via CRL DP should be supported to ensure that the user is not denied service because a valid CRL is not available locally.

This reasoning is generally applicable for most DoD environments; however, for the most flexibility to meet individual deployments' needs, the ideal implementation would provide a configuration option that allows the administrator to specify the preferred order of revocation check methods. In addition, a configurable threshold of validation request volume above which the system will switch to a different preferred method order for a particular issuing Certification Authority (CA) can provide traffic volume-driven performance tuning.

The system should be configurable to deny a user access (fail secure/closed) in instances where a certificate's revocation status cannot be determined by any of the available means.

---

[3] http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/NIST_Recommendation_for_X509_PVMs.pdf

[4] http://www.ietf.org/rfc/rfc3280.txt

OCSP Implementation

Responder Location/URL

For OCSP support, the system should support use of the Authority Information Access (AIA) value in the certificate to determine the OCSP responder URL. The system should also provide a configurable default responder URL value for each CA certificate in the trust store, with the options to fail over to the default value when the OCSP responder URL is not included in the AIA field of the certificate to be validated, or to use the default value as an authoritative value that overrides whatever may be listed in the AIA field.

Trust Model Support

The system should support the Delegated Trust Model (DTM) for OCSP response signatures by default, with the capability to configure use of the Explicit Trust Model or CA-signed Trust Model instead.

Nonce Support

The system should be configurable to include nonces in OCSP requests, forcing the responder to retrieve the certificate status and generate the response at the time of the request rather than allowing it to use a pre-signed response.

Local Cache

The system should be configurable to locally cache OCSP responses. The refresh schedule for the cached data should be configurable to provide the capability to require a data refresh more frequently than required by the validity periods of the responses, but should never exceed the Next Update date of the response.

CRLs Implementation

Local Cache

The system should be configurable to use a local cache of CRLs to check revocation status of certificates. The system should ensure that retrieval of new CRLs for the local cache does not cause denial of service, and that users can authenticate against locally cached valid CRLs while new CRLs are being retrieved and populated in the local cache. This cache should also be capable of handling the volume of CRL data that a typical federal interoperability implementation might require. For example, currently the DoD CRLs comprise about 200 MB of data. Assuming that the entire federal community is roughly twice the size of the DoD (see Appendix D) and accounting for growth and error, 500 MB of CRL data might be reasonable to expect for a federal interoperability implementation. To improve performance when dealing with large CRLs, support of technologies such as partitioned and delta CRLs should be considered.

Similarly to the OCSP response cache, the refresh schedule for the CRL cache should be configurable, but should never exceed the Next Update date of the response.

CRL DPs

The system should be capable of retrieving CRLs from CRL DPs at run time and adding them to the local cache if the appropriate CRL for the certificate being validated does not already exist in the local CRL cache. Similarly to the OCSP responder URL value, the system should support use of the CRL DP value in the certificate to determine the CRL DP URL, as well as provide a configurable default value per CA certificate in the trust store that can be used as either an override or failover value for the CRL DP value in the certificate.

Interoperability Considerations

Policy Control

The system should be configurable to require EE certificates to assert an allowed policy object identifier (OID) in their Certificate Policies extension in order to authenticate. For human readability, it is preferable to provide the capability to configure allowed OIDs per trust anchor. However, since each PKI has a unique OID arc, a white list approach can also be used. If the white list approach is taken, it is recommended that the capability to include comments in, or otherwise annotate, the configured OID list be provided to aid the administrator in tracking which allowed OIDs correspond to which organizations.

Cross-Certificate or Implicit Path Processing

To facilitate the use of cross-certificates in certificate paths, the system should support use of both AIA and Subject Information Access (SIA) extensions for path processing. Any path building algorithms should also prefer the shortest valid path.

The system should also ensure that the "hint list" sent to the browser does not result in the browser prohibiting the user from selecting a certificate that could have a valid path to a configured trust anchor through a cross certificate. For systems that have the capability to dynamically build paths (i.e. do not require that all certificates in a path other than the EE certificate be explicitly stored in the trust store), the hint list should be empty/null to support certificates that chain to trusted roots through cross-certificates. For systems that require all trusted CAs in a path to be explicitly included in the trust store, the hint list can include all trusted roots.

Delegated Validation

Including support for technologies such as Server-based Certificate Validation Protocol[5] (SCVP) that allow the entire certificate validation process to be delegated to an external entity should be considered.

[5] http://tools.ietf.org/html/rfc5055

Appendix A: Acronyms and Definitions

Acronyms

AIA	Authority Information Access
CA	Certificate Authority
CRL	Certificate Revocation List
CRL DP	CRL Distribution Point
DoD	Department of Defense
DTM	Delegated Trust Model
ECC	Elliptical Curve Cryptography
EE	End Entity
NIST	National Institute of Standards & Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RFC	Request for Comment
RSA	Rivest, Shamir and Adleman
SCVP	Server-based Certificate Validation Protocol
SHA	Secure Hash Algorithm
SIA	Subject Information Access
SP	Special Publication
URL	Universal Resource Locator

Definitions

arc	A specific OID sub-tree assigned to an organization
CA-signed Trust Model	OCSP trust model in which the OCSP client expects the OCSP response to be signed by the same CA that issued the certificate for which status is being requested
Delegated Trust Model	OCSP trust model in which the OCSP client expects the OCSP response to be signed by a certificate issued for OCSP signing by the same CA that issued the certificate for which status is being requested
Explicit Trust Model	OCSP trust model in which the OCSP client expects the OCSP response to be signed by a certificate explicitly identified in the client's configuration

nonce	A set of random bits that can be included in an OCSP request to force a fresh (rather than pre-signed) response

Appendix B: Standards & Policies

The following are standards and policies pertinent to certificate validation and cryptography requirements.

RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

http://datatracker.ietf.org/doc/rfc5280/

This standard specifies the standard validation activities for X.509 certificate path validation, along with a sample algorithm for executing the necessary activities. It also describes the structure of X.509 v3 certificates and X.509 v2 CRLs.

HSPD 12: Policy for a Common Identification Standard for Federal Employees and Contractors

http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

The Homeland Security Presidential Directive that orders the implementation of a mandatory, Government-wide standard for physical and logical identification.

FIPS PUB 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors

http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

The standard that implements HSPD 12. Section 6.2.4 defines the required PIV PKI certificate validation process.

NIST SP 800-78-2: Cryptographic Algorithms and Key Sizes for Personal Identity Verification

http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf

Contains approved PIV algorithms for various cryptographic uses and timelines for use.

NIST Draft SP 800-131: Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

http://csrc.nist.gov/publications/drafts/800-131/draft-sp800-131_spd-june2010.pdf

Section 9 discusses approved hash functions, and requires that digital signature generation be done with SHA-2 functions (which for most practical purposes for the federal government translates to use of SHA-256) starting January 1, 2011. For certificate validation purposes, this means certificates and revocation data signed with SHA-256 need to be able to be used in the certificate validation process.

NIST SP 800-57: Recommendation for Key Management

http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf
Discusses best practices for key management and provides guidance for cryptographic algorithm and key size selection.

FIPS 140-2: Security Requirements for Cryptographic Modules

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
Defines requirements for cryptographic modules of systems with sensitive but unclassified (SBU) contents. The current list of FIPS-validated modules is available at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

Appendix C: Test Resources

The following are PKI test resources that may be useful in verification of a certificate validation capability.

NIST PKI Test Suite (PKITS)

http://csrc.nist.gov/groups/ST/crypto_apps_infra/pki/pkitesting.html
Suite includes test cases as well as test data to aid in execution of the test cases.

DoD Joint Interoperability Test Command (JITC) Test Suite

Test cases:
http://jitc.fhu.disa.mil/pki/documents/conformance_testing_of_relying_party_client_certificate_path_v1_07_september_28_2001.
Test data:
http://jitc.fhu.disa.mil/pki/documents/conformance_testing_of_relying_party_client_certificate_path_v1_07_certificates.zip

Appendix D: Federal Community Size Estimate

Department	Staff Type	Number	As of Date	Source
Defense	Civilian	700,000	2010	[1]
	Active Duty Military	1,300,000	2010	[1]
	Reservist/ National	1,100,000	2010	[1]
	**Contractor	466,667	2009	[2]
	Total	3,566,667		
Veterans Affairs	Civilian	235,000	2010	[1]
Homeland Security	Civilian	216,000	2010	[1]
	Contractor	200,000	2010	[3]
Justice	Civilian	108,000	2008	[4]
Treasury	Civilian	100,000	2010	[1]
Agriculture	Civilian	100,000	2010	[1]
Interior	Civilian	70,000	2010	[1]
	Volunteer	200,000	2010	[1]
Health and Human Services	Civilian	65,000	2010	[1]
Transportation	Civilian	55,000	2010	[1]
Commerce	Civilian	38,000	2010	[1]
Labor	Civilian	15,000	2010	[1]
Energy	Civilian/Contractor	100,000	2010	[1]
State	Civilian	30,000	2010	[1]
Housing and Urban Development	Civilian	9,000	2010	[1]
Education	Civilian	4,200	2010	[1]
Social Security Administration	Civilian	64,000	2008	[4]
National Aeronautics and Space	Civilian	18,000	2008	[4]
Environmental Protection Agency	Civilian	18,000	2008	[4]
General Services Administration	Civilian	12,000	2008	[4]
Office of Personnel Management	Civilian	5,000	2008	[4]
Smithsonian Institution	Civilian	4,000	2008	[4]
Other Independent Agencies	Civilian	59,000	2008	[4]
Judicial branch	Civilian	33,000	2008	[4]
Legislative branch	Civilian	30,000	2008	[4]
*Other Dept Contractors	Contractor	1,072,200		
**Intelligence community		200,000		[5]
Total		6,627,067		

* Estimated at 50% of workforce for all departments with unlisted contractor counts
**Rough estimates are provided for these groups based on publicly available information

Sources

[1] http://www.whitehouse.gov/our-government/executive-branch
[2] http://www.govexec.com/dailyfed/0409/040609kp1.htm
[3] http://fcw.com/articles/2010/03/01/dhs-has-too-many-contract-employees-senators-charge.aspx
[4] http://www.bls.gov/oco/cg/cgs041.htm
[5] http://www.bradley.edu/academics/las/is/is306uscommunity.htm

Appendix E: Support

Website

Visit the URL below for the PKE website.
www.iase.disa.mil/pki/pke

Technical Support

Contact technical support through the email address below.
dodpke@mail.mil