Infrastructure Support for Retention of PKI Artifacts

draft-ietf-ltans-pki-retention-01.txt

Abstract

In most PKIs, directory servers are used to provide current certificates and revocation information to relying parties. In situations where certificates must be validated relative to a time in the past, relying parties often have no means of obtaining the necessary PKI artifacts. This specification defines several directory attributes to support validation using historical PKI artifacts.
Table of Contents

1. Introduction ......................................................... 3
   1.1. Requirements notation ........................................ 3
2. Concept of Operations .................................................. 4
3. Object classes .......................................................... 5
4. Public key certificates .................................................. 6
5. Security Considerations .................................................. 7
6. References ............................................................... 8
   6.1. Normative References .............................................. 8
   6.2. Informative References .......................................... 8
Appendix A. ASN.1 Module ................................................ 9
Appendix B. Revocation information ..................................... 10
   B.1. Historical CRLs ................................................ 10
   B.2. Entry Revocation Publication extension .......................... 11
   B.3. Historical CRL issuance extension .............................. 11
Author’s Address ......................................................... 13
Intellectual Property and Copyright Statements ......................... 14
1. Introduction

Digital signatures are frequently verified using public key infrastructure (PKI) artifacts such as public key certificates and certificate revocation lists (CRLs). Verifiers construct and validate certification paths from a public key certificate containing the public key used to verify the signature to a trusted public key. Construction of a certification path may require acquisition of different types of information generated by multiple PKIs. When verifying digital signatures many years after signature generation, additional considerations must be addressed. For example, some necessary PKI artifacts may no longer be available, some may have expired and the cryptographic algorithms or keys used in generating digital signatures may no longer provide the desired degree of security.

The "Standard Certificate Validation Protocol" (SCVP) [I-D.ietf-pkix-scvp] defines a means of delegating certification path construction and/or validation to a server, including the ability to request the server to perform the operations relative to a time in the past. The "Evidence Record Syntax" (ERS) [I-D.ietf-ltans-ers] defines structures for preserving materials over long periods of time through a regimen that includes periodic re-signing of relevant materials using newer keys and stronger cryptographic algorithms. "Using SCVP to Convey Evidence Records" [I-D.ietf-ltans-ers-scvp] defines a means of using SCVP to retrieve evidence records covering historical PKI artifacts.

Directory servers are frequently used to make PKI artifacts available for use by public key-enabled applications. However, in many PKIs, artifacts are removed from the directory when the artifact is updated by a newer version or the artifact expires. This document describes a means of using LDAP or X.500 directory servers to retrieve historical PKI artifacts and, optionally, associated evidence records.

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].
2. Concept of Operations

Public key-enabled applications build and validate certification paths in support of functions including digital signature verification and public key encryption. In many cases, the materials used to validate a certification path are available via an X.500 or LDAP directory in accord with the schema defined in [RFC2587]. For many reasons, including size constraints on the server and performance impact on relying parties, directories usually contain PKI artifacts that are current, i.e., non-expired and most recent. Applications requiring access to historical PKI artifacts, i.e., not the most recent and possibly expired, are forced to rely upon other mechanisms. This document defines an object class and a set of directory attributes that complement those defined in [RFC2587] for the purpose of making historical PKI artifacts available.
3. Object classes

Two object classes are defined for historical certificates and CRLs: historicalPKIEntity and historicalCRLDistributionPoint. These auxiliary object classes MAY be used to represent entities associated with historical PKI artifacts.

historicalPKIEntity OBJECT-CLASS ::= { SUBCLASS OF {top} KIND auxiliary MAY CONTAIN {historicalCertificate} ID TBD }

historicalCRLDistributionPoint OBJECT-CLASS ::= { SUBCLASS OF {top} KIND auxiliary MAY CONTAIN {historicalCRL} ID TBD }

This specification differs from [RFC2587] by not defining separate object classes or attributes to delineate between end entities and certification authorities.
4. Public key certificates

Public key certificates are digitally signed. As such, certificates are subject to the same concerns as described for digitally signed forms, contracts, etc. in [I-D.ietf-ltans-ers]. To address these concerns, the integrity of public key certificates can be protected by generating and maintaining an evidence record covering the certificate. A certificate and an evidence record can be bound together using the structure defined below. Certificates are defined in [RFC3280] and evidence records are defined in [I-D.ietf-ltans-ers].

HistoricalCertificate ::= SEQUENCE
{ certificate Certificate, evidenceRecord EvidenceRecord OPTIONAL }

HistoricalCertificates can be made available via an X.500 or LDAP directory using the following attribute. When a certificate is to be removed from a directory due to replacement or due to expiration, it MAY be removed from the userCertificate or cACertificate attribute and it SHOULD be added to the historicalCertificate attribute. An evidence record for the certificate MAY be requested at that time or at a later time.

historicalCertificate ATTRIBUTE ::= 
{ WITH SYNTAX HistoricalCertificate
EQUALITY MATCHING RULE historicalCertificateExactMatch,
ID TBD }
5. Security Considerations

Since the information stored in the attributes defined in this specification are signed, no additional integrity service is required.

Security considerations with respect to retrieval, addition, deletion and modification of the information supported by this schema definition are addressed in [RFC2559].

The timing of the application or update of evidence records is a matter of local policy. Security considerations associated with evidence records are described in [I-D.ietf-ltans-ers].
6. References

6.1. Normative References

[I-D.ietf-ltans-ers]
Brandner, R., "Evidence Record Syntax (ERS)",

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet
X.509 Public Key Infrastructure Certificate and
Certificate Revocation List (CRL) Profile", RFC 3280,
April 2002.

6.2. Informative References

[I-D.ietf-ltans-ers-scvp]
Wallace, C., "Using SCVP to Convey Long-term Evidence
Records", draft-ietf-ltans-ers-scvp-01 (work in progress),
May 2006.

[I-D.ietf-pkix-scvp]
(SCVP)", draft-ietf-pkix-scvp-27 (work in progress),
June 2006.

[RFC2559] Boeyen, S., Howes, T., and P. Richard, "Internet X.509
Public Key Infrastructure Operational Protocols - LDAPv2",
RFC 2559, April 1999.

[RFC2587] Boeyen, S., Howes, T., and P. Richard, "Internet X.509
Public Key Infrastructure LDAPv2 Schema", RFC 2587,
June 1999.
Appendix A. ASN.1 Module

LTANS_PKI_RETENTION
-- { iso(1) identified-organization(3) dod(6) internet(1)
    --    security(5) mechanisms(5) pkix(7) id-mod(0) TBD }

DEFINITIONS IMPLICIT TAGS ::= BEGIN
IMPORTS

Certificate, CertificateList, Time FROM PKIX1Explicit88
    { iso(1) identified-organization(3) dod(6)
        internet(1) security(5) mechanisms(5) pkix(7)
        mod(0) pkix1-explicit(18) }

EvidenceRecord FROM ERS
    {iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-ers(TBD) }

HistoricalCertificate ::= SEQUENCE {
    certificate Certificate,
    evidenceRecord EvidenceRecord OPTIONAL
}

HistoricalCRL ::= SEQUENCE {
    crl CertificateList,
    evidenceRecord EvidenceRecord OPTIONAL
}

EntryRevocationPublication ::= Time
HistoricalCRLIssuance ::= Time

END
Appendix B. Revocation information

Preservation of revocation information is more complicated than preservation of certificates due, primarily, to the volume of revocation information generated in most PKIs, i.e., CRLs are generated more frequently than certificates and are often much larger. CRLs are signed and the signatures require preservation. However, the number of CRLs makes preservation difficult and complicates validation operations for relying parties. A cumulative CRL provides a better target for preservation. However, cumulative CRLs introduce additional processing rules. To account for the HoldInstruction extension, all entries on a CRL must be reviewed, the entries applicable to a certificate sorted and the time of interest compared to the sorted list to determine if the certificate was on hold at that time.

X.509 specifies a the expiredCertsOnCRL CRL extension, that is not present in [RFC3280], to indicate that the CRL contains expired certificates. The extension is expressed as a GeneralizedTime value that provides the time at or since which certificates may have expired but will still appear on the CRL, i.e., certificates that expired before that time do not appear on the CRL. Relying parties using a CRL of this sort must recognize that the time of interest for a path validation operation may fall outside the thisUpdate/nextUpdate period of a cumulative CRL. The following section describes a variation on the X.509 CumulativeCRL extension that preserves the property where thisUpdate is less than or equal to the time of interest and nextUpdate is greater than or equal to the time of interest.

B.1. Historical CRLs

To avoid preserving every CRL instance generated within a PKI, an historical CRL can be generated and maintained. An historical CRL is a CRL with the following properties:

- The thisUpdate field is fixed and contains the time corresponding to the instantiation of the CA(s) covered by the CRL.

- Entries optionally include an extension indicating the thisUpdate value from the first CRL on which the entry appeared.

- The CRL structure is optionally associated with an EvidenceRecord.

Historical CRLs are defined as follows.
HistoricalCRL ::= SEQUENCE
{
  crl CertificateList,
  evidenceRecord EvidenceRecord OPTIONAL
}

CRL issuers need not generate an historical CRL upon each CRL issuance. Historical CRLs can be generated on a less frequent basis since certification path validation operations relative to the current time can be serviced using conventional CRLs. When an historical CRL is generated, the thisUpdate time MUST NOT change from the value in the previous historical CRL. The new CRL MUST replace the previous historical CRL in the historicalCRL directory attribute. The thisUpdate value in the first historical CRL issued by a CRL issuer SHOULD be set to the earliest notBefore value from the set of certificates issued by the CAs covered by the CRL. After a CA no longer needs to issue CRLs, the final HistoricalCRL can be preserved by periodically updating the evidence record as described in [I-D.ietf-ltans-ers].

For sake of simplicity, historical CRLs should not be indirect CRLs and should not be delta CRLs. Where partitioned, historical CRLs MUST adhere to the partitioning scheme used by the corresponding conventional CRLs.

B.2. Entry Revocation Publication extension

This CRL entry extension identifies the thisUpdate time from the CRL on which the entry first appeared. If this extension is not present on the first entry in a CRL, the revocation publication value defaults to the thisUpdate value of the CRL. On subsequent entries, if this extension is not present, the revocation publication value for the entry is the same as that for the preceding entry. This extension is defined as follows:

EntryRevocationPublication ::= Time

B.3. Historical CRL issuance extension

This optional CRL extension indicates the CRL is an historical CRL, i.e., the thisUpdate time is not based on the time of issuance. The extension is used to convey the issuance time and is defined as follows:
HistoricalCRLIssuance ::= Time

If used by conforming CRL issuers, this extension MUST always be non-critical.

Historical CRLs can be made available via an X.500 or LDAP directory using the following attribute.

historicalCRL ATTRIBUTE ::= 
{
  WITH SYNTAX HistoricalCRL
  EQUALITY MATCHING RULE historicalCRLExactMatch,
  ID TBD
}

Historical CRLs are not intended to replace CRLs used by applications performing certification path validation relative to the current time. CRL issuers should continue to publish conventional CRLs.
Author’s Address

Carl Wallace
Cygnacom Solutions
Suite 5200
7925 Jones Branch Drive
McLean, VA  22102

Email: cwallace@cygnacom.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2006). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.