Network Working Group
Request for Comments: 5276
Category: Standards Track

C. Wallace
Cygnacom Solutions

August 2008

Using the Server-Based Certificate Validation Protocol (SCVP) to Convey Long-Term Evidence Records

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

The Server-based Certificate Validation Protocol (SCVP) defines an extensible means of delegating the development and validation of certification paths to a server. It can be used to support the development and validation of certification paths well after the expiration of the certificates in the path by specifying a time of interest in the past. The Evidence Record Syntax (ERS) defines structures, called evidence records, to support the non-repudiation of the existence of data. Evidence records can be used to preserve materials that comprise a certification path such that trust in the certificates can be established after the expiration of the certificates in the path and after the cryptographic algorithms used to sign the certificates in the path are no longer secure. This document describes usage of the SCVP WantBack feature to convey evidence records, enabling SCVP responders to provide preservation evidence for certificates and certificate revocation lists (CRLs).

Table of Contents

1. Introduction 3
1.1. Requirements Notation 3
2. Concept of Operations 4
3. Requests 5
4. Responses 6
5. WantBacks 6
5.1. Evidence Record for a Complete Certification Path 7
5.2. Evidence Record for a Partial Certification Path 7
5.3. Evidence Record for a Public Key Certificate 8
5.4. Evidence Record for Revocation Information 8
5.5. Evidence Record for Any replyWantBack 8
5.6. Partial Certification Path 9
6. Security Considerations 10
7. References 10
7.1. Normative References 10
7.2. Informative References 10
Appendix A. ASN.1 Module 11

1. Introduction

Digital signatures are frequently verified using public key infrastructure (PKI) artifacts, including public key certificates and certificate revocation information. 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 the acquisition of different types of information generated by multiple PKIs. To verify 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.

SCVP [RFC5055] provides a means of delegating certification path construction and/or validation to a server, including the ability to request the status of a certificate relative to a time in the past. SCVP does not define a means of providing or validating long-term non-repudiation information. ERS [RFC4998] defines a syntax 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. LTAP [LTANS-LTAP] defines a protocol for communicating with a long-term archive (LTA) server for the purpose of preserving evidence records and data. Clients store, retrieve, and delete data using LTAP; LTAs maintain evidence records covering data submitted by clients.

This document defines an application of SCVP to permit retrieval of an evidence record corresponding to information returned by the SCVP server by creating an association between an evidence record and information contained in an SCVP response. The SCVP response can then in turn be used to verify archived data objects retrieved using LTAP. Separating the preservation of the certification path information from the preservation of data enables the LTA to store archived data objects more efficiently, i.e., complete verification information need not be stored with each archived data object. Verifiers can more efficiently process archived data objects by reusing the same certification path information to verify multiple archived data objects of similar vintage without retrieving and/or validating the same PKI artifacts multiple times.

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

During certification path processing, active SCVP servers may encounter a large portion of the PKI artifacts generated by a particular PKI. By storing and preserving these artifacts, an SCVP server can respond to queries for certificate status over very long periods of time. Optionally, SCVP servers may actively seek PKI information for storage and preservation, even when no query is made, that requires the information during its period of validity in order to service future queries relative to any point in time.

SCVP permits clients to request as much or as little information as desired from the SCVP server. Clients include zero or more Object Identifiers (OIDs) indicating the type(s) of information the server should include in the response. By defining additional OID values, clients can request an evidence record for specific types of information returned by the SCVP server. This document defines OIDs to permit the retrieval of evidence records for the following four types of information:

- end entity certificates.
- certification paths containing an end entity certificate up to a trust anchor.
- certification paths containing an intermediate certificate up to a trust anchor.
- revocation information.

Additionally, an OID is defined to permit inclusion of a single OID indicating an evidence record is desired for all information requested via the WantBack mechanism.

By associating evidence records with information maintained by an SCVP server, clients are able to determine the status of certificates over very long periods of time using SCVP without consulting additional resources. The nature of SCVP servers is well suited to the preservation of infrastructure materials. Additionally, the SCVP server's signature over an SCVP response can secure the transmission of trust anchors included in evidence records, allowing clients to refrain from establishing additional trust relationships with LTAs.

The transactions used to verify an archived data object using LTAP and the SCVP WantBacks described in this document are as follows:

- Client retrieves a signed archived data object from an LTA using LTAP.

- Client prepares an SCVP request to validate the signer's certificate at the time of interest and includes WantBacks for evidence records corresponding to the PKI artifacts required to validate the signer's certificate.

- SCVP server returns a response with status as of the time of interest and includes requested evidence records.

- Client processes the SCVP request, determines the status, and verifies the evidence records.

- Client verifies signatures in the archived data object using the validated signer's certificate.

3. Requests

Clients request long-term archive evidence records from an SCVP server by including one of the following OIDs in the wantBack field of a CVRequest sent to an SCVP server:

- id-swb-ers-best-cert-path

- id-swb-ers-partial-cert-path

- id-swb-ers-pkc-cert

- id-swb-ers-revocation-info

- id-swb-ers-all

Additionally, id-swb-partial-cert-path is defined to permit clients to request a partial certification path consisting of the certification authority (CA) that issued the end entity certificate through a trust anchor. This is similar to the id-swb-best-cert-path WantBack defined in SCVP except the resulting replyWantBack will contain a CertBundle containing the certification path minus the end entity certificate.

For each id-swb-ers OID except id-swb-ers-all, an EvidenceRecord (as defined in [RFC4998]) covering the corresponding information in the response will be returned as a replyWantBack. For example, if a client wishes to obtain a certification path and revocation information plus an evidence record for each, the SCVP request would include the following four replyWantBack OIDs: id-swb-best-cert-path, id-swb-pkc-revocation-info, id-swb-ers-best-cert-path, and id-swb-ers-revocation-info.

Alternatively, for id-swb-ers-all, an EvidenceRecordWantBacks structure will be returned containing an EvidenceRecord for each information item contained in the replyWantBacks field. For example, if a client wishes to obtain a certification path and revocation information plus an evidence record for each, the SCVP request could include the following three replyWantBack OIDs: id-swb-best-cert-path, id-swb-pkc-revocation-info, and id-swb-ers-all.

4. Responses

When a client request contains a WantBack request for an evidence record, the response generated MUST include the replyWantBack containing the requested information plus a replyWantBack containing the evidence record corresponding to that information. For each id-swb-ers OID except id-swb-ers-pkc-cert and id-swb-ers-revocation-info, the evidence record MUST be calculated over the value of the value field in the corresponding replyWantBack; the tag and length bytes are not covered by the evidence record. The targets for the id-swb-ers-pkc-cert and id-swb-ers-revocation-info replyWantBacks are described below. For example, if a client request contains id-swb-pkc-best-cert-path and id-swb-ers-best-cert-path, the resulting response will contain a replyWantBack of each type where the evidence record covers the DER-encoded CertBundle returned in the id-swb-pkc-best-cert-path replyWantBack. For id-swb-ers-pkc-cert, the evidence record MUST be calculated over the value of the cert field in the CertReply object. For id-swb-ers-revocation-info, a sequence of evidence records is returned. Each revocation information object contained in the id-swb-pkc-revocation-info replyWantBack is covered by an evidence record in the id-swb-ers-revocation-info replyWantBack. A single evidence record may cover multiple revocation information objects. The correct evidence record can be identified by locating the hash of the revocation information object in the first initial timestamp of the evidence record.

If the server cannot return an EvidenceRecord for the requested information item, a replyWantBack of the appropriate type MUST be returned with an empty value field. For example, if a client requests id-swb-ers-pkc-cert and the server cannot fulfill the request, the resulting response will contain a replyWantBack with the wb field set to id-swb-ers-pkc-cert and the value field empty, i.e., zero length.

5. WantBacks

The following sections describe each WantBack defined in this document. Each WantBack for an evidence record requires a corresponding WantBack for the object covered by the evidence record to be present in the request. Upon receipt of a request missing the

corresponding WantBack for the object covered by a requested evidence record, the server MUST indicate wantBackUnsatisfied in the ReplyStatus. Clients MAY ignore evidence record WantBacks when the WantBack for the corresponding object is not present.

5.1. Evidence Record for a Complete Certification Path

The id-swb-ers-best-cert-path OID is used to request an evidence record for a complete certification path. It is used in conjunction with the id-swb-best-cert-path OID. Requests containing id-swb-ers-best-cert-path as a WantBack MUST also contain id-swb-best-cert-path. Responses containing id-swb-ers-best-cert-path MUST also contain id-swb-best-cert-path.

An SCVP server may maintain evidence records for complete certification paths, i.e., certification paths containing all certificates from end entity to trust anchor. The evidence record MUST be calculated over the CertBundle returned via the id-swb-best-cert-path replyWantBack. In such cases, a signature within the archived data object may be verified using an end entity certificate returned via SCVP. The end entity certificate can be verified using SCVP using a request containing id-swb-ers-best-cert-path, id-swb-best-cert-path, id-swb-pkc-revocation-info, and id-swb-ers-revocation-info.

5.2. Evidence Record for a Partial Certification Path

The id-swb-ers-partial-cert-path OID is used to request an evidence record for a partial certification path. It is used in conjunction with the id-swb-partial-cert-path OID. Requests containing id-swb-ers-partial-cert-path as a WantBack MUST also contain id-swb-partial-cert-path. Responses containing id-swb-ers-partial-cert-path MUST also contain id-swb-partial-cert-path.

As an alternative to relying on SCVP to obtain evidence records for end entity certificates, the certificate could be included in the archived data object(s) submitted to an LTA. In such cases, a signature within the archived data object may be verified using the included end entity certificate, which is protected by the evidence record covering the archived data object, including the certificate. The end entity certificate can be verified using SCVP using a request containing id-swb-partial-cert-path, id-swb-ers-partial-cert-path, id-swb-pkc-revocation-info, and id-swb-ers-revocation-info. Unlike the partial certification path, the revocation information includes material that can be used to determine the status of the end entity certificate.

By maintaining an evidence record for a partial certification path, SCVP servers can achieve greater storage efficiency.

5.3. Evidence Record for a Public Key Certificate

The id-swb-ers-pkc-cert OID is used to request an evidence record for an individual public key certificate. It is used in conjunction with the id-swb-pkc-cert OID. Requests containing id-swb-ers-pkc-cert as a WantBack MUST also contain id-swb-pkc-cert. Responses containing id-swb-ers-pkc-cert MUST also contain id-swb-pkc-cert.

SCVP servers may maintain evidence records for individual certificates. This enables clients to omit the signer's certificate from archived data object(s) submitted to an LTA. In such cases, a signature within the archived data object may be verified using an end entity certificate returned via SCVP. The end entity certificate can be verified using SCVP using a request containing id-swb-pkc-cert, id-swb-ers-pkc-cert, id-swb-partial-cert-path, id-swb-ers-partial-cert-path, id-swb-pkc-revocation-info, and id-swb-ers-revocation-info.

5.4. Evidence Record for Revocation Information

The id-swb-ers-revocation-info OID is used to request evidence records for a set of revocation information. It is used in conjunction with the id-swb-revocation-info OID. Requests containing id-swb-ers-revocation-info as a WantBack MUST also contain id-swb-revocation-info. Responses containing id-swb-ers-revocation-info MUST also contain id-swb-revocation-info. A sequence of evidence records is returned, with one evidence record provided for each element in id-swb-revocation-info.

```
EvidenceRecords ::= SEQUENCE SIZE (1..MAX) OF EvidenceRecord
```

An SCVP server may maintain evidence records for revocation information. Revocation information may be provided in the form of CRLs or Online Certificate Status Protocol (OCSP) responses. Cumulative CRLs may be generated for archiving to simplify evidence record maintenance.

5.5. Evidence Record for Any replyWantBack

An SCVP server may maintain evidence records for additional types of information that can be returned using the wantBack mechanism, e.g., attribute certificate information. The id-swb-ers-all OID provides a shorthand means for clients to request evidence records for all information returned via the replyWantBacks field. Since id-swb-ers-all can result in the return of multiple evidence records in the

response, a mechanism is needed to associate an evidence record with the type of information covered by the evidence record. The EvidenceRecordWantBacks structure provides a flexible means of conveying an evidence record for different types of information.

```
EvidenceRecordWantBack ::= SEQUENCE
{
    targetWantBack    OBJECT IDENTIFIER,
    evidenceRecord    EvidenceRecord OPTIONAL
}

EvidenceRecordWantBacks ::=
    SEQUENCE SIZE (1..MAX) OF EvidenceRecordWantBack
```

EvidenceRecordWantBacks is a SEQUENCE OF EvidenceRecordWantBack structures. The targetWantBack field indicates the type of replyWantBack covered by the associated EvidenceRecord. The evidenceRecord field, if present, contains an EvidenceRecord structure calculated over the replyWantBack indicated by the targetWantBack field. Where EvidenceRecordWantBacks is used, there MUST be a one-to-one correspondence between other replyWantBack objects and objects in the EvidenceRecordWantBacks collection. If a server does not have an EvidenceRecord for a particular replyWantBack object, an EvidenceRecordWantBack with the evidenceRecord field absent should be included in the EvidenceRecordWantBacks collection.

5.6. Partial Certification Path

The id-swb-partial-cert-path is an alternative to id-swb-best-cert-path. This is the only OID defined in this document for which an EvidenceRecord is not returned in the response. For efficiency, SCVP servers that maintain evidence records for certification paths may only do so for partial paths instead of maintaining one or more paths for each end entity certificate.

SCVP clients can include id-swb-partial-cert-path in a request when a partial certification path is required. This would typically be included along with id-swb-ers-partial-cert-path to account for the fact that some SCVP servers only produce evidence records for partial paths for storage and computational efficiency reasons. In such cases, a separate evidence record may be available for the end entity certificate by including id-swb-pkc-cert and id-swb-ers-pkc-cert in the request.

6. Security Considerations

For security considerations specific to SCVP, see [RFC5055]. For security considerations specific to ERS, see [RFC4998].

The signature on the SCVP response containing one or more ERS structures must be verified using a public key trusted by the relying party. The response may contain trust anchors used to verify interior layers of an ERS structure. The trust anchors are protected by the SCVP server's signature covering the response. The relying party may elect to use the trust anchors conveyed in the response or ignore the trust anchors in favor of trust anchors retrieved out of band. Relying parties SHOULD ignore trust anchors contained in unsigned SCVP responses.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4998] Gondrom, T., Brandner, R., and U. Pordesch, "Evidence Record Syntax (ERS)", RFC 4998, August 2007.

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, December 2007.

7.2. Informative References

[LTANS-LTAP] Jerman-Blazic, A., Sylvester, P., and C. Wallace, "Long-term Archive Protocol (LTAP)", Work in Progress, February 2008.

Appendix A. ASN.1 Module

The following ASN.1 module defines object identifiers used to identify six new forms of SCVP WantBacks and three new structures. EvidenceRecordWantBack and EvidenceRecordWantBacks are used in conjunction with the id-swb-ers-all WantBack to correlate evidence records with WantBacks. EvidenceRecords is used in conjunction with the id-swb-ers-revocation-info WantBack to return evidence records for individual revocation information objects.

```
LTANS-SCVP-EXTENSION
{ iso(1) identified-organization(3) dod(6) internet(1)
   security(5) mechanisms(5) ltans(11) id-mod(0) id-mod-ers-scvp(5)
   id-mod-ers-scvp-v1(1) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

id-swb
FROM SCVP
{ iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0) 21 }

EvidenceRecord
FROM ERS
{iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) ltans(11) id-mod(0) id-mod-ers88(2)
    id-mod-ers88-v1(1) };

id-swb-partial-cert-path        OBJECT IDENTIFIER ::= {id-swb 15 }

id-swb-ers-pkc-cert             OBJECT IDENTIFIER ::= {id-swb 16 }
id-swb-ers-best-cert-path       OBJECT IDENTIFIER ::= {id-swb 17 }
id-swb-ers-partial-cert-path    OBJECT IDENTIFIER ::= {id-swb 18 }
id-swb-ers-revocation-info      OBJECT IDENTIFIER ::= {id-swb 19 }
id-swb-ers-all                  OBJECT IDENTIFIER ::= {id-swb 20 }

EvidenceRecordWantBack ::= SEQUENCE
{
    targetWantBack    OBJECT IDENTIFIER,
    evidenceRecord    EvidenceRecord OPTIONAL
}
```

```
   EvidenceRecordWantBacks ::=
       SEQUENCE SIZE (1..MAX) OF EvidenceRecordWantBack

   EvidenceRecords ::= SEQUENCE SIZE (1..MAX) OF EvidenceRecord

   END
```

Author's Address

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

EMail: cwallace@cygnacom.com

Full Copyright Statement

Intellectual Property