Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

J. Peterson
Neustar
S. Turner
sn3rd

March 13, 2017

OCSP Usage for Secure Telephone Identity Certificates
draft-ietf-stir-certificates-ocsp-00.txt

Abstract

When certificates are used as credentials to attest the assignment or ownership of telephone numbers, some mechanism is required to convey certificate freshness to relying parties. This document specifies the use of the Online Certificate Status Protocol (OCSP) as a means of retrieving real-time status information about such certificates, defining new extensions to compensate for the dynamism of telephone number assignments.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 14, 2017.

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] discusses many attacks on the telephone network that are enabled by impersonation, including various forms of robocalling, voicemail hacking, and swatting. One of the most important components of a system to prevent impersonation is the implementation of credentials which identify the parties who control telephone numbers. The STIR certificates [I-D.ietf-stir-certificates] specification describes a credential system based on [X.509] version 3 certificates in accordance with [RFC5280] for that purpose. Those credentials can then be used by STIR authentication services [I-D.ietf-stir-rfc4474bis] to sign PASSporT objects [I-D.ietf-stir-passport] carried in a SIP [RFC3261] request.

The STIR certificates document specifies an extension to X.509 that defines a Telephony Number (TN) Authorization List that may be included by certificate authorities in certificates. This extension provides additional information that relying parties can use when validating transactions with the certificate. When a SIP request, for example, arrives at a terminating administrative domain, the calling number attested by the SIP request can be compared to the TN Authorization List of the certificate that signed the request to determine if the caller is authorized to use that calling number in SIP.

However, there is significant dynamism in telephone number assignment, and due to practices like number portability, information about number assignment can suddenly become stale. This problem is especially pronounced when a TN Authorization List extension associates a large block of telephone numbers with a certificate, as relying parties need a way to learn if any one of those telephone numbers has been ported to a different administrative entity.

No specific recommendation is made in the STIR certificates document for a means of determining the freshness of certificates with a TN Authorization List. This document explores approaches to real-time status information for such certificates, and recommends an approach.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Certificate Verification Methods

For traditional certificate status information, there are three common certificate verification mechanisms employed by CAs:

1. Certificate Revocation Lists (CRLs) [RFC5280] (and [RFC6818])

2. Online Certificate Status Protocol (OCSP) [RFC6960], and

3. Server-based Certificate Validation Protocol (SCVP) [RFC5055].

When relying on status information, the verifier needs to obtain the status information - but before that can happen, the verifier needs to know where to locate it. Placing the location of the status information in the certificate makes the certificate larger, but it eases the client workload. The CRL Distribution Point certificate extension includes the location of the CRL and the Authority Information Access certificate extension includes the location of OCSP and/or SCVP servers; both of these extensions are defined in [RFC5280]. In all cases, the status information location is provided in the form of an URI.

CRLs are an attractive solution because they are supported by every CA. CRLs have a reputation of being quite large (10s of MBytes), because CAs maintain and issue one monolithic CRL with all of their revoked certificates, but CRLs do support a variety of mechanisms to scope the size of the CRLs based on revocation reasons (e.g., key compromise vs CA compromise), user certificates only, and CA

certificates only as well as just operationally deciding to keep the CRLs small. However, scoping the CRL introduces other issues (i.e., does the RP have all of the CRL partitions).

CAs in the STIR architecture will likely all create CRLs for audit purposes, but probably not for real-time status information. Any such CRLs used MUST be signed with the same algorithm as the certificate. We thus anticipate that one of the two "online" options is preferred. Between the two, OCSP is much more widely deployed and this document therefore RECOMMENDS the use of OCSP in high-volume environments (HVE) for validating the freshness of certificates, based on [RFC6960], incorporating some (but not all) of the optimizations of [RFC5019].

3.1. Using OCSP with TN Auth List

Certificates compliant with this specification SHOULD include a URL [RFC3986] pointing to an OCSP service in the Authority Information Access (AIA) certificate extension, via the "id-ad-ocsp" accessMethod specified in [RFC5280]. It is RECOMMENDED that entities that issue certificates with the Telephone Number Authorization List certificate extension run an OCSP server for this purpose. Baseline OCSP however supports only three possible response values: good, revoked, or unknown. Without some extension, OCSP would not indicate whether the certificate is authorized for a particular telephone number that the verifier is validating.

At a high level, there are two ways that a client might pose this authorization question:

> For this certificate, is the following number currently in its scope of validity?
>
> What are all the telephone numbers associated with this certificate, or this certificate subject?

Only the former lends itself to piggybacking on the OCSP status mechanism; since the verifier is already asking an authority about the certificate’s status, that mechanism can be reused instead of creating a new service that requires additional round trips? Like most PKIX-developed protocols, OCSP is extensible; OCSP supports request extensions (including sending multiple requests at once) and per-request extensions. It seems unlikely that the verifier will be requesting authorization checks on multiple telephone numbers in one request, so a per-request extension is what is needed.

The requirement to consult OCSP in real time results in a network round-trip delay, which is something to consider because it will add

to the call setup time. OCSP server implementations commonly pre-generate responses, and to speed up HTTPS connections, servers often provide OCSP responses for each certificate in their hierarchy. If possible, both of these OCSP concepts should be adopted for use with STIR.

3.1.1. OCSP Extension Specification

The extension mechanism for OCSP follows X.509 v3 certificate extensions, and thus requires an OID, a criticality flag, and ASN.1 syntax as defined by the OID. The criticality specified here is optional: per [RFC6960] Section 4.4, support for all OCSP extensions is optional. If the OCSP server does not understand the requested extension, it will still provide the baseline validation of the certificate itself. Moreover, in practical STIR deployments, the issuer of the certificate will set the accessLocation for the OCSP AIA extension to point to an OCSP service that supports this extension, so the risk of interoperability failure due to lack of support for this extension is minimal.

The OCSP TNQuery extension is included as one of the request's singleRequestExtensions. It may also appear in the response's singleExtensions. When an OCSP server includes a number in the response's singleExtensions, this informs the client that the certificate is still valid for the number that appears in the TNQuery extension field. If the TNQuery is absent from a response to a query containing a TNQuery in its singleRequestExtension, then the server is not able to validate that the number is still in the scope of authority of the certificate.

```
id-pkix-ocsp-stir-tn  OBJECT IDENTIFIER ::= { id-pkix-ocsp 10 }

TNQuery ::= E164Number
```

The HVE OCSP profile [RFC5019] prohibits the use of per-request extensions. As it is anticipated that STIR will use OCSP in a high-volume environment, many of the optimizations recommended by HVE are desirable for the STIR environment. This document therefore uses the HVE optimizations augmented as follows:

- Implementations MUST use SHA-256 as the hashing algorithm for the CertID.issuerNameHash and the CertID.issuerKeyHash values. That is CertID.hashAlgorithm is id-sha256 [RFC4055] and the values are truncated to 160-bits as specified Option 1 in Section 2 of [RFC7093].

- Clients MUST include the OCSP TNQuery extension in requests' singleRequestExtensions.

- Servers MUST include the OCSP TNQuery extension in responses' singleExtensions.

- Servers SHOULD return responses that would otherwise have been "unknown" as "not good" (i.e., return only "good" and "not good" responses).

- Clients MUST treat returned "unknown" responses as "not good".

- If the server uses ResponderID, it MUST generate the KeyHash using SHA-256 and truncate the value to 160-bits as specified in Option 1 in Section 2 of [RFC7093].

- Implementations MUST support ECDSA using P-256 and SHA-256. Note that [RFC6960] requires RSA with SHA-256 be supported.

- This removes the requirement to support SHA-1, RSA with SHA-1, or DSA with SHA-1.

OCSP responses MUST be signed using the same algorithm as the certificate being checked.

To facilitate matching the authority key identifier values found in CA certificates with the KeyHash used in the OCSP response, certificates compliant with this specification MUST generate authority key identifiers and subject key identifiers using the SHA-256 and truncate the value to 160-bits as specified in Option 1 in Section 2 of [RFC7093].

Ideally, once a certificate has been acquired by a verifier, some sort of asynchronous mechanism could notify and update the verifier if the scope of the certificate changes so that verifiers could implement a cache. While not all possible categories of verifiers could implement such behavior, some sort of event-driven notification of certificate status is another potential subject of future work. One potential direction is that a future SIP SUBSCRIBE/NOTIFY-based accessMethod for AIA might be defined (which would also be applicable to the method described in the following section) by some future specification.

4. IANA Considerations

This document makes use of object identifiers for the TN-HVE OCSP extension in Section 3.1.1 and the ASN.1 module identifier defined in Appendix A. It therefore requests that the IANA make the following assignments:

TN-HVE OCSP extension in the SMI Security for PKIX Online Certificate Status Protocol (OCSP) registry: http://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#smi-numbers-1.3.6.1.5.5.7.48.1

5. Privacy Considerations

Querying for real-time status information about certificates can allow parties monitoring communications to gather information about relying parties and the originators of communications. Unfortunately, the TNQuery extension adds a new field that could potentaily be monitored by OCSP eavesdroppers: the calling telephone number provides a specific piece of additional data about the originator of communications. Using OCSP over TLS is one potential countermeasure to this threat, as described in [RFC6960] Appendix A.1.

Another way to mitigate leaking information about relying parties is to use OCSP stapling. Strategies for stapling OCSP [RFC6961] have become common in some web PKI environments as an optimization which allows web servers to send up-to-date certificate status information acquired from OCSP to clients as TLS is negotiated. A similar mechanism could be implemented for SIP requests, in which the authentication service adds status information for its certificate to the SIP request, which would save the verifier the trouble of performing the OCSP dip itself. Especially for high-volume authentication and verification services, this could furthermore result in significant performance improvements. This would however require work on a generic SIP capability to carry OCSP staples that is outside the scope of this document.

6. Security Considerations

This document is entirely about security. For further information on certificate security and practices, see [RFC5280], in particular its Security Considerations. For OCSP-related security considerations see [RFC6960] and [RFC5019].

7. Acknowledgments

Stephen Farrell provided key input to the discussions leading to this document. Russ Housley provided some direct assistance and text surrounding the ASN.1 module.

8. References

8.1. Normative References

[I-D.ietf-stir-certificates]
Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", draft-ietf-stir-certificates-11 (work in progress), October 2016.

[I-D.ietf-stir-passport]
Wendt, C. and J. Peterson, "Personal Assertion Token (PASSporT)", draft-ietf-stir-passport-11 (work in progress), February 2017.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-16 (work in progress), February 2017.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, DOI 10.17487/RFC4055, June 2005, <http://www.rfc-editor.org/info/rfc4055>.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, DOI 10.17487/RFC5019, September 2007, <http://www.rfc-editor.org/info/rfc5019>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <http://www.rfc-editor.org/info/rfc5912>.

[RFC6818] Yee, P., "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 6818, DOI 10.17487/RFC6818, January 2013, <http://www.rfc-editor.org/info/rfc6818>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <http://www.rfc-editor.org/info/rfc6960>.

[RFC7093] Turner, S., Kent, S., and J. Manger, "Additional Methods for Generating Key Identifiers Values", RFC 7093, DOI 10.17487/RFC7093, December 2013, <http://www.rfc-editor.org/info/rfc7093>.

[X.509] ITU-T Recommendation X.509 (10/2012) | ISO/IEC 9594-8, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", 2012.

[X.680] ITU-T Recommendation X.680 (08/2015) | ISO/IEC 8824-1, "Information Technology - Abstract Syntax Notation One: Specification of basic notation".

[X.681] ITU-T Recommendation X.681 (08/2015) | ISO/IEC 8824-2, "Information Technology - Abstract Syntax Notation One: Information Object Specification".

[X.682] ITU-T Recommendation X.682 (08/2015) | ISO/IEC 8824-2, "Information Technology - Abstract Syntax Notation One: Constraint Specification".

[X.683] ITU-T Recommendation X.683 (08/2015) | ISO/IEC 8824-3, "Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications".

8.2. Informative References

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, DOI 10.17487/RFC5055, December 2007, <http://www.rfc-editor.org/info/rfc5055>.

[RFC6961] Pettersen, Y., "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", RFC 6961, DOI 10.17487/RFC6961, June 2013, <http://www.rfc-editor.org/info/rfc6961>.

[RFC7340] Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", RFC 7340, DOI 10.17487/RFC7340, September 2014, <http://www.rfc-editor.org/info/rfc7340>.

Appendix A. ASN.1 Module

This appendix provides the normative ASN.1 [X.680] definitions for the structures described in this specification using ASN.1, as defined in [X.680] through [X.683].

The modules defined in this document are compatible with the most current ASN.1 specification published in 2015 (see [X.680], [X.681], [X.682], [X.683]). None of the newly defined tokens in the 2008 ASN.1 (DATE, DATE-TIME, DURATION, NOT-A-NUMBER, OID-IRI, RELATIVE-OID-IRI, TIME, TIME-OF-DAY)) are currently used in any of the ASN.1 specifications referred to here.

This ASN.1 module imports ASN.1 from [RFC5912].

[TO DO: this ASN.1 module is a stub and needs to be redone!]

```
  TN-Module-2016-2 {
  iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-tn-module(88) }

  DEFINITIONS EXPLICIT TAGS ::= BEGIN

  IMPORTS
  id-ad, id-ad-ocsp, id-pe                              -- From [RFC5912]
  FROM PKIX1Explicit-2009 {
  iso(1) identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

  EXTENSION                                          -- From [RFC5912]
  FROM PKIX-CommonTypes-2009 {
  iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-pkixCommon-02(57) }

  ;

  id-pkix-ocsp OBECT IDENTIFIER ::= id-ad-ocsp

  --
  -- Telephone Number Query OCSP Extension
  --

  re-ocsp-tn-query  EXTENSION ::= {
  SYNTAX TNQuery IDENTIFIED BY id-pkix-ocsp-stir-tn }

  TNQuery ::= E164Number

  id-pkix-ocsp-stir-tn    OBJECT IDENTIFIER ::= { id-pkix-ocsp 10 }



  END
```

Authors' Addresses

Jon Peterson
Neustar, Inc.

Email: jon.peterson@neustar.biz

Sean Turner
sn3rd

Email: sean@sn3rd.com