Workgroup: Network Working Group
Internet-Draft:
draft-peterson-stir-ocsp-staple-00
Published: 24 October 2022
Intended Status: Standards Track
Expires: 27 April 2023
Authors: J. Peterson
Neustar

OCSP Stapling for Secure Telephone Identity

Abstract

In order to facilitate the use of the Online Certificate Status Protocol (OCSP) with Secure Telephone Identity Revisited (STIR), this specification defines a mechanism for incorporating an OCSP staple into a Personal Assertion Token (PASSporT).

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 https://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 27 April 2023.

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 [RFC8226] 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 [RFC8224] to sign PASSporT objects [RFC8225] carried in a SIP [RFC3261] request.

[RFC8226] 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.

[I-D.ietf-stir-certificates-ocsp] defines a means to use OCSP to establish that, at the time of STIR verification, a particular telephone number (the calling number) is within the scope of authority of a certificate. This is especially useful with STIR delegate certificates [RFC9060], which typically claim authority over telephone number ranges rather than Service Provider Codes (SPCs) in their TN Authorization List. However, this requires an additional round-trip request and response from the verification service to the OCSP responder, and the telephony applications are

delay sensitive. Thus, this document specifies a means to incorporate an OCSP staple into the PASSporT object.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Approaches to OCSP Stapling

At a high level, there are a number of potential solutions that could mitigate the round-trip time incurred on the verification service side to perform OCSP validation.

A verification service validating a PASSporT acquires the certificate referenced by its "x5u" header element, if that certificate is not cached. Typically, that acquisition happens by derefencing the URI in the value of the "x5u" element. One could design an system where OCSP validation is piggybacked onto that network fetch. This solution is however not optimal for cases where signing certificates are long-lived and cached, so that queries will otherwise be very infrequent. Requiring certificate fetches every time a new telephone number is seen at the verification service would likely incur roughly the same number of round trips as the [I-D.peterson-stir-certificates-shortlived] mechanism.

There are also variants of the "x5u" approach that sidestep OCSP entirely, by decorating the "x5u" URI with query parameters that incorporate the calling telephone number. As the authentication service necessarily knows the telephone number from the "orig" field, and controls the contents of "x5u", it has the means to decorate the URI appropriately during PASSporT creation. The certificate repository (i.e. HTTP service) receiving a certificate fetch with a decorated URI could could then verify that the calling number is currently in the scope of the requested certificate - if it is not, the service could then fail to return a certificate, preventing the verification service from validating. However, like the approach above, this would have implications for certificate fetch frequency similar to short-lived certs, as the decorated URIs would be governed by HTTP caching mechanics.

Thus, the solution proposed here is that the authentication service instead inserts a new PASSporT payload element, "stpl", which has as its value an OCSP staple compliant with the STIR extension defined in [I-D.ietf-stir-certificates-ocsp]. Such staples can either be pre-generated ([RFC6960] Section 2.5) and published regularly to the

authentication service, or the authentication service can query for a staple on a per-call basis. Note that OCSP for STIR does furnish a response concerning only a single telephone number, and thus if a certificate can sign for a large number range, one pre-generated staple would need to be furnished to the authentication service for each telephone number that could potentially originate a call. Generating OCSP staples on the fly may however cause a round-trip time delay of its own, which depending on how the authentication service and the certificate authority are connected, could effectively incur the same delay as an OCSP dip from the verification service.

One alternative design would be to carry an OCSP staple at the SIP layer, in a body or header. But the because PASSporT can be used in non-SIP environments, and this OCSP extension is specific to certificates that use the TNAuthList extension, embedding the staple in the PASSporT is a superior choice. While encoding and embedding an OCSP response will increase the size of the PASSporT, that overall increase in SIP message size will ideally be the same as if the response had been placed in a separate header.

Finally, it could be argued that the round-trip delay incurred at the verification service is not actually problematic, as there is a fungible delay on the terminating side during which ringing can be played to the caller without commencing alerting on the end-user called device. But [I-D.ietf-stir-certificates-ocsp] also describes the potential privacy implications of revealing to the OCSP responder the verification service that has received a call for a particular calling number. On balance, stapling at the authentication service, especially pre-generated stapling, seems to offer the best all-around solution.

4. OCSP Staple PASSporT Element

TBD.

5. IANA Considerations

This specification requests that the IANA add one new claim to the JSON Web Token Claims registry as defined in [RFC7519].

Claim Name: "stpl"

Claim Description: OCSP Staple

Change Controller: IESG

Specification Document(s): [RFCThis]

6. Privacy Considerations

The use of OCSP stapling should largely mitigate the privacy risks noted in [I-D.ietf-stir-certificates-ocsp].

7. 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].

8. Acknowledgments

We thank the STIR working group for its input into this document.

9. References

9.1. Normative References

[I-D.ietf-stir-certificates-ocsp] Peterson, J. and S. Turner, "OCSP Usage for Secure Telephone Identity Certificates", Work in Progress, Internet-Draft, draft-ietf-stir-certificates-ocsp-02, 11 July 2022, <https://www.ietf.org/archive/id/draft-ietf-stir-certificates-ocsp-02.txt>.

[I-D.peterson-stir-certificates-shortlived] Peterson, J., "Short-Lived Certificates for Secure Telephone Identity", Work in Progress, Internet-Draft, draft-peterson-stir-certificates-shortlived-03, 21 April 2022, <https://www.ietf.org/archive/id/draft-peterson-stir-certificates-shortlived-03.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://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, <https://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, <https://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, <https://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, <https://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, <https://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, <https://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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7093>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8224] Peterson, J., Jennings, C., Rescorla, E., and C. Wendt, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 8224, DOI 10.17487/RFC8224, February 2018, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, February 2018, <https://www.rfc-editor.org/info/rfc8225>.

[RFC8226] Peterson, J. and S. Turner, "Secure Telephone Identity Credentials: Certificates", RFC 8226, DOI 10.17487/RFC8226, February 2018, <https://www.rfc-editor.org/info/rfc8226>.

[RFC9060] Peterson, J., "Secure Telephone Identity Revisited (STIR) Certificate Delegation", RFC 9060, DOI 10.17487/RFC9060, September 2021, <https://www.rfc-editor.org/info/rfc9060>.

[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".

9.2. 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, <https://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, <https://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, <https://www.rfc-editor.org/info/rfc7340>.

Author's Address

Jon Peterson
Neustar (a TransUnion company)

Email: jon.peterson@team.neustar