Short-Lived Certificates for Secure Telephone Identity
draft-peterson-stir-certificates-shortlived-02.txt

Abstract

When certificates are used as credentials to attest the assignment of
ownership of telephone numbers, some mechanism is required to provide
certificate freshness. This document specifies short-lived
certificates as a means of guaranteeing certificate freshness for
secure telephone identity (STIR), in particular relying on the
Automated Certificate Management Environment (ACME) to allow signers
to acquire certificates as needed.

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 September 6, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(https://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
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.

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.

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 how short-lived certificates could be used as a means of preserving that freshness. Short-lived certificates also have a number of other desirable
properties that fulfill important operational requirements for network operators. The use of the Automated Certificate Management Environment (ACME) [I-D.ietf-acme-acme] to manage these short-lived certificates is the focus of the architecture specified, in particular adapting the Short-Term Automatically Renewed (STAR) [I-D.ietf-acme-star] mechanism to STIR. The interaction of STIR with ACME has already been explored in [I-D.wendt-acme-authority-token-tauthlist].

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. Short-lived certificates for STIR

While there is no easy definition of what constitutes a "short-lived" certificate, the term typically refers to certificates that are valid only for days or even hours, as opposed to the months or years common in traditional public key infrastructures. When the private keying material associated with that has an expiry of months or years is compromised by an adversary, the issuing authority must revoke the certificate, which requires relying parties to review certificate revocation lists or to access real-time status information with protocols such as OCSP. Short-lived certificates offer an alternative where, if compromised, certificates will shortly expire anyway, and rather than revoking and reissuing the certificate in response to a crisis, certificates routinely roll-over and cannot be cached for a long term by relying parties, minimizing their value to attackers.

One of the additional benefits of using short-lived certificates is that they do not require relying parties to perform any certificate freshness check. The trade-off is that the signer must acquire new certificates frequently, so the cost of round-trip times to the certificate authority is paid on the signer’s side rather than the verifier’s side; however, in environments where many parties may rely on a single certificate, or at least where a single certificate will be used to sign many transactions during its short lifetime, the overall architecture will incur fewer round-trip times to the certificate authority and thus less processing delay.

In the STIR context, the TN Authorization List defined in [RFC8226] adds a new wrinkle to the behavior of short-lived certificates. Because a subject may have authority over multiple telephone numbers, a certificate issued to that subject could attest the authority over
all, some, or just one of those telephone numbers. If an authentication service wanted to acquire a new certificate on a per-call basis, for example, they could acquire a certificate that can only sign for the calling party number of the call in question. At the other end of the spectrum, a large service provider could acquire a certificate valid for millions of numbers, but expire the certificate after a very short duration — on the order of hours — to reduce the risk that the certificate would be compromised.

This inherent flexibility in the short-lived certificate architecture would also permit authentication services to implement very narrow policies for certificate usage. A large service provider who wanted to avoid revealing which phone numbers they controlled, for example, could provide no information in the certificate that signs a call other than just the single telephone number that corresponds to the calling party’s number. How frequently the service provider feels that they need to expire that certificate and acquire a new one is entirely a matter of policy to them. This makes it much harder for entities monitoring signatures over calls to guess who owns which numbers, and provides a much more complicated threat surface for attackers trying to compromise the service.

In order to reduce the burden on verification services, an authentication service could also piggyback a short-lived certificate onto the signed SIP request, so that no network lookup and consequent round-trip delay would be required on the terminating side to acquire the new certificate. [RFC8224] already provides a way of pointing to a certificate in a MIME body associated with the SIP request. Future work could specify other means of carrying certificates within SIP requests via a header rather than a body, to optimize for intermediaries adding and extracting these certificates.

4. Certificate Acquisition with ACME

One of the primary challenges facing short-lived certificates is building an operational system that allows signers to acquire new certificates and put them to immediate use. ACME [I-D.ietf-acme-acme] is designed for exactly this purpose. After a client registers with an ACME server, and the authority of the client for the names in question is established (through means such as [I-D.wendt-acme-authority-token-tauthlist]), the client can at any time apply for a certificate to be issued by sending an appropriate JSON request to the server. That request will contain a CSR [RFC2986] indicating the intended scope of authority as well the validity interval of the certificate in question. Ultimately, this will enable the client to download the certificate from a certificate URL designated by the server.
ACME is based on the concept that clients establish accounts at an ACME server, and that through challenges, the server learns which identifiers it will issue for certificates requested for an account. Any given certificate issued for an account can be for just one of those identifiers, or potentially for more: this is determined by the CSR that an ACME client creates for a particular order. Thus, a service provider with authority for millions of identifiers – that is, millions of telephone numbers – could create a CSR for an ACME order that requests a certificate only associated with one of those telephone numbers if it so desired. The same would be true of certificates based on Service Provider Codes (SPCs) as described in [RFC8226]: a service provider might have just one SPC or perhaps many. ACME thus puts needed flexibility into the hands of the clients requesting certificates to determine how much of their authority they want to invest in any given certificate.

ACME also provides a mechanism that allows the assignee of a number to delegate temporary authority for it to a user. ACME Short-Term Automatically-Renewed (STAR [I-D.ietf-acme-star]) certificates provide a property of automatic renewal for ACME orders, one that assumes that certificates issuance is based on a hierarchical delegation. A short-term certificate attesting authority for a particular identifier might be issued for an interval of 72 hours, for example, by the owner of the identifier to a delegate. In the STAR model, the interface used by the owner of the identifier and the delegate is out of the scope of ACME, as it would be for an adaptation of STAR to telephone numbers (likely it would be an interface similar to MODERN [I-D.ietf-modern-problem-framework]). STAR permits the delegate to acquire new certificates directly from the ACME server at each renewal interval. Because the owner of the identifier in STAR actually fulfills the ACME challenge and retrieves the Order ID for the certificate, the owner may at any time send a certificate termination request to the ACME server, which will prevent the certificate from being renewed by the delegate at the next renewal interval.

[I-D.wendt-acme-authority-token-tnauthlist] uses the ATC framework of [I-D.peterson-acme-authority-token] to generate tokens that are provided to the CA in response to ACME challenges. For a usage with short-term certificates, it may make sense for the ATC tokens to have a relatively long expiry, so that the ACME client does not have to constantly return to the Token Authority for new tokens.

[TBD: More on when the ACME stuff gets into better shape, and on adapting STAR]
5. IANA Considerations

This document contains no actions for the IANA.

6. Privacy Considerations

Short-lived certificates provide attractive privacy properties when compared to real-time status query protocols like OCSP, which require relying parties to perform a network dip that can reveal a great deal about the source and destination of communications. For STIR, these problems are compounded by the presence of the TN Authorization List extension to certificates. Short-lived certificates can minimize the data that needs to appear in the TN Authorization List, and consequently reduce the amount of information about the caller leaked by certificate usage to an amount equal to what is leaked by the call signaling itself.

[More TBD]

7. Security Considerations

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

8. Acknowledgments

Stephen Farrell provided key input to the discussions leading to this document.

9. References

9.1. Normative References

[ATIS-0300251]


Internet-Draft              STIR Certs Short                  March 2018

[ RFC7519 ]  Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token
             (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015,

[ 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,

[ RFC8225 ]  Wendt, C. and J. Peterson, "PASSporT: Personal Assertion
             Token", RFC 8225, DOI 10.17487/RFC8225, February 2018,

             Credentials: Certificates", RFC 8226,
             DOI 10.17487/RFC8226, February 2018,

[ 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.

             "Information Technology - Abstract Syntax Notation One:
             Specification of basic notation".

             "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".

             "Information Technology - Abstract Syntax Notation One:
             Parameterization of ASN.1 Specifications".

9.2.  Informative References

[ I-D.ietf-modern-problem-framework ]
        Peterson, J. and T. McGarry, "Modern Problem Statement,
        Use Cases, and Framework", draft-ietf-modern-problem-
        framework-03 (work in progress), July 2017.


Author’s Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar