Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 January 2026

J. Peterson
TransUnion

6 July 2025

Short-Lived Certificates for Secure Telephone Identity
draft-ietf-stir-certificates-shortlived-03

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), potentially relying on the Automated Certificate Management Environment (ACME) or similar mechanisms 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 7 January 2026.

Copyright Notice

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.

The STIR certificates document specifies an extension to X.509 that defines a Telephony Number (TN) Authorization List that may be included by certification authorities in certificates. This extension provides additional information that relying parties can use when validating transactions with the certificate: either in the form of Service Provider Codes (SPCs) or telephone numbers. Telephone numbers or number ranges are used in delegate STIR certificates [RFC9060]. When a SIP request arrives at a terminating administrative domain, for example, the calling number attested by

the SIP request can be compared to the TN Authorization List of the delegate 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. A mechanism such as the Automated Certificate Management Environment (ACME) [RFC8555] could be leveraged to manage these short-lived certificates, as well as various web-based interfaces or other out-of-band mechanisms. The interaction of STIR with ACME has already been explored in [RFC9448], so it provides a potentially attractive way of delivering short-lived certificates.

As the use of short-lived certificates described below involves a certificate chain included by-value in the PASSporT header, this document revises the guidance of [RFC8224] Section 4.1 to REQUIRE the use of "x5c" in the PASSporT header when short-lived certificates are present.

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. 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 a certificate with 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 certification 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 certification 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, especially when the TN Authorization List is populated with telephone numbers or number ranges instead of Service Provider Codes (SPCs). A subject may have authority over multiple telephone numbers, but a particular short-lived certificate issued to that subject could attest the authority over all, some, or just one of those telephone numbers. Short-lived certificates permit a more on-demand certification process, where subjects acquire certificates as needed, potentially in reaction to calls being placed. A STIR authentication service could even acquire a new certificate on a per-call basis that can only sign for the calling party number of the call in question, as it would expire immediately thereafter. At the other end of the spectrum, a large enterprise 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 local policy. 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.

4. Certificate conveyance with ’x5c’

In order to reduce the burden on verification services, an authentication service could also piggyback a short-lived certificate onto the PASSporT, so that no network lookup and consequent round-trip delay would be required on the terminating side to acquire the new certificate. In particular, the poor cacheability of short-lived certificates may require frequent fetches of certificates via the "x5u" PASSporT header element when relying parties validate PASSporTs.

As an optimization, this specification permits the conveyance of the certificate chain for a short-lived certificate via the "x5c" JWS header element ([RFC7515] Section 4.1.6). The "x5c" element contains a base64 encoded PEM representation of the certificate chain. STIR Verification service implementations compliant with this specification MUST support the "x5c" element; authentication services MUST use the "x5c" format for PASSporTs signed by certificates with an valid lifetime shorter than one week. The presence of x5c creates PASSporT objects that are considerable larger than typical RFC8225 tokens, and the longer the certificate chain, the larger the PASSporT header will be. But provided the certificate chain leads to a trusted certification authority, "x5c" precludes the need for a round-trip time before validation at the STIR verification service. The root cerificate SHOULD NOT be included in the chain, though it may be required in some deployment environments.

An example PASSporT header with an "x5c" element with three certificates (including the root) in its chain might look as follows:

```
  { "typ":"passport",
    "ppt":"div",
    "alg":"ES256",
    "x5c":
        ["MIICkTCCAjigAwIBAgIUb689vcv/kTP7N6J7Gz9YZU21WT4wCgYIKoZIzj0EAwIw
        SzELMAkGA1UEBhMCVVMxFjAUBgNVBAoMDUFjbWUgQ0EsIEluYy4xJDAiBgNVBAMM
        G0FjbWUgU0hBS0VOIEludGVybWVkaWF0ZSBDQTAeFw0yNDA3MDgxNDI4MjVaFw0y
        NDA3MDkxNDI4MjVaMFUxCzAJBgNVBAYTAlVTMR4wHAYDVQQKDBVBY21lIEVudGVy
        cHJpc2UsIEluYy4xJjAkBgNVBAMMHVNIQUtFTiBUTi1BdXRobi1MaXN0IEJ5IFZh
        bHVlMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEuxmGGgRklHe0GyGbgANc4182
        z3y6LdJ9Xp0r6xWspI/K3msUWD3ijxA5iYEKUBLofBMbwHiDS4CfMldTHUuMFqOB
        7zCB7DAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTbmpeh0wHlpxvtJlVbI6mD+idq
        cjAfBgNVHSMEGDAWgBTNsw0NkoZNWYL1bn2vwna5gwp0szAOBgNVHQ8BAf8EBAMC
        B4AwNAYIKwYBBQUHAQEEKDAmMCQGA1UdH4YdaHR0cHM6Ly9zdGlwYS5hY21lLWNh
        LmNvbS9jcmwwVgYIKwYBBQUHARoESjBIoRMwERYLMTcwMzU1NTIwMDACAgPoog0W
        CzE3MDM1NTUxMjM0oRMwERYLMTU3MTU1NTMwMDACAgfQog0WCzE1NzE1NTUyMzQ1
        MAoGCCqGSM49BAMCA0cAMEQCIFzV0EyHdMXStqzROJkL6CO06+6FuFYZGIod9iMw
        Yyr2AiAmEK1smeSAdoFYG5WTIGfjB13xAWn7EQH0SDkqOKKBwA==",
        "MIICKjCCAdGgAwIBAgIUPV/XdduqC44On5FKIjmcqwWO1JkwCgYIKoZIzj0EAwIw
        QzELMAkGA1UEBhMCVVMxFjAUBgNVBAoMDUFjbWUgQ0EsIEluYy4xHDAaBgNVBAMM
        E0FjbWUgU0hBS0VOIFJvb3QgQ0EwHhcNMjQwNzA4MTQyODI1WhcNMzQwNzA5MTQy
        ODI1WjBLMQswCQYDVQQGEwJVUzEWMBQGA1UECgwNQWNtZSBDQSwgSW5jLjEkMCIG
        A1UEAwwbQWNtZSBTSEFLRU4gSW50ZXJtZWRpYXRlIENBMFkwEwYHKoZIzj0CAQYI
        KoZIzj0DAQcDQgAE0wypYKOwsS8JU0Ahx4niuirUv0M9v01vUDHiSfFzWbeAlbK/
        hWlVYHADeFoRC7cIldDJ3iupafdxVgQggPp+/aOBmjCBlzAPBgNVHRMBAf8EBTAD
        AQH/MB0GA1UdDgQWBBTNsw0NkoZNWYL1bn2vwna5gwp0szAfBgNVHSMEGDAWgBRL
        Uq0usIR/TU27Y5vNN94V7xKnzTAOBgNVHQ8BAf8EBAMCAQYwNAYIKwYBBQUHAQEE
        KDAmMCQGA1UdH4YdaHR0cHM6Ly9zdGlwYS5hY21lLWNhLmNvbS9jcmwwCgYIKoZI
        zj0EAwIDRwAwRAIgUoAbid+kGFQWdQnLpJGwc4c4JoYohenmm3y2duOBN58CIEDm
        nWAQfT1HWvZt2M6q0nOopZLwrt/9LzkBJqomRgzr",
        "MIIB6zCCAZGgAwIBAgIUGEca/xMNdZbTZUP8DsxrnbR246AwCgYIKoZIzj0EAwIw
        QzELMAkGA1UEBhMCVVMxFjAUBgNVBAoMDUFjbWUgQ0EsIEluYy4xHDAaBgNVBAMM
        E0FjbWUgU0hBS0VOIFJvb3QgQ0EwHhcNMjIwNTA3MDQ1ODIyWhcNNDIwNTA3MDQ1
        ODIyWjBDMQswCQYDVQQGEwJVUzEWMBQGA1UECgwNQWNtZSBDQSwgSW5jLjEcMBoG
        A1UEAwwTQWNtZSBTSEFLRU4gUm9vdCBDQTBZMBMGByqGSM49AgEGCCqGSM49AwEH
        A0IABL7UD1CBpsNNq0EzDa90JUQV9etsUe8YOyOXpFB/9A8ahDj6HAJxuZJigSCG
        dG6npehdHMeDHzHsPHMLy22qH6OjYzBhMB0GA1UdDgQWBBRLUq0usIR/TU27Y5vN
        N94V7xKnzTAfBgNVHSMEGDAWgBRLUq0usIR/TU27Y5vNN94V7xKnzTAPBgNVHRMB
        Af8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAKBggqhkjOPQQDAgNIADBFAiEA+U9j
        0vQpHOx4nF+jytmr/bpotH001R09zZiywozSydwCIE6hI66JwnmqRKeJ9OeTNyM5
        asC7YWEm3bQqgukw/uEs"]
 }
```

A potential alternative approach would be that [RFC8224] already provides a way of pointing to a certificate in a MIME body associated with the SIP request. For out-of-band uses of STIR, however, having the certificate embedded in the PASSporT itself is a superior option. Implementations MAY include both "x5u" and "x5c" in the payload header for backward compatibility if desired, provided that the two share the same certification chain.

5. 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 [RFC8555] 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 [RFC9448]), 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.

[RFC9448] uses the ATC framework of [RFC9447] 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. This could potentially be used with the ACME STAR [RFC8739] mechanism as well.

6. IANA Considerations

This document contains no actions for the IANA.

7. 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.

8. Security Considerations

This document is entirely about security. For further information on certificate security and practices, see [RFC5280], in particular its Security Considerations. The Security Considerations of [RFC8555] are relevant to the use of ACME to acquire short-lived certificates.

9. Acknowledgments

Stephen Farrell, Jack Rickard, Simon Castle, Chris Wendt, Alec Feichnel, Eric Rescorla and Ning Zhang provided key input to this document.

10. References

10.1. Normative References

[ATIS-0300251]
ATIS Recommendation 0300251, "Codes for Identification of Service Providers for Information Exchange", 2007.

[DSS] National Institute of Standards and Technology, U.S. Department of Commerce | NIST FIPS PUB 186-4, "Digital Signature Standard, version 4", 2013.

[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>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[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>.

[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>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[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>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[RFC8739] Sheffer, Y., Lopez, D., Gonzalez de Dios, O., Pastor Perales, A., and T. Fossati, "Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated

Certificate Management Environment (ACME)", RFC 8739, DOI 10.17487/RFC8739, March 2020, <https://www.rfc-editor.org/info/rfc8739>.

[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>.

[RFC9447] Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "Automated Certificate Management Environment (ACME) Challenges Using an Authority Token", RFC 9447, DOI 10.17487/RFC9447, September 2023, <https://www.rfc-editor.org/info/rfc9447>.

[RFC9448] Wendt, C., Hancock, D., Barnes, M., and J. Peterson, "TNAuthList Profile of Automated Certificate Management Environment (ACME) Authority Token", RFC 9448, DOI 10.17487/RFC9448, September 2023, <https://www.rfc-editor.org/info/rfc9448>.

[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".

10.2. Informative References

[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>.

[RFC7375] Peterson, J., "Secure Telephone Identity Threat Model", RFC 7375, DOI 10.17487/RFC7375, October 2014, <https://www.rfc-editor.org/info/rfc7375>.

[X.520] ITU-T Recommendation X.520 (10/2012) | ISO/IEC 9594-6, "Information technology - Open Systems Interconnection - The Directory: Selected Attribute Types", 2012.

Author’s Address

Jon Peterson
TransUnion
Email: jon.peterson@transunion.com