ï»¿

Internet Engineering Task Force (IETF)
Request for Comments: 9060
Category: Standards Track
ISSN: 2070-1721

J. Peterson
Neustar

September 2021

Secure Telephone Identity Revisited (STIR) Certificate Delegation

Abstract

The Secure Telephone Identity Revisited (STIR) certificate profile provides a way to attest authority over telephone numbers and related identifiers for the purpose of preventing telephone number spoofing. This specification details how that authority can be delegated from a parent certificate to a subordinate certificate. This supports a number of use cases, including those where service providers grant credentials to enterprises or other customers capable of signing calls with STIR.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9060.

Table of Contents

1. Introduction

The STIR problem statement [RFC7340] reviews the difficulties facing the telephone network that are enabled by impersonation, including various forms of robocalling, voicemail hacking, and swatting [RFC7375]. One of the most important components of a system to prevent impersonation is the implementation of credentials that identify the parties who control telephone numbers. The STIR certificate specification [RFC8226] describes a credential system based on version 3 certificates [X.509] 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 SIP [RFC3261] requests.

[RFC8226] specifies an extension to X.509 that defines a Telephony Number (TN) Authorization List that may be included by certification authorities (CAs) 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 PASSporT to determine if the caller is authorized to use that calling number.

Initial deployment of [RFC8226] has focused on the use of Service Provider Codes (SPCs) to attest to the scope of authority of a certificate. Typically, these codes are internal telephone network identifiers such as the Operating Company Numbers (OCNs) assigned to carriers in the United States. However, these network identifiers are effectively unavailable to non-carrier entities, and this has raised questions about how such entities might best participate in STIR when needed. Additionally, a carrier may sometimes operate numbers that are formally assigned to another carrier. [RFC8226] gives an overview of a certificate enrollment model based on "delegation", whereby the holder of a certificate might allocate a subset of that certificate's authority to another party. This specification details how delegation of authority works for STIR certificates.

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.

This specification also uses the following terms:

delegation: The concept of STIR certificate delegation and its terms are defined in [RFC8226].

legitimate spoofing: The practice of selecting an alternative presentation number for a telephone caller legitimately.

3. Motivation

The most pressing need for delegation in STIR arises in a set of use cases where callers want to use a particular calling number, but for whatever reason, their outbound calls will not pass through the authentication service of the service provider that controls that numbering resource.

One example would be an enterprise that places outbound calls through a set of service providers; for each call, a provider is chosen based on a least-cost routing algorithm or similar local policy. The

enterprise was assigned a calling number by a particular service provider, but some calls originating from that number will go out through other service providers.

A user might also roam from their usual service provider to a different network or administrative domain for various reasons. Most "legitimate spoofing" examples are of this form, where a user wants to be able to use the main callback number for their business as a calling party number, even when the user is away from the business.

These sorts of use cases could be addressed if the carrier who controls the numbering resource were able to delegate a credential that could be used to sign calls regardless of which network or administrative domain handles the outbound routing for the call. In the absence of something like a delegation mechanism, outbound carriers may be forced to sign calls with credentials that do not cover the originating number in question. Unfortunately, that practice would be difficult to distinguish from malicious spoofing, and if it becomes widespread, it could erode trust in STIR overall.

4. Delegation of STIR Certificates

STIR delegate certificates are certificates containing a TNAuthList object that have been signed with the private key of a parent certificate that itself contains a TNAuthList object (either by value or by reference; see Section 4.1). The parent certificate needs to contain a basic constraints extension with the cA boolean set to "true" [RFC5280], indicating that the subject can sign certificates. Every STIR delegate certificate identifies its parent certificate with a standard Authority Key Identifier extension [RFC5280].

The authority bestowed on the holder of the delegate certificate by the parent certificate is recorded in the delegate certificate's TNAuthList. Because STIR certificates use the TNAuthList object rather than the Subject Name for indicating the scope of their authority, traditional name constraints [RFC5280] are not directly applicable to STIR. In a manner similar to the Resource Public Key Infrastructure (RPKI) [RFC6480] "encompassing" semantics, each delegate certificate MUST have a TNAuthList scope that is equal to or a subset of its parent certificate's scope: it must be "encompassed". For example, a parent certificate with a TNAuthList that attested authority for the numbering range +1-212-555-1000 through 1999 could issue a certificate to one delegate attesting authority for the range +1-212-555-1500 through 1599 and, to another delegate, a certificate for the individual number +1-212-555-1824.

Delegate certificates MAY also contain a basic constraints extension with the cA boolean set to "true", indicating that they can sign subordinate certificates for further delegates. As only end-entity certificates can actually sign PASSporTs, the holder of a STIR certificate with a "true" cA boolean may create a separate end-entity certificate with either an identical TNAuthList to its parent or a subset of the parent's authority, which would be used to sign PASSporTs.

4.1. Scope of Delegation

The TNAuthList of a STIR certificate may contain one or more SPCs, one or more telephone number ranges, or even a mix of SPCs and telephone number ranges. When delegating from a STIR certificate, a child certificate may inherit from its parent either or both of the above, and this specification explicitly permits SPC-only parent certificates to delegate individual telephone numbers or ranges to a child certificate, as this will be necessary in some operating environments. Depending on the sort of numbering resources that a delegate has been assigned, various syntaxes can be used to capture the delegated resource.

Some non-carrier entities may be assigned large and complex allocations of telephone numbers, which may be only partially contiguous or entirely disparate. Allocations may also change

frequently in minor or significant ways. These resources may be so complex, dynamic, or extensive that listing them in a certificate is prohibitively difficult. Section 10.1 of [RFC8226] describes one potential way to address this: including the TNAuthList (specified in [RFC8226]) in the certificate by reference rather than by value, where a URL in the certificate points to a secure, dynamically updated list of the telephone numbers in the scope of authority of a certificate. For entities that are carriers in all but name, another alternative is the allocation of an SPC; this yields much the same property, as the SPC is effectively a pointer to an external database that dynamically tracks the numbers associated with the SPC. Either of these approaches may make sense for a given deployment. Certification path construction as detailed below treats by-reference TNAuthLists in a certificate as if they had been included by value.

Other non-carrier entities may have straightforward telephone number assignments, such as enterprises receiving a set of a thousand blocks from a carrier that may be kept for years or decades. Particular freephone numbers may also have a long-term association with an enterprise and its brand. For these sorts of assignments, assigning an SPC may seem like overkill, and using the TN ranges of the TNAuthList (by value) is sufficient.

Whichever approach is taken to represent the delegated resource, there are fundamental trade-offs regarding when and where in the architecture a delegation is validated -- that is, when the delegated TNAuthList is checked and determined to be "encompassed" by the TNAuthList of its parent. This might be performed at the time the delegate certificate is issued, at the time that a verification service receives an inbound call, or potentially both. It is generally desirable to offload as much of this as possible to the certification process as verification occurs during call setup; thus, additional network dips could lead to perceptible delay, whereas certification happens outside of call processing as a largely administrative function. Ideally, if a delegate certificate can supply a by-value TN range, then a verification service could ascertain that an attested calling party number is within the scope of the provided certificate without requiring any additional transactions with a service. In practice, verification services may already incorporate network queries into their processing (for example, to dereference the "x5u" field of a PASSporT) that could piggyback any additional information needed by the verification service.

Note that the permission semantics of the TNAuthList [RFC8226] are additive: that is, the scope of a certificate is the superset of all of the SPCs and telephone number ranges enumerated in the TNAuthList. As SPCs themselves are effectively pointers to a set of telephone number ranges, and a telephone number may belong to more than one SPC, this may introduce some redundancy to the set of telephone numbers specified as the scope of a certificate. The presence of one or more SPCs and one or more sets of telephone number ranges are similarly treated additively, even if the telephone number ranges turn out to be redundant to the scope of an SPC.

5. Authentication Service Signing with Delegate Certificates

Authentication service behavior varies from [RFC8224] as follows, although the same checks are performed by the authentication service when comparing the calling party number attested in call signaling with the scope of the authority of the signing certificate. Authentication services SHOULD NOT use a delegate certificate without validating that its scope of authority is encompassed by that of its parent certificate, and if that certificate has its own parent, the entire certification path SHOULD be validated.

This delegation architecture does not require that a non-carrier entity act as its own authentication service. That function may be performed by any authentication service that holds the private key corresponding to the delegate certificate, including one run by an outbound service provider, a third party in an enterprise’s outbound

call path, or in the SIP User Agent itself.

Note that authentication services creating a PASSporT for a call signed with a delegate certificate MUST provide an "x5u" link corresponding to the entire certification path rather than just the delegate certificate used to sign the call, as described in Section 7.

6. Verification Service Behavior for Delegate Certificate Signatures

The responsibility of a verification service validating PASSporTs signed with delegate certificates, while largely following baseline specifications [RFC8224] and [RFC8225], requires some additional procedures. When the verification service dereferences the "x5u" parameter, it will acquire a certificate list rather than a single certificate. It MUST then validate all of the credentials in the list, identifying the parent certificate for each delegate through its Authority Key Identifier extension.

While relying parties ordinarily have significant latitude in certification path construction when validating a certification path, STIR assumes a more rigid hierarchical subordination model rather than one where relying parties may want to derive their own certification path to particular trust anchors. If the certificates acquired from the "x5u" element of a PASSporT do not lead to an anchor that the verification service trusts, it treats the validation no differently than it would when a non-delegated certificate was issued by an untrusted root; in SIP, it MAY return a 437 "Unsupported Credential" response if the call should be failed for lack of a valid Identity header.

7. Acquiring Multiple Certificates in STIR

PASSporT [RFC8225] uses the "x5u" element to convey the URL where verification services can acquire the certificate used to sign a PASSporT. This value is mirrored by the "info" parameter of the Identity header when a PASSporT is conveyed via SIP. Commonly, this is an HTTPS URI.

When a STIR delegate certificate is used to sign a PASSporT, the "x5u" element in the PASSporT will contain a URI indicating where a certificate list is available. While the baseline JSON Web Signature (JWS) also supports an "x5c" element specifically for certificate chains, in operational practice, certification paths are already being delivered in the STIR environment via the "x5u" element, so this specification RECOMMENDS that implementations continue to use "x5u". "x5c" is OPTIONAL for environments where it is known to be supported. That list will be a concatenation of certificates encoded with Privacy Enhanced Mail (PEM) of the type "application/pem-certificate-chain" defined in [RFC8555]. The certificate path [RFC5280] ordering MUST be ordered from the signer to the trust anchor. The list begins with the certificate used to sign the PASSporT, followed by its parent, and then any subsequent grandparents, great-grandparents, and so on. The key identifier in the Authority Key Identifier extension in the first certificate MUST appear in the Subject Key Identifier extension in the second certificate. The key identifier pairing MUST match in this way throughout the entire chain of certificates. Note that Automatic Certificate Management Environment (ACME) [RFC8555] requires the first element in a pem-certificate-chain to be an end-entity certificate.

8. Certification Authorities and Service Providers

Once a telephone service provider has received a CA certificate attesting to their numbering resources, they may delegate resources from it as they see fit. Note that the allocation to a service provider of a certificate with a basic constraints extension with the cA boolean set to "true" does not require that a service provider act as a certification authority itself; serving as a certification authority is a function requiring specialized expertise and

infrastructure. Certification authorities are, for example, responsible for maintaining certificate revocation lists and related functions as well as publishing certification practice statements. A third-party certification authority, including the same one that issued the service provider its parent certificate, could act as the CA that issues delegate certificates for the service provider if the necessary business relationships permit it. A service provider might in this case act as a Token Authority (see Section 8.1) granting its customers permissions to receive certificates from the CA.

Note that if the same CA that issued the parent certificate is also issuing a delegate certificate, it may be possible to shorten the certification path, which reduces the work required of verification services. The trade-off here is that if the CA simply issued a non-delegate certificate (whose parent is the CA's trust anchor) with the proper TNAuthList value, relying parties might not be able to ascertain which service provider owned those telephone numbers, information that might be used to make an authorization decision on the terminating side. However, some additional object in the certificate outside of the TNAuthList could preserve that information; this is a potential area for future work, and longer certification paths are the only mechanism currently defined.

All CAs must detail in their practices and policies a requirement to validate that the "encompassing" of a delegate certificate is done by its parent. Note that this requires that CAs have access to the necessary industry databases to ascertain whether, for example, a particular telephone number is encompassed by an SPC. Alternatively, a CA may acquire an Authority Token (see Section 8.1) that affirms that a delegation is in the proper scope. Exactly what operational practices this entails may vary in different national telephone administrations and are thus left to the Certificate Policy / Certification Practice Statement (CP/CPS) [RFC3647].

8.1. ACME and Delegation

STIR deployments commonly use ACME [RFC8555] for certificate acquisition, and it is anticipated that delegate certificates will also be acquired through an ACME interface. An entity can acquire a certificate from a particular CA by requesting an Authority Token [ACME-CHAL] from the parent with the desired TNAuthList [ACME-TOKEN] object. Note that if the client intends to do further subdelegation of its own, it should request a token with the "ca" Authority Token flag set.

The entity then presents that Authority Token to a CA to acquire a STIR delegate certificate. ACME returns an "application/pem-certificate-chain" object, and that object would be suitable for publication as an HTTPS resource for retrieval with the PASSporT "x5u" mechanism as discussed in Section 7. If the Certificate Signing Request (CSR) presented to the ACME server is for a certificate with the cA boolean set to "true", then the ACME server makes a policy decision to determine whether or not it is appropriate to issue that certificate to the requesting entity. That policy decision will be reflected by the "ca" flag in the Authority Token.

Service providers that want the capability to rapidly age out delegated certificates can rely on the ACME Short-Term, Automatically Renewed (STAR) [RFC8739] mechanism to automate the process of short-term certificate expiry.

8.2. Handling Multiple Certificates

In some deployments, non-carrier entities may receive telephone numbers from several different carriers. This could lead to enterprises needing to maintain a sort of STIR keyring, with different certificates delegated to them from different providers. These certificates are potentially issued by different CAs, which enterprises choose between when signing a call. This could be the case regardless of which syntax is used in the TNAuthList to represent the scope of the delegation (see Section 4.1). As noted in

Section 8, if the parent certs use the same CA, it may be possible to shorten the certification path.

For non-carrier entities handling a small number of certificates, this is probably not a significant burden. For cases where it becomes burdensome, a few potential approaches exist. A delegate certificate could be cross-certified with another delegate certificate via an Authority Information Access (AIA) field containing the URL of a Certificate Authority Issuer so that a signer would only need to sign with a single certificate to inherit the privileges of the other certificate(s) with which it has cross-certified. In very complex delegation cases, it might make more sense to establish a bridge CA that cross-certifies with all of the certificates held by the enterprise rather than requiring a mesh of cross-certification between a large number of certificates. Again, this bridge CA function would likely be performed by some existing CA in the STIR ecosystem. These procedures would, however, complicate the fairly straightforward certification path reconstruction approach described in Section 7 and would require further specification.

9. Alternative Solutions

At the time this specification was written, STIR was only starting to see deployment. In some future environment, the policies that govern CAs may not permit them to issue intermediate certificates with a TNAuthList object and a cA boolean set to "true" in the basic constraints certificate extension [RFC5280]. Similar problems in the web PKI space motivated the development of TLS subcerts [TLS-CRED], which substitutes a signed "delegated credential" token for a certificate for such environments. A comparable mechanism could be developed for the STIR space, which would allow STIR certificates to sign a data object that contains effectively the same data as the delegate certificate specified here, including a public key that could sign PASSporTs. The TLS subcerts system has further explored leveraging ACME to issue short-lived certificates for temporary delegation as a means of obviating the need for revocation. Specification of a mechanism similar to TLS subcerts for STIR is future work and will be undertaken only if the market requires it.

10. IANA Considerations

This document has no IANA actions.

11. Privacy Considerations

Any STIR certificate that identifies a narrow range of telephone numbers potentially exposes information about the entities that are placing calls. As such a telephone number range is a necessary superset of the calling party number that is openly signaled during call setup, the privacy risks associated with this mechanism are not substantially greater than baseline STIR. See [RFC8224] for guidance on the use of anonymization mechanisms in STIR.

12. Security Considerations

This document is entirely about security. As delegation can allow signing-in scenarios where unauthenticated "legitimate" spoofing would otherwise be used, the hope is that delegation will improve the overall security of the STIR ecosystem. For further information on certificate security and practices, see [RFC5280], particularly its security considerations. Also see the security considerations of [RFC8226] for general guidance on the implications of the use of certificates in STIR and [RFC7375] for the STIR threat model.

Much of the security of delegation depends on the implementation of the encompassing semantics described in Section 4. When delegating from an SPC-based TNAuthList to a set of telephone number ranges, understanding the encompassing semantics may require access to industry databases that track the numbering assets of service providers associated with a given SPC. In some operating environments, such databases might not exist. How encompassing is

policed is therefore a matter outside the scope of this document and specific to operational profiles of STIR.

The use of by-reference TNAuthLists as described in Section 4 means that the TNAuthList associated with a certificate can change over time; see the security considerations of [RFC3986] for more on the implications of this property. It is considered a useful feature here due to the potential dynamism of large lists of telephone numbers, but this dynamism means that a relying party might at one point accept that a particular telephone number is associated with a certificate but later reject it for the same certificate as the dynamic list changes. Also note that if the HTTPS service housing the by-reference telephone number list is improperly secured, that too can lead to vulnerabilities. Ultimately, the CA that issued a delegated certificate populates the URL in the AIA field and is responsible for making a secure selection. Service providers acting as CAs are directed to the cautionary words about running a CA in Section 8 regarding the obligations this entails for certificate revocation and so on.

13. References

13.1. Normative References

[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>.

[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>.

[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>.

[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>.

13.2. Informative References

[ACME-CHAL] Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "ACME Challenges Using an Authority Token", Work in Progress, Internet-Draft, draft-ietf-acme-authority-token-06, 12 July 2021, <https://datatracker.ietf.org/doc/html/draft-

ietf-acme-authority-token-06>.

[ACME-TOKEN]
Wendt, C., Hancock, D., Barnes, M., and J. Peterson, "TNAuthList profile of ACME Authority Token", Work in Progress, Internet-Draft, draft-ietf-acme-authority-token-tnauthlist-08, 27 March 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-acme-authority-token-tnauthlist-08>.

[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>.

[RFC3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <https://www.rfc-editor.org/info/rfc3647>.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

[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>.

[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>.

[TLS-CRED] Barnes, R., Iyengar, S., Sullivan, N., and E. Rescorla, "Delegated Credentials for TLS", Work in Progress, Internet-Draft, draft-ietf-tls-subcerts-10, 24 January 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-subcerts-10>.

[X.509] ITU-T, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, October 2016, <https://www.itu.int/rec/T-REC-X.509>.

Acknowledgments

We would like to thank Ines Robles, Richard Barnes, Chris Wendt, Dave Hancock, Russ Housley, Benjamin Kaduk, and Sean Turner for key input on this document.

Author's Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar