STIR Certificate Delegation
draft-peterson-stir-cert-delegation-00.txt

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, in cases where service providers grant credentials to enterprises or other customers capable of signing calls with STIR.

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 12, 2019.

Copyright Notice

Copyright (c) 2019 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
the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................................. 2
2. Terminology .................................................. 3
3. Delegation of STIR Certificates .............................. 3
   3.1. Authentication Services Signing with Delegate Certificates .......... 4
   3.2. Verification Service Behavior for Delegate Certificate Signatures .......... 4
4. Acquiring Certificate Chains in STIR .......................... 5
5. ACME and Delegation ........................................... 5
6. IANA Considerations .......................................... 6
7. Privacy Considerations ....................................... 6
8. Security Considerations ...................................... 6
9. Acknowledgments .............................................. 6
10. References .................................................. 6
   10.1. Normative References .................................... 6
   10.2. Informative References ................................... 7
Author’s Address .................................................. 9

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. 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 SIP [RFC3261] requests.

[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 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 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. Allocations at finer levels of granularity, to blocks of telephone numbers or even to individual numbers, are also desirable for enterprise use cases. [RFC8226] gave an overview of a certificate enrollment model based on "delegation," whereby the holder of certificate might allocate a subset of that certificates 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 RFC 2119 [RFC2119].

3. 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. The parent certificate needs to have its CA boolean set to "true", indicating that it can sign certificates. Every STIR delegate certificate identifies its parent certificate with a standard [RFC5280] Authority Key Identifier.

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 [RFC5280] name constraints are not directly applicable to STIR. In a manner similar to the 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 themselves be issued with the CA boolean set to "true" so that they can serve as parent certificates to further delegates; effectively, this delegate certificate is a cross-certificate, as its issuer is not the same as its subject. In the
STIR ecosystem, certification authority certificates may be used to sign PASSporTs; this removes the need for creating a redundant end-entity certificate with an identical TNAuthList to its parent, though if for operational or security reasons certificate holders wish to do so, they may.

Parent certificates may have a TNAuthList containing one or more SPCs, one or more telephone number ranges, or both. Delegations from a parent certificate that contains only SPCs to a delegate certificate containing a telephone number or number range are permitted. Ascertaining whether or not a given telephone number belongs to the service provider identified by an SPC requires access to industry numbering databases that are outside the scope of this specification; entities that are constructing a certificate path who have access to those resources can validate those delegations.

3.1. Authentication Services Signing with Delegate Certificates

Authentication service behavior for delegate certificates is little changed from baseline STIR behavior. The same checks are performed by the authentication service, 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 in turn has its own parent, the entire certificate path should be validated.

Note that authentication services creating a PASSporT for a call signed with a delegate certificate MUST provide an "x5u" link corresponding to the entire certificate chain, rather than just the delegate certificate used to sign the call, as described in Section 4.

3.2. Verification Service Behavior for Delegate Certificate Signatures

The responsibility of a verification service validating PASSporTs signed with delegate certificates, while largely following baseline [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 AKID object.

While ordinarily, relying parties have significant latitude in path construction when validating a certificate chain, STIR assumes a more rigid hierarchical subordination model, rather than one where relying parties may want to derive their own chains to particular trust
anchors. If the certificate chain acquired from the "x5u" element of a PASSporT does 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 untrust root; in SIP, it MAY return a 437 "Unsupported Credential" response if the call should be failed for lack of a valid Identity header.

4. Acquiring Certificate Chains 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. That list will be a concatenation of PEM encoded certificates of the type "application/pem-certificate-chain" defined in [I-D.ietf-acme-acme]. 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 ordering MUST conform to the AKID/SKID order chain encoded in the certs themselves. Note that ACME requires the first element in a pem-certificate-chain to be an end-entity certificate; STIR relaxes this requirement, as CA certificates are permitted to sign PASSporTs, so the first element in a pem-certificate-chain used for STIR MAY be a CA certificate.

5. ACME and Delegation

STIR deployments commonly use ACME [I-D.ietf-acme-acme] for certificate acquisition, and it is anticipated that delegate certificates as well will be acquired through an ACME interface. An entity that wishes to acquire a certificate from a particular CA will request an Authority Token [I-D.ietf-acme-authority-token] from the parent with the desired TNAuthList [I-D.ietf-acme-authority-token-tnauthlist] object. Note that if the client wishes 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 certificate authority to acquire a STIR delegate certificate. ACME returns an "application/pem-certificate-chain" object with suitable for publishing as an HTTPS resource for retrieval with the PASSporT "x5u" mechanism as discussed in Section 4. If the 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. In most ACME cases, that policy decision will be made based on the "ca" flag in the Authority Token.

6. IANA Considerations

This document contains no actions for the IANA.

7. Privacy Considerations

[TBD.]

8. Security Considerations

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

9. Acknowledgments

We would like to thank Richard Barnes, Chris Wendt, Dave Hancock, Russ Housley, and Sean Turner for key input to the discussions leading to this document.

10. References

10.1. Normative References

[I-D.ietf-acme-acme]

[I-D.ietf-acme-authority-token]
Peterson, J., Barnes, M., Hancock, D., and C. Wendt, "ACME Challenges Using an Authority Token", draft-ietf-acme-authority-token-01 (work in progress), October 2018.

[I-D.ietf-acme-authority-token-tnauthlist]


10.2. Informative References


Author’s Address

Jon Peterson
Neustar, Inc.

Email: jon.peterson@team.neustar