Network Working Group J. Peterson
Internet-Draft Neustar
Intended status: Standards Track S. Turner
Expires: January 6, 2016 IECA
July 5, 2015

Secure Telephone Identity Credentials: Certificates
draft-ietf-stir-certificates-02.txt

Abstract

In order to prove ownership of telephone numbers on the Internet, some kind of public infrastructure needs to exist that binds cryptographic keys to authority over telephone numbers. This document describes a certificate-based credential system for telephone numbers, which could be used as a part of a broader architecture for managing telephone numbers as identities in protocols like SIP.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

As is discussed in the STIR problem statement [I-D.ietf-stir-problem-statement], the primary enabler of robocalling, vishing, swatting and related attacks is the capability to impersonate a calling party number. The starkest examples of these attacks are cases where automated callees on the PSTN rely on the calling number as a security measure, for example to access a voicemail system. Robocallers use impersonation as a means of obscuring identity; while robocallers can, in the ordinary PSTN, block (that is, withhold) their caller identity, callees are less likely to pick up calls from blocked identities, and therefore appearing to calling from some number, any number, is preferable. Robocallers however prefer not to call from a number that can trace back to the robocaller, and therefore they impersonate numbers that are not assigned to them.

One of the most important components of a system to prevent impersonation is an authority responsible for issuing credentials to parties who control telephone numbers. With these credentials, parties can prove that they are in fact authorized to use telephony numbers, and thus distinguish themselves from impersonators unable to present credentials. This document describes a credential system for

telephone numbers based on X.509 version 3 certificates in accordance with [RFC5280]. While telephone numbers have long been a part of the X.509 standard, the certificates described in this document may contain telephone number blocks or ranges, and accordingly it uses an alternate syntax.

In the STIR in-band architecture, two basic types of entities need access to these credentials: authentication services, and verification services (or verifiers); see [I-D.ietf-stir-rfc4474bis]. An authentication service must be operated by an entity enrolled with the certification authority (see Section 3), whereas a verifier need only trust the root certificate of the authority, and have a means to acquire and validate certificates.

This document attempts to specify only the basic elements necessary for this architecture. Only through deployment experience will it be possible to decide directions for future work.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [RFC2119] and RFC 6919 [RFC6919].

3. Enrollment and Authorization

This document assumes a threefold model for certificate enrollment.

The first enrollment model is one where the certification authority acts in concert with national numbering authorities to issue credentials to those parties to whom numbers are assigned. In the United States, for example, telephone number blocks are assigned to Local Exchange Carriers (LECs) by the North American Numbering Plan Administrator (NANPA), who is in turn directed by the national regulator. LECs may also receive numbers in smaller allocations, through number pooling, or via an individual assignment through number portability. LECs assign numbers to customers, who may be private individuals or organizations - and organizations take responsibility for assigning numbers within their own enterprise.

The second enrollment model is one where a certification authority requires that an entity prove control by means of some sort of test. For example, an authority might send a text message to a telephone number containing a URL (which might be dereferenced by the recipient) as a means of verifying that a user has control of terminal corresponding to that number. Checks of this form are frequently used in commercial systems today to validate telephone

numbers provided by users. This is comparable to existing enrollment systems used by some certificate authorities for issuing S/MIME credentials for email by verifying that the party applying for a credential receives mail at the email address in question.

The third enrollment model is delegation: that is, the holder of a certificate (assigned by either of the two methods above) may delegate some or all of their authority to another party. In some cases, multiple levels of delegation could occur: a LEC, for example, might delegate authority to customer organization for a block of 100 numbers, and the organization might in turn delegate authority for a particular number to an individual employee. This is analogous to delegation of organizational identities in traditional hierarchical Public Key Infrastructures (PKIs) who use the name constraints extension [RFC5280]; the root CA delegates names in sales to the sales department CA, names in development to the development CA, etc. As lengthy certificate delegation chains are brittle, however, and can cause delays in the verification process, this document considers optimizations to reduce the complexity of verification.

[TBD] Future versions of this specification may address adding a level of assurance indication to certificates to differentiate those enrolled from proof-of-possession versus delegation.

[TBD] Future versions of this specification may also discuss methods of partial delegation, where certificate holders delegate only part of their authority. For example, individual assignees may want to delegate to a service authority for text messages associated with their telephone number, but not for other functions.

3.1. Certificate Scope and Structure

The subjects of telephone number certificates are the administrative entities to whom numbers are assigned or delegated. For example, a LEC might hold a certificate for a range of telephone numbers.

[TBD - what if the subject is considered a privacy leak?]

This specification places no limits on the number of telephone numbers that can be associated with any given certificate. Some service providers may be assigned millions of numbers, and may wish to have a single certificate that is capable of signing for any one of those numbers. Others may wish to compartmentalize authority over subsets of the numbers they control.

Moreover, service providers may wish to have multiple certificates with the same scope of authority. For example, a service provider with several regional gateway systems may want each system to be

capable of signing for each of their numbers, but not want to have each system share the same private key.

The set of telephone numbers for which a particular certificate is valid is expressed in the certificate through a certificate extension; the certificate's extensibility mechanism is defined in [RFC5280] but the telephone number authorization extension is defined in this document.

3.2. Provisioning Private Keying Material

In order for authentication services to sign calls via the procedures described in [I-D.ietf-stir-rfc4474bis], they must possess a private key corresponding to a certificate with authority over the calling number. This specification does not require that any particular entity sign requests, only that it be an entity with an appropriate private key; the authentication service role may be instantiated by any entity in a SIP network. For a certificate granting authority only over a particular number which has been issued to an end user, for example, an end user device might hold the private key and generate the signature. In the case of a service provider with authority over large blocks of numbers, an intermediary might hold the private key and sign calls.

The specification recommends distribution of private keys through PKCS#8 objects signed by a trusted entity, for example through the CMS package specified in [RFC5958].

4. Acquiring Credentials to Verify Signatures

This specification documents multiple ways that a verifier can gain access to the credentials needed to verify a request. As the validity of certificates does not depend on the circumstances of their acquisition, there is no need to standardize any single mechanism for this purpose. All entities that comply with [I-D.ietf-stir-rfc4474bis] necessarily support SIP, and consequently SIP itself can serve as a way to acquire certificates. This specific does allow delivery through alternate means as well.

The simplest way for a verifier to acquire the certificate needed to verify a signature is for the certificate be conveyed along with the signature itself. In SIP, for example, a certificate could be carried in a multipart MIME body [RFC2046], and the URI in the Identity-Info header could specify that body with a CID URI [RFC2392]. However, in many environments this is not feasible due to message size restrictions or lack of necessary support for multipart MIME.

Alternatively, the Identity-Info header of a SIP request may contain a URI that the verifier dereferences with a network call. Implementations of this specification are required to support the use of SIP for this function (via the SUBSCRIBE/NOTIFY mechanism), as well as HTTP, via the Enrollment over Secure Transport mechanisms described in RFC 7030 [RFC7030].

A verifier can however have access to a service that grants access to certificates for a particular telephone number. Note however that there may be multiple valid certificates that can sign a call setup request for a telephone number, and that as a consequence, there needs to be some discriminator that the signer uses to identify their credentials. The Identity-Info header itself can serve as such a discriminator.

4.1. Verifying Certificate Scope

The subjects of these certificates are the administrative entities to whom numbers are assigned or delegated. When a verifier is validating a caller's identity, local policy always determines the circumstances under which any particular subject may be trusted, but for the purpose of validating a caller's identity, this certificate extension establishes whether or not a signer is authorized to sign for a particular number.

The Telephony Number (TN) Authorization List certificate extension is identified by the following object identifier:

```
id-ce-TNAuthList OBJECT IDENTIFIER ::= { TBD }
```

The TN Authorization List certificate extension has the following syntax:

```
   TNAuthorizationList ::= SEQUENCE SIZE (1..MAX) OF TNAuthorization

   TNAuthorization ::= SEQUENCE SIZE (1..MAX) OF TNEntry


   TNEntry ::= CHOICE {

      spid  ServiceProviderIdentifierList,

      range TelephoneNumberRange,

      one   E164Number }


   ServiceProviderIdentifierList ::= SEQUENCE SIZE (1..3) OF

                                          OCTET STRING

     -- When all three are present: SPID, Alt SPID, and Last Alt SPID


   TelephoneNumberRange ::= SEQUENCE {

      start E164Number,

      count INTEGER }



   E164Number ::= IA5String (SIZE (1..15)) (FROM ("0123456789"))
```

[TBD- do we really need to do IA5String? The alternative would be UTF8String, e.g.: UTF8String (SIZE (1..15)) (FROM ("0123456789"))]

The TN Authorization List certificate extension indicates the authorized phone numbers for the call setup signer. It indicates one or more blocks of telephone number entries that have been authorized for use by the call setup signer. There are three ways to identify the block: 1) a Service Provider Identifier (SPID) can be used to indirectly name all of the telephone numbers associated with that service provider, 2) telephone numbers can be listed in a range, and 3) a single telephone number can be listed.

Note that because large-scale service providers may want to associate many numbers, possibly millions of numbers, with a particular certificate, optimizations are required for those cases to prevent certificate size from becoming unmanageable. In these cases, the TN

Authorization List may be given by reference rather than by value, through the presence of a separate certificate extension that permits verifiers to either securely download the list of numbers associated with a certificate, or to verify that a single number is under the authority of this certificate. This optimization will be detailed in future version of this specification.

4.2. Certificate Freshness and Revocation

The problem of certificate freshness gains a new wrinkle in the telephone number context, because verifiers must establish not only that a certificate remains valid, but also that the certificate's scope contains the telephone number that the verifier is validating. Dynamic changes to number assignments can occur due to number portability, for example. So even if a verifier has a valid cached certificate for a telephone number (or a range containing the number), the verifier must determine that the entity that signed is still a proper authority for that number.

To verify the status of the certificate, the verifier needs the certificate, which is included with the call, and then would need to either:

Rely on short-lived certificates and not check the certificate's status, or

Rely on status information from the authority

The tradeoff between short lived certificates and using status information is the former's burden is on the front end (i.e., enrollment) and the latter's burden is on the back end (i.e., verification). Both impact call setup time, but it is assumed that performing enrollment for each call is more of an impact that using status information. This document therefore recommends relying on status information.

4.2.1. Choosing a Verification Method

There are three common certificate verification mechanisms employed by CAs:

Certificate Revocation Lists (CRLs) [RFC5280]

Online Certificate Status Protocol (OCSP) [RFC6960], and

Server-based Certificate Validation Protocol (SCVP) [RFC5055].

When relying on status information, the verifier needs to obtain the status information - but before that can happen, the verifier needs to know where to locate it. Placing the location of the status information in the certificate makes the certificate larger, but it eases the client workload. The CRL Distribution Point certificate extension includes the location of the CRL and the Authority Information Access certificate extension includes the location of OCSP and/or SCVP servers; both of these extensions are defined in [RFC5280]. In all cases, the status information location is provided in the form of an URI.

CRLs are an obviously attractive solution because they are supported by every CA. CRLs have a reputation of being quite large (10s of MBytes), because CAs maintain and issue one monolithic CRL with all of their revoked certificates, but CRLs do support a variety of mechanisms to scope the size of the CRLs based on revocation reasons (e.g., key compromise vs CA compromise), user certificates only, and CA certificates only as well as just operationally deciding to keep the CRLs small. However, scoping the CRL introduces other issues (i.e., does the RP have all of the CRL partitions).

CAs in the STIR architecture will likely all create CRLs for audit purposes, but it NOT RECOMMENDED that they be relying upon for status information. Instead, one of the two "online" options is preferred. Between the two, OCSP is much more widely deployed and this document therefore recommends the use of OCSP in high-volume environments for validating the freshness of certificates, based on [RFC6960], incorporating some (but not all) of the optimizations of [RFC5019].

4.2.2. Using OCSP with STIR Certificates

Certificates compliant with this specification therefore SHOULD include a URL pointing to an OCSP service in the Authority Information Access (AIA) certificate extension, via the "id-ad-ocsp" accessMethod specified in [RFC5280]. Baseline OCSP however supports only three possible response values: good, revoked, or unknown. With some extension, OCSP would not indicate whether the certificate is authorized for a particular telephone number that the verifier is validating.

[TBD] What would happen in the unknown case? Can we profile OCSP usage so that unknown is never returned for our extension?

At a high level, there are two ways that a client might pose this authorization question:

> For this certificate, is the following number currently in its scope of validity?

What are all the telephone numbers associated with this certificate, or this certificate subject?

Only the former lends itself to piggybacking on the OCSP status mechanism; since the verifier is already asking an authority about the certificate's status, why not reuse that mechanism, instead of creating a new service that requires additional round trips? Like most PKIX-developed protocols, OCSP is extensible; OCSP supports request extensions (including sending multiple requests at once) and per-request extensions. It seems unlikely that the verifier will be requesting authorization checks on multiple telephone numbers in one request, so a per-request extension is what is needed.

[TBD] HVE OCSP requires SHA-1 be used as the hash algorithm, we're6960 obviously going to change this to be SHA-256.

The requirement to consult OCSP in real time results in a network round-trip time of day, which is something to consider because it will add to the call setup time. OCSP server implementations commonly pre-generate responses, and to speed up HTTPS connections, servers often provide OCSP responses for each certificate in their hierarchy. If possible, both of these OCSP concepts should be adopted for use with STIR.

4.2.2.1. OCSP Extension Specification

The extension mechanism for OCSP follows X.509 v3 certificate extensions, and thus requires an OID, a criticality flag, and ASN.1 syntax as defined by the OID. The criticality specified here is optional: per [RFC6960] Section 4.4, support for all OCSP extensions is optional. If the OCSP server does not understand the requested extension, it will still provide the baseline validation of the certificate itself. Moreover, in practical STIR deployments, the issuer of the certificate will set the accessLocation for the OCSP AIA extension to point to an OCSP service that supports this extension, so the risk of interoperability failure due to lack of support for this extension is minimal.

The OCSP TNQuery extension is included as one of the requestExtensions in requests. It may also appear in the responseExtensions. When an OCSP server includes a number in the responseExtensions, this informs the client that the certificate is still valid for the number that appears in the TNQuery extension field. If the TNQuery is absent from a response to a query containing a TNQuery in its requestExtensions, then the server is not able to validate that the number is still in the scope of authority of the certificate.

```
id-pkix-ocsp-stir-tn     OBJECT IDENTIFIER ::= { id-pkix-ocsp TBD }

TNQuery ::= E164Number
```

Note that HVE OCSP profile [RFC5019] prohibits the use of per-request extensions. As it is anticipated that STIR will use OCSP in a high-volume environment, many of the optimizations recommended by HVE are desirable for the STIR environment. This document therefore uses these extensions in a baseline OCSP environment with some HVE optimizations. [More TBD]

Ideally, once a certificate has been acquired by a verifier, some sort of asynchronous mechanism could notify and update the verifier if the scope of the certificate changes so that verifiers could implement a cache. While not all possible categories of verifiers could implement such behavior, some sort of event-driven notification of certificate status is another potential subject of future work. One potential direction is that a future SIP SUBSCRIBE/NOTIFY-based accessMethod for AIA might be defined (which would also be applicable to the method described in the following section) by some future specification.

4.2.3. Acquiring TN Lists By Reference

Acquiring a list of the telephone numbers associated with a certificate or its subject lends itself to an application-layer query/response interaction outside of OCSP, one which could be initiated through a separate URI included in the certificate. The AIA extension (see [RFC5280]) supports such a mechanism: it designates an OID to identify the accessMethod and an accessLocation, which would most likely be a URI. A verifier would then follow the URI to ascertain whether the list of TNs authorized for use by the caller.

HTTPS is the most obvious candidate for a protocol to be used for fetching the list of telephone number associated with a particular certificate. This document defines a new AIA accessMethod, called "id-ad-stir-tn", which uses the following AIA OID:

```
id-ad-stir-tn     OBJECT IDENTIFIER ::= { id-ad TBD }
```

When the "id-ad-stir-tn" accessMethod is used, the accessLocation MUST be an HTTPS URI. The document returned by dereferencing that URI will contain the complete TN Authorization List (see Section 4.1) for the certificate.

Delivering the entire list of telephone numbers associated with a particular certificate will divulge to STIR verifiers information about telephone numbers other than the one associated with the particular call that the verifier is checking. In some environments, where STIR verifiers handle a high volume of calls, maintaining an up-to-date and complete cache for the numbers associated with crucial certificate holders could give an important boost to performance.

5. Acknowledgments

Russ Housley, Brian Rosen, Cullen Jennings and Eric Rescorla provided key input to the discussions leading to this document.

6. IANA Considerations

This document makes use of object identifiers for the TN Certificate Extension defined in Section 4.1, TN-HVE OCSP extension in Section 4.2.2.1, and the TN by reference AIA access descriptor defined in Section 4.2.3. It therefore requests that the IANA make the following assignments:

- TN Certificate Extension in the SMI Security for PKIX Certificate Extension registry: http://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#smi-numbers-1.3.6.1.5.5.7.1

- TN-HVE OCSP extension in the SMI Security for PKIX Online Certificate Status Protocol (OCSP) registry: http://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#smi-numbers-1.3.6.1.5.5.7.48.1

- TNS by reference access descriptor in the SMI Security for PKIX Access Descriptor registry: http://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#smi-numbers-1.3.6.1.5.5.7.48

7. Security Considerations

This document is entirely about security. For further information on certificate security and practices, see RFC 3280 [RFC3280], in particular its Security Considerations.

8. Informative References

[I-D.ietf-stir-problem-statement]
Peterson, J., Schulzrinne, H., and H. Tschofenig, "Secure Telephone Identity Problem Statement and Requirements", draft-ietf-stir-problem-statement-05 (work in progress), May 2014.

[I-D.ietf-stir-rfc4474bis]
Peterson, J., Jennings, C., and E. Rescorla, "Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-stir-rfc4474bis-03 (work in progress), March 2015.

[I-D.peterson-sipping-retarget]
Peterson, J., "Retargeting and Security in SIP: A Framework and Requirements", draft-peterson-sipping-retarget-00 (work in progress), February 2005.

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2392] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2392, August 1998.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC5019] Deacon, A. and R. Hurst, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", RFC 5019, September 2007.

[RFC5055] Freeman, T., Housley, R., Malpani, A., Cooper, D., and W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", RFC 5055, December 2007.

[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, May 2008.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, August 2010.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words for Use in RFCs to Indicate Requirement Levels", RFC 6919, April 2013.

[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, June 2013.

[RFC7030] Pritikin, M., Yee, P., and D. Harkins, "Enrollment over Secure Transport", RFC 7030, October 2013.

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, July 2014.

[X.680] USC/Information Sciences Institute, "Information Technology - Abstract Syntax Notation One.", ITU-T X.680, ISO/IEC 8824-1:2002, 2002.

[X.681] USC/Information Sciences Institute, "Information Technology - Abstract Syntax Notation One: Information Object Specification", ITU-T X.681, ISO/IEC 8824-2:2002, 2002.

[X.682] USC/Information Sciences Institute, "Information Technology - Abstract Syntax Notation One: Constraint Specification", ITU-T X.682, ISO/IEC 8824-3:2002, 2002.

[X.683] USC/Information Sciences Institute, "Information Technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications", ITU-T X.683, ISO/IEC 8824-4:2002, 2002.

Appendix A. ASN.1 Module

This appendix provides the normative ASN.1 [X.680] definitions for the structures described in this specification using ASN.1, as defined in [X.680] through [X.683].

TBD

Authors' Addresses

Jon Peterson
Neustar, Inc.
1800 Sutter St Suite 570
Concord, CA 94520
US

Email: jon.peterson@neustar.biz

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Farifax, VA 22031
US

Email: turners@ieca.com