Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 20, 2018

J. Peterson
Neustar
S. Turner
sn3rd

November 16, 2017

Secure Telephone Identity Credentials: Certificates draft-ietf-stir-certificates-15

Abstract

In order to prevent the impersonation of telephone numbers on the Internet, some kind of credential system needs to exist that cryptographically asserts authority over telephone numbers. This document describes the use of certificates in establishing authority over telephone numbers, as a component of a broader architecture for managing telephone numbers as identities in protocols like SIP.

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 http://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 May 20, 2018.

Table of Contents

1. Introduction

The Secure Telephone Identity Revisited (STIR) problem statement [RFC7340] identifies the primary enabler of robocalling, vishing (voicemail hacking), swatting, and related attacks as the capability to impersonate a calling party number. The starkest examples of these attacks are cases where automated callees on the Public Switched Telephone Network (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; therefore, appearing to call 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 the implementation of credentials that identify the

parties who control telephone numbers. With these credentials, parties can assert that they are in fact authorized to use telephony numbers (TNs), and thus they distinguish themselves from impersonators unable to present such credentials. For that reason, the STIR threat model [RFC7375] stipulates that "The design of the credential system envisioned as a solution to these threats must, for example, limit the scope of the credentials issued to carriers or national authorities to those numbers that fall under their purview." This document describes credential systems for telephone numbers based on [X.509] version 3 certificates in accordance with [RFC5280]. While telephone numbers have long been part of the X.509 standard (X.509 supports arbitrary naming attributes to be included in a certificate; the telephoneNumber attribute was defined in the 1988 [X.520] specification), this document provides ways to determine authority more aligned with telephone network requirements, including extending X.509 with a Telephony Number Authorization List certificate extension, which binds certificates to asserted authority for particular telephone numbers or, potentially, telephone number blocks or ranges.

In the STIR in-band architecture specified in [RFC8224], two basic types of entities need access to these credentials: authentication services and verification services (or verifiers). An authentication service must be operated by an entity enrolled with the certification authority (CA) (see Section 5), whereas a verifier need only trust the trust anchor of the authority and also have a means to access and validate the public keys associated with these certificates. Although the guidance in this document is written with the STIR in-band architecture in mind, the credential system described in this document could be useful for other protocols that want to make use of certificates to assert authority over telephone numbers on the Internet.

This document specifies only the credential syntax and semantics necessary to support this architecture. It does not assume any particular CA or deployment environment. We anticipate that some deployment experience will be necessary to determine optimal operational models.

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. Authority for Telephone Numbers in Certificates

At a high level, this specification details two non-exclusive approaches that can be employed to determine authority over telephone numbers with certificates.

The first approach is to leverage the existing subject of the certificate to ascertain that the holder of the certificate is authorized to claim authority over a telephone number. The subject might be represented as a domain name in the subjectAltName, such as an "example.net" where that domain is known to relying parties as a carrier, or represented with other identifiers related to the operation of the telephone network, including Service Provider Codes (SPCs) such as Operating Company Numbers (OCNs) or Service Provider Identifiers (SPIDs) via the TN Authorization List specified in this document. A relying party could then employ an external data set or service that determines whether or not a specific telephone number is under the authority of the carrier identified as the subject of the certificate and use that to ascertain whether or not the carrier should have authority over a telephone number. Potentially, a certificate extension to convey the URI of such an information service trusted by the issuer of the certificate could be developed (though this specification does not propose one). Alternatively, some relying parties could form bilateral or multilateral trust relationships with peer carriers, trusting one another's assertions just as telephone carriers in the Signaling System 7 (SS7) network today rely on transitive trust when displaying the calling party telephone number received through SS7 signaling.

The second approach is to extend the syntax of certificates to include a new attribute, defined here as the TN Authorization List, which contains a list of telephone numbers defining the scope of authority of the certificate. Relying parties, if they trust the issuer of the certificate as a source of authoritative information on telephone numbers, could therefore use the TN Authorization List instead of the subject of the certificate to make a decision about whether or not the signer has authority over a particular telephone number. The TN Authorization List could be provided in one of two ways: as a literal value in the certificate or as a network service that allows relying parties to query in real time to determine that a telephone number is in the scope of a certificate. Using the TN Authorization List rather than the certificate subject makes sense when, for example, for privacy reasons the certificate owner would prefer not to be identified, or in cases where the holder of the certificate does not participate in the sort of traditional carrier infrastructure that the first approach assumes.

The first approach requires little change to existing Public Key Infrastructure (PKI) certificates; for the second approach, we must define an appropriate enrollment and authorization process. For the purposes of STIR, the over-the-wire format specified in [RFC8224] accommodates either of these approaches: the methods for canonicalizing, for signing, for identifying and accessing the certificate, and so on remain the same; it is only the verifier behavior and authorization decision that will change, depending on the approach to telephone number authority taken by the certificate. For that reason, the two approaches are not mutually exclusive, and in fact a certificate issued to a traditional telephone network service provider could contain a TN Authorization List or not, were it supported by the CA issuing the credential. Regardless of which approach is used, certificates that assert authority over telephone numbers are subject to the ordinary operational procedures that govern certificate use per [RFC5280]. This means that verification services must be mindful of the need to ensure that they trust the trust anchor that issued the certificate and that they have some means to determine the freshness of the certificate (see Section 10).

4. Certificate Usage with STIR

[RFC8224], Section 7.4 requires that all credential systems used by STIR explain how they address the requirements enumerated below. Certificates as described in this document address the STIR requirements as follows:

1. The URI [RFC3986] schemes permitted in the SIP Identity header "info" parameter, as well as any special procedures required to dereference the URIs: while normative text is given below in Section 7, this mechanism permits the HTTP [RFC7230], CID (Content-ID) [RFC2392], and SIP URI schemes to appear in the "info" parameter.

2. Procedures required to extract keying material from the resources designated by the URI: implementations perform no special procedures beyond dereferencing the "info" URI. See Section 7.

3. Procedures used by the verification service to determine the scope of the credential: this specification effectively proposes two methods, as outlined in Section 3: one where the subject (or, more properly, subjectAltName) of the certificate indicates the scope of authority through a domain name, and relying parties either trust the subject entirely or have some direct means of determining whether or not a number falls under a subject's authority; and another where an extension to the certificate as described in Section 9 identifies the scope of authority of the certificate.

4. The cryptographic algorithms required to validate the credentials: for this specification, that means the signature algorithms used to sign certificates. This specification REQUIRES that implementations support both the Elliptic Curve Digital Signature Algorithm (ECDSA) with the P-256 curve (see [DSS]) and RSA PKCS #1 v1.5 ("PKCS" stands for "Public-Key Cryptography Standards") (see [RFC8017], Section 8.2) for certificate signatures. Implementers are advised that RS256 is mandated only as a transitional mechanism, due to its widespread use in existing PKIs, but we anticipate that this mechanism will eventually be deprecated.

5. Finally, note that all certificates compliant with this specification:

   * MUST provide cryptographic keying material sufficient to generate the ECDSA using P-256 and SHA-256 signatures necessary to support the ES256 hashed signatures required by PASSporT [RFC8225], which in turn follows the JSON Web Token (JWT) [RFC7519].

   * MUST support both ECDSA with P-256 and RSA PKCS #1 v1.5 for certificate signature verification.

This document also includes additional certificate-related requirements:

- See Section 5.1 for requirements related to the JWT Claim Constraints certificate extension.

- See Section 7 for requirements related to relying parties acquiring credentials.

- See Sections 10 and 10.1 for requirements related to certificate freshness and the Authority Information Access (AIA) certificate extension.

5. Enrollment and Authorization Using the TN Authorization List

This document covers three models for enrollment when using the TN Authorization List extension.

The first enrollment model is one where the CA 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 Administration (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. This model requires top-down adoption of the model from regulators through to carriers. Assignees of E.164 numbering resources participating in this enrollment model should take appropriate steps to establish trust anchors.

The second enrollment model is a bottom-up approach where a CA requires that an entity prove control by means of some sort of test that, as with certification authorities for web PKI, might either be (1) automated or (2) a manual administrative process. As an example of an automated process, 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 a 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) might 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 a customer organization for a block of 100 numbers used by an IP PBX, 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 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.

Future work might explore 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.

5.1. Constraints on Signing PASSporTs

The public key in the certificate is used to validate the signature on a JWT [RFC7519] that conforms to the conventions specified in PASSporT [RFC8225]. This specification supports constraints on the JWT claims, thereby allowing the CA to grant different permissions to certificate holders -- for example, those enrolled from proof-of-possession versus delegation. A Certificate Policy (CP) and a Certification Practice Statement (CPS) [RFC3647] are produced as part of the normal PKI bootstrapping process (i.e., the CP is written first, and then the CA says how it conforms to the CP in the CPS). A CA that wishes to place constraints on the JWT claims MUST include the JWT Claim Constraints certificate extension in issued certificates. See Section 8 for information about the certificate extension.

5.2. Certificate Extension Scope and Structure

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 can be applied to 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 TN Authorization List extension is specified in this document.

The subjects of certificates containing the TN Authorization List extension are typically the administrative entities to whom numbers are assigned or delegated. For example, a LEC might hold a certificate for a range of telephone numbers. In some cases, the organization or individual issued such a certificate may not want to associate themselves with a certificate; for example, a private individual with a certificate for a single telephone number might not want to distribute that certificate publicly if every verifier immediately knew their name. The certification authorities issuing certificates with the TN Authorization List extensions may, in accordance with their policies, obscure the identity of the subject,

though mechanisms for doing so are outside the scope of this document.

6. Provisioning Private Keying Material

In order for authentication services to sign calls via the procedures described in [RFC8224], they must hold a private key corresponding to a certificate with authority over the calling number. [RFC8224] does not require that any particular entity in a SIP deployment architecture 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 that 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 Cryptographic Message Syntax (CMS) package specified in [RFC5958].

7. 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 method of their acquisition, there is no need to standardize any single mechanism for this purpose. All entities that comply with [RFC8224] necessarily support SIP, and consequently SIP itself can serve as a way to deliver certificates. [RFC8224] provides an "info" parameter of the Identity header; this parameter contains a URI for the credential used to generate the Identity header. [RFC8224] also requires that documents that define credential systems list the URI schemes that may be present in the "info" parameter. For implementations compliant with this specification, three URI schemes are REQUIRED: the CID URI, the SIP URI, and the HTTP URI.

The simplest way for a verifier to acquire the certificate needed to verify a signature is for the certificate to be conveyed in a SIP request 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 header "info" parameter 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.

The Identity header "info" parameter in a SIP request may contain a URI that the verifier dereferences. Implementations of this specification are REQUIRED to support the use of SIP for this function (via the SUBSCRIBE/NOTIFY mechanism) as well as HTTP and HTTPS.

Note well that as an optimization, a verifier may have access to a service, a cache, or other local store that grants access to certificates for a particular telephone number. However, there may be multiple valid certificates that can sign a call setup request for a telephone number, and as a consequence, there needs to be some discriminator that the signer uses to identify their credentials. The Identity header "info" parameter itself can serve as such a discriminator, provided implementations use that parameter as a key when accessing certificates from caches or other sources.

8. JWT Claim Constraints Syntax

Certificate subjects are limited to specific values for PASSporT claims with the JWT Claim Constraints certificate extension; issuers permit all claims by omitting the JWT Claim Constraints certificate extension from the certificate's extension field [RFC5280]. The extension is non-critical, applicable only to end-entity certificates, and defined with ASN.1 [X.680] [X.681] [X.682] [X.683] later in this section. The syntax of the claims is given in PASSporT; specifying new claims follows the procedures in [RFC8225], Section 8.3.

This certificate extension is optional, but if present, it constrains the claims that authentication services may include in the PASSporT objects they sign. Constraints are applied by issuers and enforced by verifiers when validating PASSporT claims as follows:

1. mustInclude indicates claims that MUST appear in the PASSporT in addition to iat, orig, and dest. The baseline claims of PASSporT ("iat", "orig", and "dest") are considered to be permitted by default and SHOULD NOT be included. If mustInclude is absent, iat, orig, and dest MUST appear in the PASSporT.

2. permittedValues indicates that if the claim name is present, the claim MUST contain one of the listed values.

Consider two examples with a PASSporT claim called "confidence" with values "low", "medium", and "high":

- If a CA issues to an authentication service a certificate that contains the mustInclude JWTClaimName "confidence", then an authentication service MUST include the "confidence" claim in all

PASSporTs it generates; a verification service will treat as invalid any PASSporT it receives with a PASSporT claim that does not include the "confidence" claim.

o If a CA issues to an authentication service a certificate that contains the permittedValues JWTClaimName "confidence" and a permitted "high" value, then an authentication service will treat as invalid any PASSporT it receives with a PASSporT claim that does not include the "confidence" claim with a "high" value.

The JWT Claim Constraints certificate extension is identified by the following object identifier (OID), which is defined under the id-pe OID arc defined in [RFC5280] and managed by IANA (see Section 11):

```
id-pe-JWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe 27 }
```

The JWT Claim Constraints certificate extension has the following syntax:

```
JWTClaimConstraints ::= SEQUENCE {
  mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT
    -- in addition to iat, orig, and dest.  If absent, iat, orig,
    -- and dest MUST appear in the PASSporT.
  permittedValues [1] JWTClaimPermittedValuesList OPTIONAL }
    -- If the claim name is present, the claim MUST contain one of
    -- the listed values.
( WITH COMPONENTS { ..., mustInclude PRESENT } |
  WITH COMPONENTS { ..., permittedValues PRESENT } )

JWTClaimPermittedValuesList ::= SEQUENCE SIZE (1..MAX) OF
                                  JWTClaimPermittedValues

JWTClaimPermittedValues ::= SEQUENCE {
  claim  JWTClaimName,
  permitted  SEQUENCE SIZE (1..MAX) OF UTF8String }

JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

JWTClaimName ::= IA5String
```

9. TN Authorization List Syntax

The subjects of certificates containing the TN Authorization List extension 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 the purpose of the

TN Authorization List extension in particular is to allow a verifier to ascertain when the CA has designated that the subject has authority over a particular telephone number or number range. The non-critical TN Authorization List certificate extension is included in the certificate's extension field [RFC5280]. The extension is defined with ASN.1 [X.680] [X.681] [X.682] [X.683]. The syntax and semantics of the extension are as follows.

The subjects of certificates containing the TN Authorization List extension are the administrative entities to whom numbers are assigned or delegated. In an end-entity certificate, the TN Authorization List indicates the TNs that it has authorized. In a CA certificate, the TN Authorization List limits the set of TNs for certification paths that include this certificate.

The TN Authorization List certificate extension is identified by the following object identifier (OID), which is defined under the id-pe OID arc defined in [RFC5280] and managed by IANA (see Section 11):

```
  id-pe-TNAuthList OBJECT IDENTIFIER ::= { id-pe 26 }
```

The TN Authorization List certificate extension has the following syntax:

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

 TNEntry ::= CHOICE {
   spc   [0] ServiceProviderCode,
   range [1] TelephoneNumberRange,
   one   [2] TelephoneNumber
   }

 ServiceProviderCode ::= IA5String

 -- SPCs may be OCNs, various SPIDs, or other SP identifiers
 -- from the telephone network.

 TelephoneNumberRange ::= SEQUENCE {
   start TelephoneNumber,
   count INTEGER (2..MAX),
   ...
   }

 TelephoneNumber ::= IA5String (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. SPCs as described in this document are a generic term for the identifiers used to designate service providers in telephone networks today. In North American context, these would include OCNs as specified in [ATIS-0300251], related SPIDs, or other similar identifiers for service providers. SPCs can be used to indirectly name all of the telephone numbers associated with that identifier for a service provider.

2. Telephone numbers can be listed in a range (in the TelephoneNumberRange format), which consists of a starting telephone number and then an integer count of numbers within the range, where the valid boundaries of ranges may vary according to national policies. The count field is only applicable to start fields' whose values do not include "*" or "#" (i.e., a TelephoneNumber that does not include "*" or "#"). count never overflows a TelephoneNumber digit boundary (i.e., a TelephoneNumberRange with TelephoneNumber=10 with a count=91 will address numbers 10-99).

3. A single telephone number can be listed (as a TelephoneNumber).

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 the 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 (1) securely download the list of numbers associated with a certificate or (2) verify that a single number is under the authority of this certificate. For more on this optimization, see Section 10.1.

10. Certificate Freshness and Revocation

Regardless of which of the approaches in Section 3 is followed for using certificates, a certificate verification mechanism is required. However, the traditional problem of certificate freshness gains a new wrinkle when using the TN Authorization List extension with telephone numbers or number ranges (as opposed to SPCs), 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 created the PASSporT, which includes a digital signature, is still a proper authority for that number.

To verify the status of such a certificate, the verifier needs to acquire the certificate if necessary (via the methods described in Section 7) and then would need to either:

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

b. Rely on status information from the authority (e.g., the Online Certificate Status Protocol (OCSP)).

The trade-off between short-lived certificates and using status information is that 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 some approaches to generating a short-lived certificate, like requiring one for each call, would incur a greater operational cost than acquiring status information. This document makes no particular recommendation for a means of determining certificate freshness for STIR, as this requires further study and implementation experience. Acquiring online status information for certificates has the potential to disclose private information [RFC7258] if proper precautions are not taken. Future specifications that define certificate freshness mechanisms for STIR MUST note any such risks and provide countermeasures where possible.

10.1. Acquiring the TN List by Reference

One alternative to checking certificate status for a particular telephone number is simply acquiring the TN Authorization List by reference, that is, through dereferencing a URL in the certificate, rather than including the value of the TN Authorization List in the certificate itself.

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 certificate status, one that 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 TNs in the list are authorized for use by the caller. As with the certificate extension defined in Section 9, a URI dereferenced from an end entity certificate will indicate the TNs which the caller has been authorized. Verifiers MUST support the AIA extension and the

dereferenced URI from a CA certificate limits the the set of TNs for certification paths that include this certificate.

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

```
id-ad-stirTNList  OBJECT IDENTIFIER ::= { id-ad 14 }
```

When the "id-ad-stirTNList" accessMethod is used, the accessLocation MUST be an HTTPS URI. Dereferencing the URI will return the complete DER encoded TN Authorization List (see Section 9) for the certificate with a Content-Type of application/tnauthlist (see Section 11.2).

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.

11. IANA Considerations

11.1. ASN.1 Registrations

This document makes use of object identifiers for the TN certificate extension defined in Section 9, the "TN List by reference" AIA access descriptor defined in Section 10.1, and the ASN.1 module identifier defined in Appendix A. Therefore, per this document, IANA has made the following assignments, as shown on <https://www.iana.org/assignments/smi-numbers>:

- TN Authorization List certificate extension in the "SMI Security for PKIX Certificate Extension" (1.3.6.1.5.5.7.1) registry:

  26 id-pe-TNAuthList

- JWT Claim Constraints certificate extension in the "SMI Security for PKIX Certificate Extension" (1.3.6.1.5.5.7.1) registry:

  27 id-pe-JWTClaimConstraints

- TN List by reference access descriptor in the "SMI Security for PKIX Access Descriptor" (1.3.6.1.5.5.7.48) registry:

  14 id-ad-stirTNList

- The TN ASN.1 module in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry:

  89 id-mod-tn-module

11.2. Media Type Registrations

```
Type name: application
 Subtype name: tnauthlist
 Required parameters: None.
 Optional parameters: None.
 Encoding considerations: Binary.
 Security considerations:  See Section 12 of this specification.
 Interoperability considerations:
    The TN Authorization List inside this media type MUST be
    DER-encoded TNAuthorizationList.
 Published specification: This specification.
 Applications that use this media type:
 Additional information:
    Magic number(s): None
    File extension(s): None
    Macintosh File Type Code(s): None
 Person & email address to contact for further information:
    Jon Peterson <jon.peterson@team.neustar>
 Intended usage: COMMON
 Restrictions on usage: none
 Author: Sean Turner <sean@sn3rd.com>
 Change controller: The IESG <iesg@ietf.org>
```

12. Security Considerations

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

If a certification authority issues a certificate attesting authority over many telephone numbers, the TNAuthList element can divulge to relying parties extraneous telephone numbers associated with the certificate which have no bearing on any given call in progress. The potential privacy risk can be exacerbated by the use of AIA, as described in Section 10.1, to link many thousand of numbers to a single certificate. Even an SPC in a certificate can be used to link a certificate to a particular carrier and, with access to industry databases, potentially the set of numbers associated with that SPC. While these practices may not cause concern in some environments, in other scenarios alternative approaches could minimize the data revealed to relying parties. For example, a service provider with authority over a large block of numbers could generate short-lived

certificates for individual TNs that are not so easily linked to the service provider or any other numbers that the service provider controls. Optimizations to facilitate acquiring short-lived certificates are a potential area of future work for STIR.

13. References

13.1. 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, "Digital Signature Standard (DSS)", NIST FIPS PUB 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>.

[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>.

[RFC2392] Levinson, E., "Content-ID and Message-ID Uniform Resource Locators", RFC 2392, DOI 10.17487/RFC2392, August 1998, <https://www.rfc-editor.org/info/rfc2392>.

[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>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <https://www.rfc-editor.org/info/rfc5958>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[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, November 2017, <https://www.rfc-editor.org/info/rfc8224>.

[RFC8225] Wendt, C. and J. Peterson, "PASSporT: Personal Assertion Token", RFC 8225, DOI 10.17487/RFC8225, November 2017, <https://www.rfc-editor.org/info/rfc8225>.

[X.509] International Telecommunication Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO/IEC 9594-8, October 2016, <https://www.itu.int/rec/T-REC-X.509>.

[X.680] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1, August 2015, <https://www.itu.int/rec/T-REC-X.680>.

[X.681] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Information object specification", ITU-T Recommendation X.681, ISO/IEC 8824-2, August 2015, <https://www.itu.int/rec/T-REC-X.681>.

[X.682] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Constraint specification", ITU-T Recommendation X.682, ISO/IEC 8824-3, August 2015, <https://www.itu.int/rec/T-REC-X.682>.

[X.683] International Telecommunication Union, "Information Technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", ITU-T Recommendation X.683, ISO/IEC 8824-4, August 2015, <https://www.itu.int/rec/T-REC-X.683>.

13.2. Informative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[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>.

[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] International Telecommunication Union, "Information technology - Open Systems Interconnection - The Directory: Selected attribute types", ITU-T Recommendation X.520, ISO/IEC 9594-6, October 2016, <https://www.itu.int/rec/T-REC-X.520>.

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], [X.681], [X.682], and [X.683].

The modules defined in this document are compatible with the most current ASN.1 specifications published in 2015 (see [X.680], [X.681], [X.682], and [X.683]). None of the newly defined tokens in the 2008 ASN.1 (DATE, DATE-TIME, DURATION, NOT-A-NUMBER, OID-IRI, RELATIVE-OID-IRI, TIME, TIME-OF-DAY) are currently used in any of the ASN.1 specifications referred to here.

This ASN.1 module imports ASN.1 from [RFC5912].

```
TN-Module-2016
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-tn-module(89) }

DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

id-ad, id-pe
FROM PKIX1Explicit-2009  -- From [RFC5912]
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

EXTENSION
FROM PKIX-CommonTypes-2009  -- From [RFC5912]
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0) id-mod-pkixCommon-02(57) }

;

--
-- JWT Claim Constraints Certificate Extension
--

ext-jwtClaimConstraints EXTENSION  ::= {
  SYNTAX JWTClaimConstraints IDENTIFIED BY id-pe-JWTClaimConstraints
  }

id-pe-JWTClaimConstraints OBJECT IDENTIFIER ::= { id-pe 27 }

JWTClaimConstraints ::= SEQUENCE {
  mustInclude [0] JWTClaimNames OPTIONAL,
    -- The listed claim names MUST appear in the PASSporT
```

```
      -- in addition to iat, orig, and dest.  If absent, iat, orig,
      -- and dest MUST appear in the PASSporT.
    permittedValues [1] JWTClaimPermittedValuesList OPTIONAL }
      -- If the claim name is present, the claim MUST contain one of
      -- the listed values.
  ( WITH COMPONENTS { ..., mustInclude PRESENT } |
    WITH COMPONENTS { ..., permittedValues PRESENT } )

  JWTClaimPermittedValuesList ::= SEQUENCE SIZE (1..MAX) Of
                                  JWTClaimPermittedValues

  JWTClaimPermittedValues ::= SEQUENCE {
    claim  JWTClaimName,
    permitted  SEQUENCE SIZE (1..MAX) OF UTF8String }

  JWTClaimNames ::= SEQUENCE SIZE (1..MAX) OF JWTClaimName

  JWTClaimName ::= IA5String

  --
  -- Telephony Number Authorization List Certificate Extension
  --

  ext-tnAuthList  EXTENSION  ::= {
    SYNTAX TNAuthorizationList IDENTIFIED BY id-pe-TNAuthList
    }

  id-pe-TNAuthList OBJECT IDENTIFIER ::= { id-pe 26 }

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

  TNEntry ::= CHOICE {
    spc    [0] ServiceProviderCode,
    range  [1] TelephoneNumberRange,
    one    [2] TelephoneNumber
    }

  ServiceProviderCode ::= IA5String

  -- SPCs may be OCNs, various SPIDs, or other SP identifiers
  -- from the telephone network.

  TelephoneNumberRange ::= SEQUENCE {
    start TelephoneNumber,
    count INTEGER (2..MAX),
    ...
    }
```

```
    TelephoneNumber ::= IA5String (SIZE (1..15)) (FROM ("0123456789#*"))

    -- TN Access Descriptor

    id-ad-stirTNList OBJECT IDENTIFIER ::= { id-ad 14 }

    END
```

Acknowledgments

Anders Kristensen, Russ Housley, Brian Rosen, Cullen Jennings, Dave Crocker, Tony Rutkowski, John Braunberger, Eric Rescorla, and Martin Thomson provided key input to the discussions leading to this document. Russ Housley provided some direct assistance and text surrounding the ASN.1 module.

Authors' Addresses

Jon Peterson
Neustar, Inc.

Email: jon.peterson@neustar.biz

Sean Turner
sn3rd

Email: sean@sn3rd.com