STIR E. Burger
Internet-Draft Georgetown University
Intended status: Standards Track March 5, 2018
Expires: September 6, 2018

Registry for Country-Specific Secure Telephone Identity (STIR) Root Certificates
draft-burger-stir-iana-cert-00

Abstract

This document defines an IANA registry that maps country codes to secure telephone identity (STIR) root certificates authorized to create signing certificates for telephone numbers under the authority of a given country. Some countries allow carriers to block unsolicited, automatically generated nuisance calls commonly known as 'robocalls.' The use of signed STIR tokens in the Session Initiation Protocol (SIP) may be useful in such scenarios to provide positive attestations as to call origin. Legacy telephone numbering resources are administrated by national policy. Unlike the market-driven use case of Web commerce, some nations may restrict the list of STIR root certificate authorities acceptable for issuing signing certificates for STIR tokens that provide attestations for their local legacy telephone numbering resources. The registry described in this document enables call recipients in a first country to validate that signaling it receives from a caller with a telephone number claiming to be in a second country conforms to the second country's policy of (1) having a limited list of STIR root certificate authorities (or not) and (2) the certificate that produced the signature over the signaling is signed by one of those authorized STIR root certificate authorities.

1. Introduction

One problem that plagues some communications applications is where the caller deliberately misrepresents their identity with the intent to defraud, cause harm, or wrongfully obtain anything of value. The IETF Secure Telephone Identity Revisited (STIR) work group has developed a series of RFCs specifying the mechanisms for cryptographically signing the asserted identity and other elements in Session Initiation Protocol (SIP) [RFC3261] messages. One kind of identity used in SIP is a telephone number [E.164]. A telephone number is a string of digits, where the first one to three digits indicate a country code. The International Telecommunications Union - Telecommunications Sector (ITU-T) defines country codes and delegates the authority for numbers under a country code to the respective national communications authority for that country, as listed in E.164 Annex D [E.164D].

Section 7 of Authenticated Identity Management in the Session Initiation Protocol [RFC8224] describes the process for signing identity tokens. Correspondingly, the STIR Certificates document [RFC8226] describes the format of the signing certificate. The protocol and formats are independent of and can have uses beyond that of signing originating telephone numbers. As well, given that for the most part governments are responsible for managing the numbering resources within their country code, governmental policy may impact who is authorized to issue signing certificates and what constitutes a valid signing chain. As such, the base STIR documents defer certificate and validation policy to other documents. This document describes a registry for finding the appropriate STIR root certificate authority for a given country code for signed telephone numbers. This document neither implies nor endorses any policies for

non-E.164 number identity assertions, such as arbitrary SIP URI's. Moreover, while this document describes the STIR root certificate registry for various nation's STIR root certificates, it does not mandate any particular policy regime.

Recalling the STIR problem statement [RFC7340], the goal is to provide authenticated identity for the caller. When a SIP endpoint receives a message with a signed STIR token, that endpoint needs to know whether the signing certificate is, in fact, allowed to make assertions for that identity. It does us no good for a caller with ill intent to have a signed assertion that has a valid certificate chain to an unauthorized root. Likewise, it does us no good to use self-signed certificates to sign a SIP message, as even with some limited verification, if there is the slightest chance of an entity with nefarious intent to succeed in either spoofing or taking over the identify of a caller, experience has shown they will do so.

As mentioned above, telephone numbers are assigned by the ITU-T to national communications authorities responsible for the number space below the numeric country code. A national regulator can inform service providers under its authority which root certificate authorities are authoritative for numbers under its control. This is straightforward within a country. However, this does not work for the global, interconnected communications network. When someone in a first country calls someone in a second country, how is the service provider or end user in the second country to know who is authoritative for signing certificates in the first country?

To solve this problem, this document establishes an IANA registry of STIR root certificate authorities, indexed by country. This document also establishes an IANA registry of numeric country codes to ISO 3166-1 [ISO.3166-1.2013] alpha-2 country codes.

2. Data Model

2.1. Country Code Registry

The ITU-T publishes a list of assigned numeric country codes in E.164 Annex D [E.164D]. The International Standards Organization (ISO) publishes a list of two-character country codes in ISO 3166-1 [ISO.3166-1.2013]. The Country Code Registry maps the telephone country codes to two-letter country codes. From here on, this document refers to the former as "numeric country codes" and the latter as "ISO country codes".

Applications are expected to do a longest-match search to find the ISO country code corresponding to a numeric country code. This enables overlapping numeric country codes such as for +1 and +7. Let

us say an enclosing numeric country code, such as +7 for the Russian Federation, will specify the certificates of an enclosed numeric country code, such as +76 for Kazakhstan. It also enables overlapping countries to provide their own, distinct set of roots for the enclosed numeric country code or to specify they are not specifying any STIR root certificates.

2.2. STIR Root Certificate Registry

This registry maps ISO country codes to STIR root certificates. There can be one or more STIR root certificates per ISO country code.

2.3. Operation

If a country is participating, it ensures it has the appropriate mapping from numeric country code to ISO country code in the Country Code Registry. Then, if the country does have STIR root certificate(s) to list, it places them in the STIR Root Certificate Registry. If the country wants to indicate that it is not specifying STIR root certificates, it creates an entry in the Country Code Registry but has no entries in the STIR Root Certificate Registry.

Besides directly indicating non-participation, this model enables handling of overlapping country codes.

Take the case of an overlapping numeric country code where the enclosed numbering country uses the same roots as the enclosing numbering country. The enclosed numbering country refrains from making an entry in the Country Code Registry. For example, let us say Kazakhstan uses the same STIR root certificates as the Russian Federation. We would expect to see

Numeric	ISO
7	RF

in the Country Code Registry and

ISO	Certificate
RF	[STIR public root certificate]

in the STIR Root Certificate Registry. Calls to +76 and +77 will match +7 in the Country Codes Registry, which maps to the string RF, which maps to the shared STIR root certificate.

Take the case where Kazakhstan uses a different certificate than the Russian Federation. Then we would expect to see

Numeric	ISO
7	RF
76	KZ
77	KZ

in the Country Code Registry and

ISO	Certificate
RF	[RF's STIR public root certificate]
KZ	[KZ's STIR public root certificate]

in the STIR Root Certificate Registry.

Finally, take the case the Russian Federation specifies authorized STIR root certificate authorities, but Kazakhstan does not. Then we would see

Numeric	ISO
7	RF
76	KZ
77	KZ

in the Country Code Registry and

```
+-----+------------------------------------+
| ISO |             Certificate            |
+-----+------------------------------------+
|  RF | [RF's STIR public root certificate] |
+-----+------------------------------------+
```

in the STIR Root Certificate Registry. Here, calls from Kazakhstan would match the +76 mapping, but applications will notice there are no KZ STIR root certificate authorities in the STIR Root Certificates Registry.

The registry indicates multiple STIR root certificate authorities by having multiple entities with the same ISO country code and different STIR root certificates in the STIR Root Certificates Registry. For example,

```
+---------+-----+
| Numeric | ISO |
+---------+-----+
|    1    |  US |
+---------+-----+
```

in the Country Code Registry and

```
+-----+----------------------------------------------+
| ISO |                  Certificate                 |
+-----+----------------------------------------------+
|  US | [US STIR public root certificate authority A] |
|     |                                              |
|  US | [US STIR public root certificate authority Z] |
+-----+----------------------------------------------+
```

in the STIR Root Certificate Registry.

3. Registry Elements

3.1. Numeric Country Code

E.164 [E.164] defines the country code as a one- to three-digit string. However, there are some country codes that have different country delegations beyond the country code. For example, footnote b of E.164 Annex D [E.164D] shows 25 countries under country code +1 and two countries under country code +7. As well, country code +881, for satellite services, and codes +882 and +883, for international networks, are under the jurisdiction of various national authorities.

To distinguish the various national authorities under a given country code, the country code entry can contain these identity codes.

Currently, the longest entry can be seven digits, but this could change in the future.

Applications using this registry to find the ISO country code for a given numeric country code (and identity codes) use the longest match in the registry. A potential error condition would be if a country has not designated a mapping in the registry and another country with a shorter, overlapping numeric country code string does have a mapping. At the time of this writing, this is only possible for the overlapping country codes of +1 and +7 as well as the special use codes +881, +882, and +883.

Unfortunately, there is no easy algorithm or pattern to the identity digits (area codes) in country code +1. As of the time of the writing this document, the North American Numbering Plan Administrator (NANPA) reports that the United States has about 275 area codes assigned (including free phone and local number portability routing), Canada has 65 area codes assigned, and the various Caribbean nations have 1-4 area codes assigned each [NPAreport]. As a further complication, the freephone number space, such as +1800 and +1888, is also shared. Some countries have exclusive responsibility for some 800 number prefixes, such as +1800389 for the Bahamas and +1800271 for Trinidad.

3.2. STIR Root CA Public Key

Each country can have zero or more STIR root certificate authorities. The STIR root certificate authority is the trust anchor for STIR (SIP) PKI in the given jurisdiction. The expectation is the authority for signing the identity of a caller will be much stricter than the authority for signing the identity of, for example, a Web site. In the common Web browser situation, a Web server operator can purchase a certificate issued by one of hundreds of certificate authorities from anywhere in the world. To ensure interoperability, browser and operating system manufacturers need to include the STIR root certificates from those certificate authorities so when a user in one part of the world accesses a Web server in another part of the world that has a certificate issued by a certificate authority in yet a different part of the world, the site will validate. In the telephone number identity situation, it is expected that for the most part the individual national numbering authorities will choose a very limited set of STIR root certificate authorities who will be allowed to issue signing certificates for numbers assigned to that country.

Within a single country, it would be a relatively easy matter for the national communications regulator to impose and inform their domestic service providers who is the designated certificate authority within that country. However, given the large amount of international

telephone traffic (as an example, there were over 100,000,000,000 minutes of traffic between the U.S. and other countries in 2014, including VoIP [FCC_intl]), there is a need for service providers and users in different countries to validate that one of the proper certificate authorities for that country has issued the signing certificate.

The entry for each national STIR root certificate authority is a P7B certificate [RFC2315] that contains the public key of the STIR root certificate authority, matching the private key the STIR root certificate authority uses to sign signing keys used by its delegates, such as telecommunications service providers.

Countries that are not participating in STIR but want to avoid the shortest-match issue raised above can create an entry in the Country Code registry with no entry in the STIR Root Certificate registry.

4. Terminology

This document uses the terms "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" as RFC 2119 [RFC2119] defines them.

5. IANA Considerations

Refer to [RFC8126] for a description of IANA Considerations terms and their meanings.

5.1. Registry Policy: Expert Review

This registry is Expert Review with registry-based delegation. The integrity of a given nation's numbering system is generally the purview of the respective national government. We do not anticipate IANA to intervene in disputes of who has the authority for entering and changing STIR root certificates. In general, IANA SHOULD validate the request is related to the recognized national authority for the country as specified in [ITU-D.Agencies], unless it is not clear who the national authority is.

TO DO: Instead of using the RAI list, should we setup a dedicated list for dispute resolution?

5.2. Appealing Registry Decisions

IANA makes decisions based on expertise as well as guidance from the community. If a member of the community has a concern with an individual decision made by IANA with regard to the registry, the individual shall proceed as follows:

1. Attempt to resolve the concern directly with IANA.

2. If a resolution cannot be reached directly with IANA, express the concern to the community and attempt to achieve rough consensus regarding a resolution on the RAI list. The Area Directors of the IETF Real-time Applications and Infrastructure Areamay, at their discretion, attempt to guide the members of the community to rough consensus.

3. As a last resort, if a resolution cannot be reached on the RAI mailing list, appeal to the IESG for a resolution. The appellant must show that the decision made by IANA (a) was materially in error and (b) has caused material harm. In its deliberations regarding an appeal, the IESG shall weigh all the evidence presented to it and use its best judgment in determining a resolution.

5.3. Registry Elements

The STIR Root Certificate registry consists of one or more entities indicating the public keys of STIR root certificate authorities for a given country code. With around 200 countries, each of which might have one to four STIR root certificate authorities, results in a registry with a total participation of about one thousand entries. The expectation is there would be substantially fewer entries in practice.

5.3.1. Numeric Country Code

The numeric country code is a one- to eight-digit string indicating the numeric country code and optional identity digits. Identity digits are often known as an area code or city code. [E.164D] lists country codes and the identity digits when there are overlapping country codes (+1, +7, and some international codes).

IANA MUST verify the requested mapping includes a valid numeric country code as specified in E.164 Annex D.

NOTE: The conventional leading + to indicate the string identifies a country code is NOT part of the Country Code element in the registry.

5.3.2. ISO Country Code

The ISO country code is a two-character string drawn from ISO 3166-1 alpha-2 [ISO.3166-1.2013].

IANA should verify the requested mapping includes a valid two-digit country code appropriate for the requested numeric country code,

subject to the understanding that a country's numeric country code may map to an enclosing ISO country code if there is no longer match in the Country Code Registry. IANA MAY verify whether there is a need to place entries for enclosed numeric country codes if an enclosing Country Code mapping is established. This is only an issue for numeric country codes in +1, +7, +881, +882, and +883 at the time of this writing.

5.3.3. STIR Root Certificate

The STIR root certificate is a P7B file [RFC2315] that contains the public key of the authorized STIR root certificate that signs the certificates authorized to sign STIR signaling in the given country. There can be one or more entries in the registry for a given ISO country code to allow for multiple STIR root certificate authorities for a given country.

IANA MUST verify the certificate is valid.

5.4. Other IANA Considerations

The expectation is the relevant national authorities or their designates will keep IANA informed on updates to things such as numbering plans. This is most prominently an issue in numeric country code +1, where the numbering administrator often assigns new area codes, which could end up in different countries. Specifically, IANA has no obligation to monitor the ITU-T, North American Numbering Plan Administrator (NANPA), or other entity to keep the Country Code Registry up to date. It should be noted there is a single NANPA for the entire +1 numeric country code.

At the time of this writing, we expect both the United States and Canada to be specifying a limited set of STIR root certificate authorities. The most difficult overlap set is the overlap between Canada and the United States in the numeric country code list. As a convenience to the community we request IANA pre-populate the Country Code Registry with +1 mapped to the string US and to pre-populate the Country Code Registry with the area codes assigned to Canada with the string CA, as found in the authoritative listing of +1 area code assignments [NPAreport]. As an example, but not necessarily the normative entries:

Numeric	ISO
1	US
1204	CA
1226	CA
1236	CA
...	...

6. Security Considerations

The choice of having the STIR root certificate stored by IANA means that users accessing the certificates MUST use a source-authenticated retrieval mechanism, such as HTTPS [RFC7231]. It almost goes without saying implementers should be using the most up-to-date TLS implementation (or its successor) when retrieving registry elements from IANA. Likewise, the application resolving the URI MUST verify the domain in the certificate matches the IANA domain. The application resolving the URI MUST use DNSSEC [RFC4035] if it is available to the client. Finally, during TLS negotiation the application MUST verify the authority signing IANA's certificate matches the application's understanding of who is expected to sign IANA's certificate. At the time of this writing, that root certificate would be the DigiCert High Assurance EV Root CA.

7. Acknowledgements

Russ Housley and Sean Turner helped with the decision of registering certificates instead of URIs. Ken Carlberg and Padma Krishnaswamy of the United States Federal Communications Commission provided useful feedback in an incredibly short time period. Finally, a huge thank-you to Michelle Cotton and Kim Davies for helping normalize the registries and the procedures for populating them.

8. References

8.1. Normative References

[E.164D] International Telecommunications Union, "List of ITU-T Recommendation E.164 Assigned Country Codes", ITU-T Recommendation E.164 Annex D, 11 2011, <https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164D-2016-PDF-E.pdf>.

[ISO.3166-1.2013]
International Organization for Standardization, "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes, 3rd edition", ISO Standard 3166-1, 11 2013.

[ITU-D.Agencies]
International Telecommunications Union - Development Sector, "National Telecommunication Agencies", 12 2017, <http://www.itu.int/en/ITU-D/Statistics/Pages/links/nta.aspx>.

[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>.

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, DOI 10.17487/RFC2315, March 1998, <https://www.rfc-editor.org/info/rfc2315>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

8.2. Informative References

[E.164] International Telecommunications Union, "The International Public Telecommunication Numbering Plan", ITU-T Recommendation E.164, 11 2010, <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.164-201011-I!!PDF-E&type=items>.

[FCC_intl]
Ashton, S. and L. Blake, "2014 U.S. International Telecommunications Traffic and Revenue Data", 7 2016, <http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0701/DOC-340121A1.pdf>.

[NPAreport]
North American Numbering Plan Administrator, "NPA Database", 12 2017, <https://www.nationalnanpa.com/nanp1/npa_report.csv>.

[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>.

[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>.

[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>.

[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>.

Author's Address

Eric W. Burger
Georgetown University
37th & O St, NW
Washington, DC 20057
USA

Email: eburger@standardstrack.com