STIR
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2020

E. Burger
Georgetown University

March 8, 2020

# Registry for Country-Specific Secure Telephone Identity (STIR) Trust Anchors
## draft-burger-stir-iana-cert-01

Abstract

National policy defines telephone numbering governance. One area of such governance are the policies applied to the Secure Telephone Identity Credentials defined in RFC 8226. Nations have policies for the acceptable trust anchors for these credentials. This document defines an IANA registry that enables a SIP call recipient in one country to validate the signature, as defined in RFC 8224, that originates in another country useing an appropriate trust anchor for the signer's certification path, per the origination country's trust anchor policy.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 9, 2020.

## 1. Introduction

One problem that plagues some communications applications is a caller deliberately misrepresenting 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 an E.164 [E.164] telephone number. 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]. Note the country code does not itself necessarily uniquely identify a country. For example, in country codes +1 and +7, multiple countries share the country code. In the cases of +1 and +7, further digits in the E.164 number, known as national significant digits (also known as area codes in +1) further identify the country. As well, there are non-geographic services with country codes assigned to them.

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 certification path. As such, the base STIR documents defer certificate and validation policy to other documents. This document describes a registry for finding a STIR trust anchor for a given country code for signed telephone numbers. This document only enables policies for E.164 number identity assertions. Moreover, while this document describes the STIR trust anchor registry for various national STIR trust anchors, 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 certification path to an unauthorized trust anchor. 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, the ITU-T assigns telephone numbers, specifically the responsibility to assign numbers beneath a country's country code, to national communications authorities. A national regulator can inform service providers under its authority which trust anchors 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 trust anchors, indexed by country codes.

## 2. 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.

As noted above, a country code may not sufficiently identify a particular country. Likewise, national policy may assign different STIR trust anchors for different sets of national significant numbers (e.g., area codes). For example, while +7 generally identifies the Russian Federation, +76 and +77 identify Kazakhstan. Likewise, +1 generally identifies the North American Numbering Plan (NANP), which identifies countries by area code (the following three digits after the country code). For example, +1869 identifies Saint Kitts and Nevis while +1649 identifies Turks and Caicos. The term "country code" appearing from this point forward in this document refers to the country code and, if necessary, the subsequent digits that identify a country or region. With the exception of ITU-T country code +1, the ITU-T country code is the "country code" for the purposes of this registry. In the NANP (+1) case, this means the "country code" can be four digits long. Specifically, to identify a

specific country in the NANP, what this document terms the "country code" will be the leading +1 and the following three-digit area code.

## 3. STIR Trust Anchor Registry

This registry maps E.164 country codes to STIR trust anchors. There can be one or more STIR trust anchors per country code.

### 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. In these cases, we use additional digits in the number to unambituously identify a country. 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. As noted above, distinguishing the appropriate certificate to use can be a matter of local policy. We suggest longest match, but be aware that local policy may dictate another policy within that jurisdiction.

### 3.2. STIR Trust Anchor

Each country can have zero or more STIR trust anchors. The trust anchor is a self-signed certificate [RFC5280]. The STIR trust anchor is the trust anchor for STIR (SIP) PKI in the given jurisdiction. 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. The expectation is the authority for signing the identity of a caller will be more strict than the authority for signing the identity of, for example, a Web site. To ensure interoperability, browser and operating system manufacturers need to include the STIR trust anchors 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, for the most part the individual national numbering authorities will choose a very limited set of STIR trust anchors who they will allow 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 trust anchor is a text certificate [RFC7468] that contains the public key of the STIR trust anchor, matching the private key the STIR trust anchor uses to sign signing keys used by its delegates, such as telecommunications service providers.

## 4. IANA Considerations

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

### 4.1. Registry Policy: First Come First Served

This registry is First Come First Served, understanding there can be multiple trust anchors registered for a given Country Code prefix. The integrity of an originating nation's numbering system is generally the purview of the respective national government. Moreover, the integrity of a terminating network, including the accuracy of received signaling, is generally the purview of the government with jurisdiction over the terminating network. We do not anticipate IANA to intervene in disputes of who has the authority for entering and changing STIR trust anchors. In general, IANA SHOULD validate the request originates from an entity authorized by the recognized national authority for the country as specified in [ITU-D.Agencies], unless it is not clear who the national authority is. However, because it is likely the regulatory authorities in the terminating country will determine the validity of the STIR trust anchor found in the IANA registry, irrespective of the depth of vetting IANA could perform, if IANA believes the registration is not fraudulent, it SHOULD accept the registration even if it cannot positively identify or contact the appropriate national authority.

### 4.2. Registry Elements

The STIR Trust Anchor registry consists of one or more entities indicating the public keys of STIR trust anchors for a given country code. With around 200 countries, each of which might have one to

four STIR trust anchors, results in a registry with a total participation of about one thousand entries. The expectation is there would be substantially fewer entries in practice.

#### 4.2.1. 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.

#### 4.2.2. STIR Trust Anchor

The STIR trust anchor is an RFC7468 [RFC7468] text file that contains the public key of the authorized STIR trust anchor 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 trust anchors for a given country.

IANA MUST verify the certificate is valid by using the provided public key in the certificate to validate the signature in the certificate.

IANA SHOULD remove a STIR trust anchor from the registry if the certificate expires.

#### 4.2.3. Domain of Authority

For traceback and reputation purposes, IANA MUST record the validated domain of the entity that made the request to enter, delete, or modify an entry in the STIR Trust Anchor Registry. The mechanism for validating the domain is a matter of IANA policy. Mechanisms include ensuring an emailed request uses DKIM [RFC6376] with secure cryptographic algorithms [RFC8301], web requests have validated client certificates identifying the domain of the requestor, or out of band methods. Note that an unauthenticated inbound phone call is not likely to be an acceptable mechanism of identifying the domain.

### 4.3. Other IANA Considerations

There is the potential for a malicious actor attempting to load a trust anchor that could enable them to sign spoofed signaling. As such, IANA SHOULD note who is making the request, to sufficient detail to locate that party for referral to the relevant national authorities. For most countries, it will be the national authority itself or a clear delegate that will be making the registration. For example, in the United States, the Federal Communications Commission has delegated the governance of the STIR trust anchor to the U.S. STI-GA, administered by ATIS, which is an identifiable, incorporated entity with a fixed, physical address.

## 5. Security Considerations

The choice of having the STIR trust anchor 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 should sign IANA's certificate. At the time of this writing, that trust anchor would be the DigiCert High Assurance EV Root CA.

Because IANA takes no responsibility for the accuracy of any given country's STIR trust anchor entry, this document presumes the terminating provider or local authority will use local policy to determine the trustworthiness of any given entry. ATIS [ATIS-Intl] describes an example of such a local policy.

## 6. Acknowledgements

Russ Housley, Jim McEachern, and Sean Turner gave invaluable insight. 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.

# 7. References

## 7.1. 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>.

[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>.

[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>.

[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>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[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>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/info/rfc7468>.

[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>.

[RFC8301] Kitterman, S., "Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)", RFC 8301, DOI 10.17487/RFC8301, January 2018, <https://www.rfc-editor.org/info/rfc8301>.

## 7.2. Informative References

[ATIS-Intl] Alliance for Telecommunications Industry Solutions, "Mechanism for International Signature-based Handling of Asserted information using toKENs (SHAKEN)", <http://access.atis.org/apps/org/workgroup/ipnni/download.php/51306/IPNNI-2020-00032R000.docx>.

[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>.

[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