Registry for Country-Specific STIR Root Certificates

Eric Burger

Georgetown University

Thanks to Russ Housley, Sean Turner (IETF);
Ken Carlberg, Padma Krishnaswamy (FCC); and
Michelle Cotton, Kim Davies (IANA)
for help with the contents of the draft! Any errors are of course mine.

CA = Certification Authority

Problem Statement

- STIR CA's not the same as Web CA's
  - An absolute statement, as in different companies from the ecosystem
  - A structural statement, as in the roots-of-trust problem is different
- Web root of trust
  - Host operator in country A
  - Buys certificate from CA in country B (e.g., because they are inexpensive)
  - Client in country C
  - Path of least resistance today is to have all of the (recognized) CA's in the browser / operating system
  - Vulnerable to root certificate hijacking (e.g., Diginotar, BlueCoat)
  - Since the signature is over a national resource (E.164 number), countries have proprietary interest in who can vouch for a number

TN = Telephone Number

STIR CA's are different

- Who can be the CA for a given country's TN's appears to be mandated by the country

Canadian Radio-television and Telecommunications Commission | Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement and Telecom Decision CRTC 2018-32

PDF version

References: Compliance and Enforcement and Telecom Notice of Consultation 2017-4, as amended, and Compliance and Enforcement and Telecom Regulatory Policy 2016-442

Ottawa, 25 January 2018

Public record: 1011-NOC2017-0004 and 8665-C12-201507576

Measures to reduce caller identification spoofing and to determine the origins of nuisance calls

31. Accordingly, the Commission expects, by **31 March 2019**, that

- TSPs will implement measures to authenticate and verify caller ID for all IP-based voice calls; and
- the telecommunications industry will establish a Canadian certificate administrator.

Federal Communications Commission **FCC 17-89**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Call Authentication Trust Anchor) WC Docket No. 17-97

NOTICE OF INQUIRY

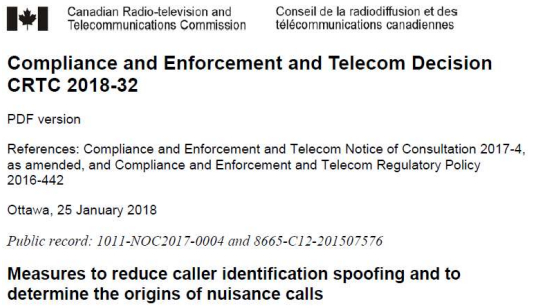
Comment Date: August 14, 2017
Reply Comment Date: September 13, 2017

Adopted: July 13, 2017 **Released: July 14, 2017**

29. *Certification Authority*. ATIS recommends that certification authorities meet two criteria: (1) having sufficient certificate management expertise; and (2) having an in-market presence (i.e. being incorporated in the United States).[49] We seek comment on these criteria, as well as any suggestions for other criteria. Are there existing entities that are likely to be appropriate certification authorities, such as numbering-related entities like the NANPA, Pooling Administrator, or LNPA? We also seek comment on the strengths and weaknesses of using both an online and offline certification authority, as used in other systems such as Domain Name System Security Extensions (DNSSEC).[50]

STIR CA's are different

- Who can be the CA for a given country's TN's is likely to be mandated by the country



Canadian Radio-television and Telecommunications Commission | Conseil de la radiodiffusion et des télécommunications canadiennes

Compliance and Enforcement and Telecom Decision CRTC 2018-32

PDF version

References: Compliance and Enforcement and Telecom Notice of Consultation 2017-4, as amended, and Compliance and Enforcement and Telecom Regulatory Policy 2016-442

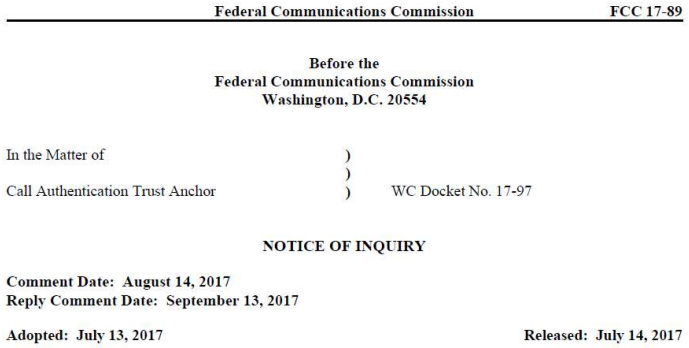
Ottawa, 25 January 2018

Public record: 1011-NOC2017-0004 and 8665-C12-201507576

Measures to reduce caller identification spoofing and to determine the origins of nuisance calls

31. Accordingly, the Commission expects, by **31 March 2019**, that

- TSPs will implement measures to authenticate and verify caller ID for all IP-based voice calls; and
- the telecommunications industry will establish a Canadian certificate administrator.



Federal Communications Commission **FCC 17-89**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Call Authentication Trust Anchor) WC Docket No. 17-97

NOTICE OF INQUIRY

Comment Date: August 14, 2017
Reply Comment Date: September 13, 2017

Adopted: July 13, 2017 **Released: July 14, 2017**

29. *Certification Authority*. ATIS recommends that certification authorities meet two criteria: (1) having sufficient certificate management expertise; and (2) having an in-market presence (i.e. being incorporated in the United States).[50] We seek comment on these criteria, as well as any suggestions for other criteria. Are there existing entities that are likely to be appropriate certification authorities, such as numbering-related entities like the NANPA, Pooling Administrator, or LNPA? We also seek comment on the strengths and weaknesses of using both an online and offline certification authority, as used in other systems such as Domain Name System Security Extensions (DNSSEC).[50]

Who should the STIR verifier trust?

- In Canada for a Canadian call, whomever CRTC says
- In the UK for a British call, whomever OFCOM says
- In the US for an American call, whomever FCC says
- Works great for calls and service providers in a country
- Does not scale for international calls
  - How would a UK operator know whom CRTC designates the official CAs to be?

STIR Root Certificates Registry

- Maps countries to root certificates (public keys)
- Managed by IANA
  - Per expert review as enumerated on prior slide
- Data Elements
  - ISO 3166-1 2-letter country code
  - P7B format public key of root certificate authority(ies)
    - Support out of the box for multiple root certificate authorities for a country or region

Country Code Registry

- Maps numeric country code (E.164 Annex D) to 2-character (ISO 3166-1) country code
- Handles overlapping numeric codes (e.g., +1, +7, +881, +882, +883)
  - Longest match
  - Regional authorities (e.g., could be one set for all of NANP, all of Europe, etc.)
  - Opting out (e.g., US and CA have designated root CA's, but MS does not sign)

Registry policy

- Expert review
- Identical process as for time zone databases
- Resources for expert:
  - ITU-D publishes directory of national numbering authorities
  - National numbering authorities likely to publish authorized STIR root CA providers
  - If dispute, take to list (as done for TZ)

Open issues

- Should we setup a dedicated list for number authority disputes?
- Should this be split into two drafts?
  - The E.164 Annex D to ISO 3166-1 registry could be generally useful beyond STIR
- Other?