APNIC 42

RPKI Trust Anchor

Geoff Huston

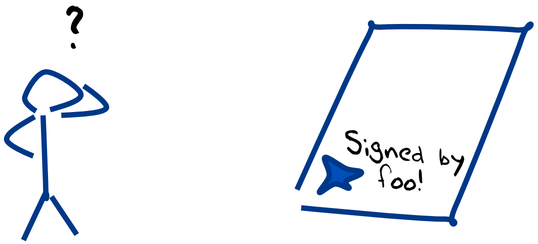
APNIC

COLOMBO, SRI LANKA

28 September – 5 October 2016

#apnic42

Public Keys



How can you "trust" a digital signature?

What if you have never met the signer and have no knowledge of them or their keys?

One approach is transitive trust via a hierarchy of public key certificates

(there are other approaches, based on "web of trust" models, but lets not go there)

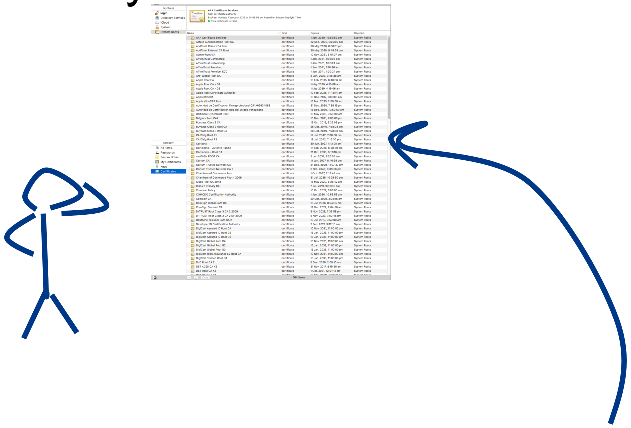
Public Key Infrastructure

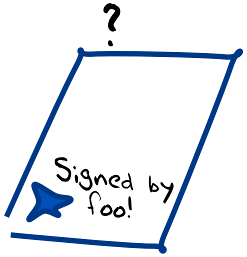
For transitive trust, you have to start somewhere with some initial entity (or entities) in whom you are prepared to trust

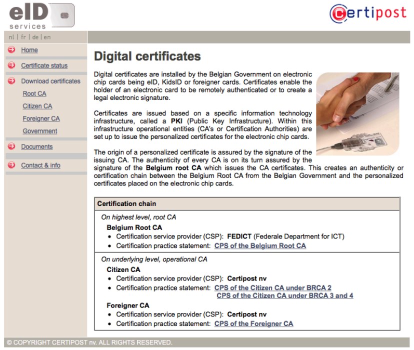
This is your TRUST ANCHOR set, and you keep a local copy of their public key in your certificate store as Trusted Certificates

Each Trust Anchor entry matches a unique PUBLIC KEY can can be used to certify a Certificate issued by this Certification Authority

Key Store







Digital certificates

Digital certificates are installed by the Belgian Government on electronic chip cards being eID, KidsID or foreigner cards. Certificates enable the holder of an electronic card to be remotely authenticated or to create a legal electronic signature.

Certificates are issued based on a specific information technology infrastructure, called a **PKI** (Public Key Infrastructure). Within this infrastructure operational entities (CA's or Certification Authorities) are set up to issue the personalized certificates for the electronic chip cards.

The origin of a personalized certificate is assured by the signature of the issuing CA. The authenticity of every CA is on its turn assured by the signature of the **Belgium root CA** which issues the CA certificates. This creates an authenticity or certification chain between the Belgium Root CA from the Belgian Government and the personalized certificates placed on the electronic chip cards.

Certification chain

On highest level, root CA

Belgium Root CA
- Certification service provider (CSP): **FEDICT** (Federale Department for ICT)
- Certification practice statement: CPS of the Belgium Root CA

On underlying level, operational CA

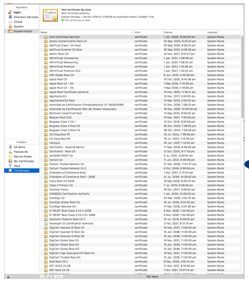
Citizen CA
- Certification service provider (CSP): **Certipost nv**
- Certification practice statement: CPS of the Citizen CA under BRCA 2
  CPS of the Citizen CA under BRCA 3 and 4

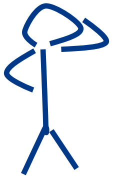
Foreigner CA
- Certification service provider (CSP): **Certipost nv**
- Certification practice statement: CPS of the Foreigner CA

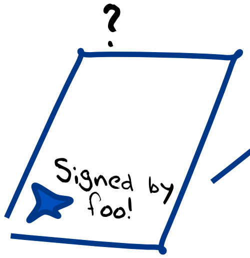
Public Key Infrastructure

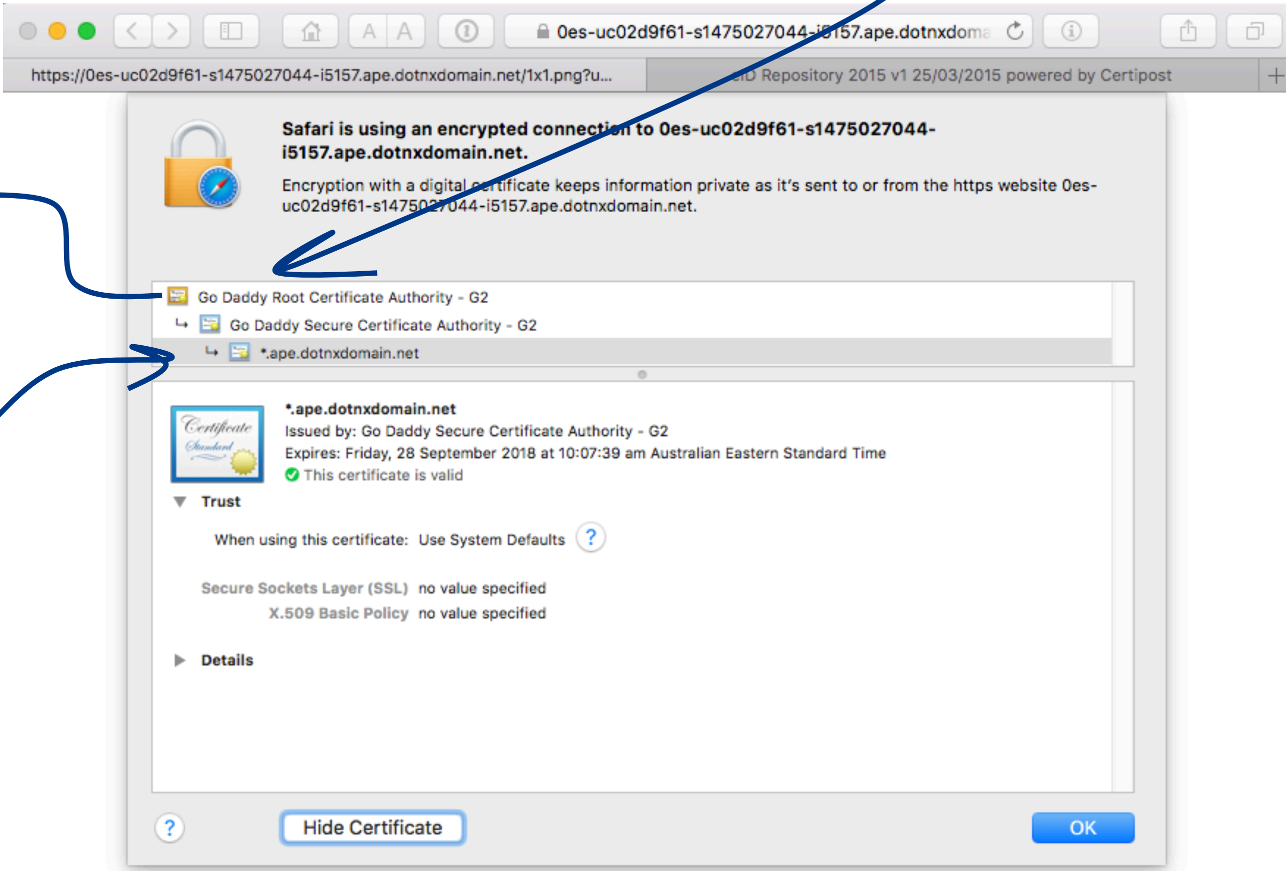
Validation is a process of finding a chain of public key certificates that link a trust anchor to the entity being validated in this manner

Key Store








0es-uc02d9f61-s1475027044-i5157.ape.dotnxdoma
https://0es-uc02d9f61-s1475027044-i5157.ape.dotnxdomain.net/1x1.png?u...
ID Repository 2015 v1 25/03/2015 powered by Certipost

Safari is using an encrypted connection to 0es-uc02d9f61-s1475027044-i5157.ape.dotnxdomain.net.

Encryption with a digital certificate keeps information private as it's sent to or from the https website 0es-uc02d9f61-s1475027044-i5157.ape.dotnxdomain.net.

- Go Daddy Root Certificate Authority - G2
  - ↳ Go Daddy Secure Certificate Authority - G2
    - ↳ *.ape.dotnxdomain.net

***.ape.dotnxdomain.net**
Issued by: Go Daddy Secure Certificate Authority - G2
Expires: Friday, 28 September 2018 at 10:07:39 am Australian Eastern Standard Time
✓ This certificate is valid

▼ **Trust**

When using this certificate: Use System Defaults ?

Secure Sockets Layer (SSL)	no value specified
X.509 Basic Policy	no value specified

▶ **Details**

The Resource Public Key Infrastructure

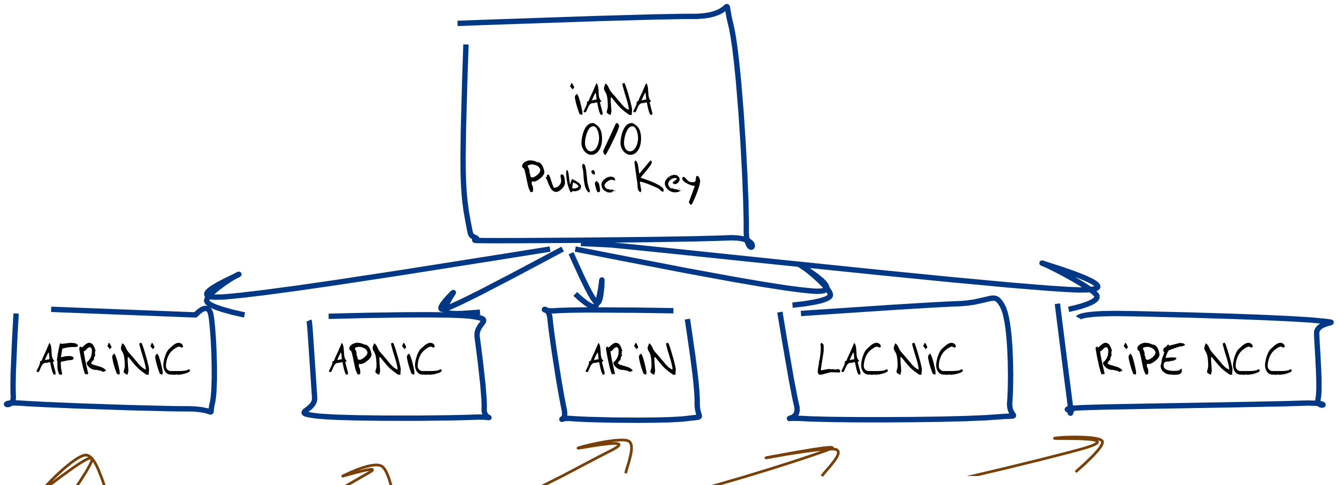
The RPKI is a conventional PKI where the Certificate Issuer certifies BOTH the public key of the subject and the subject’s number resource holdings

As it is a conventional PKI, the RPKI needs to have Trust Anchor(s)

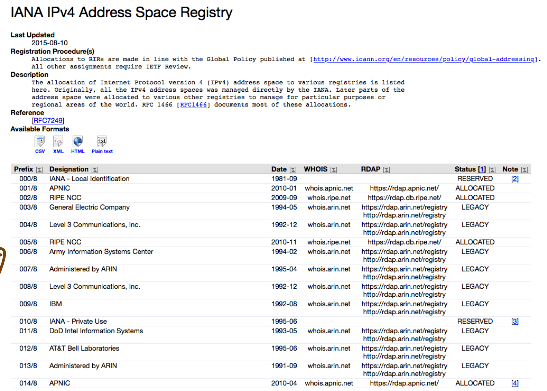
What models can be used to publish proposed Trust Anchors for the RPKI?

And who can (or should) publish this Trust Anchor Material?

RPKI Certificates Follow Allocations: A single IANA-issued Trust Anchor



Number Resource contents of RiR Subordinate CAs issued by the iANA match the contents of the iANA Number Registries



IANA IPv4 Address Space Registry

Last Updated
2015-08-10

Registration Procedure(s)

```
Allocations to RIRs are made in line with the Global Policy published at [http://www.icann.org/en/resources/policy/global-addressing].
All other assignments require IETF Review.
```

Description

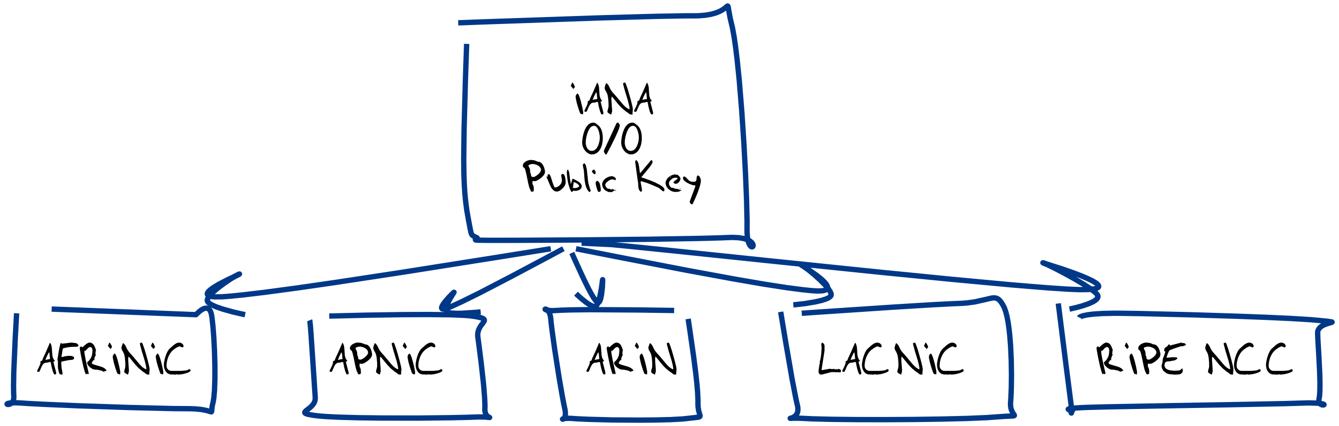
```
The allocation of Internet Protocol version 4 (IPv4) address space to various registries is listed
here. Originally, all the IPv4 address spaces was managed directly by the IANA. Later parts of the
address space were allocated to various other registries to manage for particular purposes or
regional areas of the world. RFC 1466 [RFC1466] documents most of these allocations.
```

Reference
[RFC7249]

Available Formats

Prefix	Designation	Date	WHOIS	RDAP	Status [1]	Note
000/8	IANA - Local Identification	1981-09			RESERVED	[2]
001/8	APNIC	2010-01	whois.apnic.net	https://rdap.apnic.net/	ALLOCATED	
002/8	RIPE NCC	2009-09	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED	
003/8	General Electric Company	1994-05	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
004/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
005/8	RIPE NCC	2010-11	whois.ripe.net	https://rdap.db.ripe.net/	ALLOCATED	
006/8	Army Information Systems Center	1994-02	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
007/8	Administered by ARIN	1995-04	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
008/8	Level 3 Communications, Inc.	1992-12	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
009/8	IBM	1992-08	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
010/8	IANA - Private Use	1995-06			RESERVED	[3]
011/8	DoD Intel Information Systems	1993-05	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
012/8	AT&T Bell Laboratories	1995-06	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
013/8	Administered by ARIN	1991-09	whois.arin.net	https://rdap.arin.net/registry http://rdap.arin.net/registry	LEGACY	
014/8	APNIC	2010-04	whois.apnic.net	https://rdap.apnic.net/	ALLOCATED	[4]

RPKI Certificates Follow Allocations: A single IANA-issued Trust Anchor

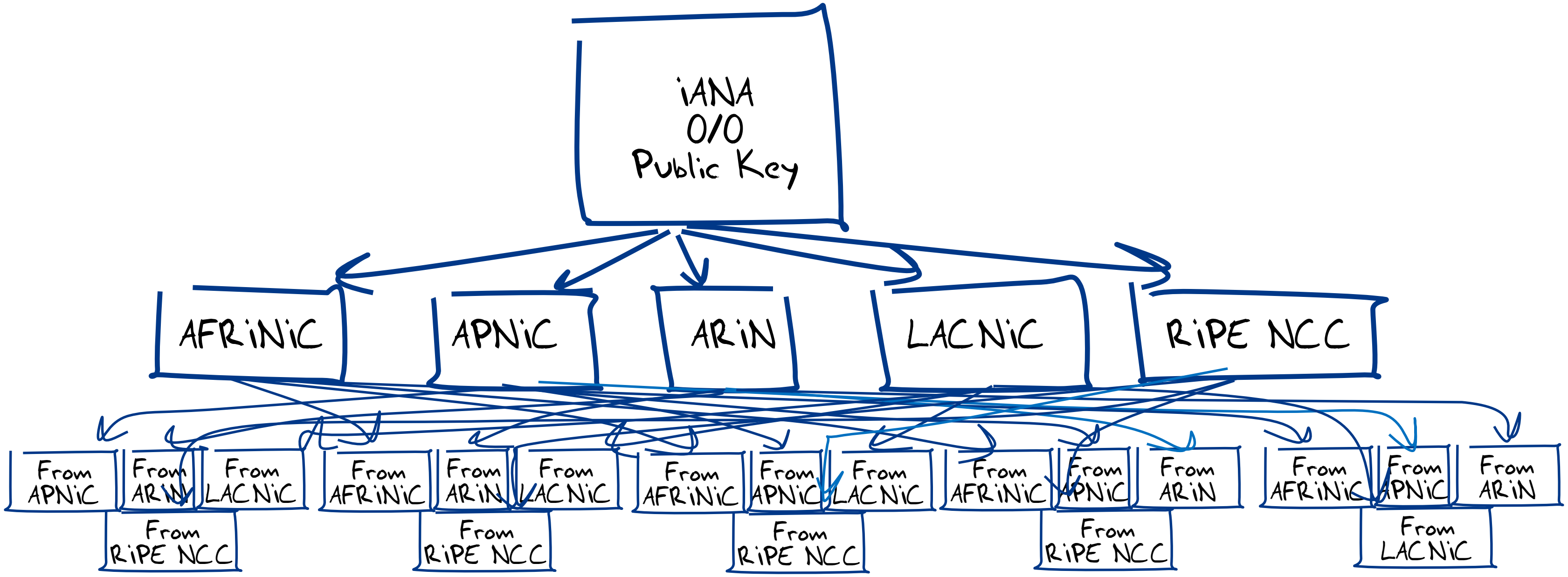


The issue here is how to certify transferred resources. These resources are not separately listed in the IANA registries so will not be included in the IANA-issued CA Certificate.

If we want to preserve this clear top-level certificate model then the implication is that modelling transferrred resources in this RPKI will:

- require RIRs to issue certificates for each other
- and because the certification validation paths will differ, a user holding transferred resources may be issued with multiple certificates

IANA TA, RPKI Certificates Follow Allocations

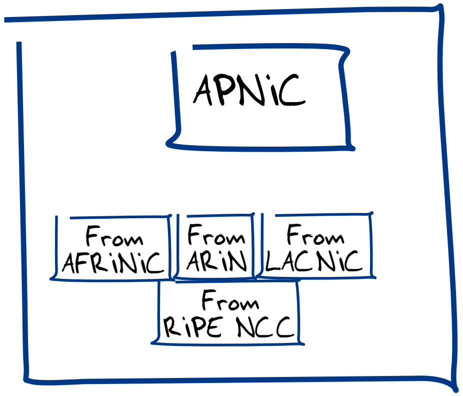


This results in a complex inter-RIR CA structure to support transfers

And ALL RIRs need to be in a position to support this model as a precondition to adoption

But if one of more RIRs are not ready to do this, what can be done?

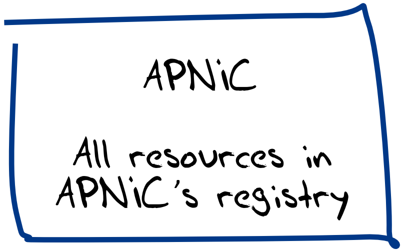
Interim APNIC TA Structure



The interim model used by APNIC promotes the 5 “top level” certificates where APNIC would be the subject into a compound trust anchor containing 5 self-signed certificates

This will allow APNIC to migrate to a single IANA TA without major change (the self signed certificates are changed to certificate signing requests and the local trust structure can be removed)

Other possible interim TA models

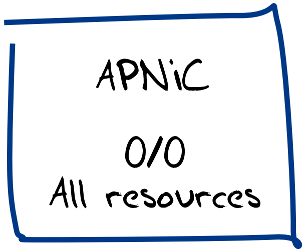


This is a much simpler model, and is the one used by other RIRs as an interim per-RIR TA

But this is some distance from the requirements to support a single IANA TA in the future

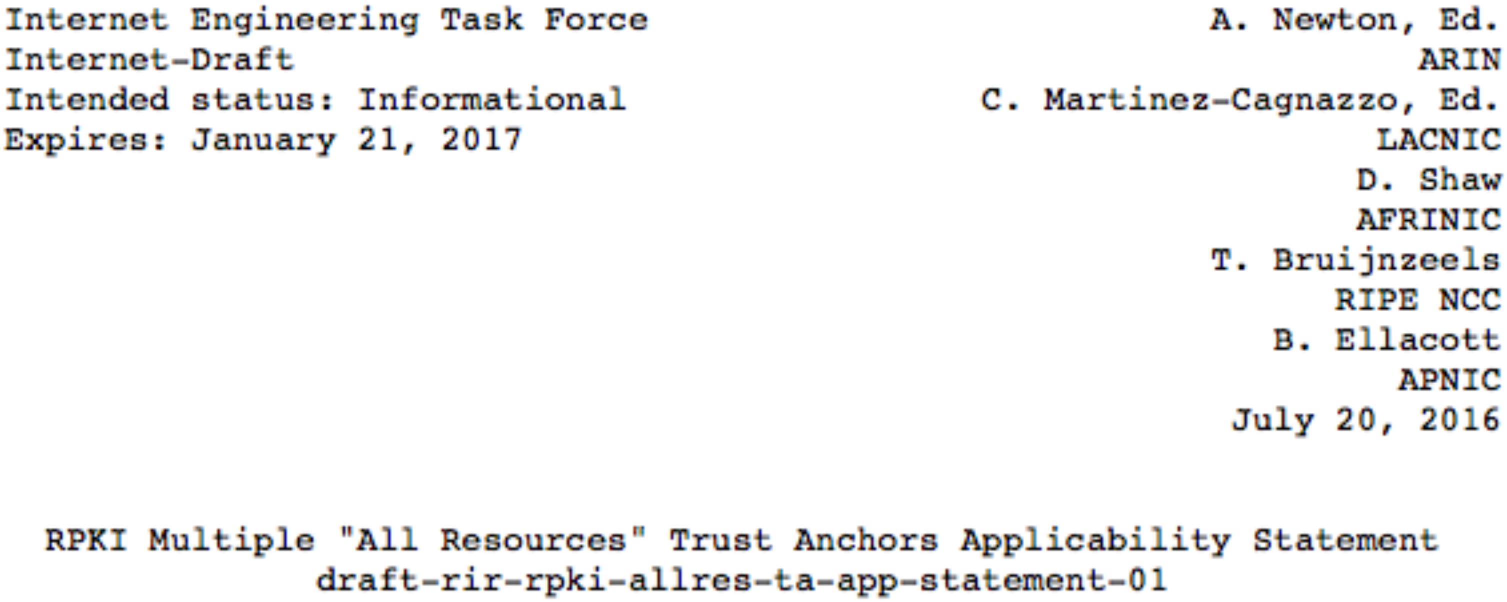
So the amount of work and user impact to transform from this self-signed TA cert structure to a single IANA TA would be far larger

Other possible interim TA models



This simplifies the TA structure further, as no changes are required to the TA in the event of resource movement. The published per RIR TA is essentially static so off-line (or even one-shot use) keys can be used

However it does not reflect APNIC's current resource holdings in the TA certificate



Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 21, 2017

A. Newton, Ed.
ARIN
C. Martinez-Cagnazzo, Ed.
LACNIC
D. Shaw
AFRINIC
T. Bruijnzeels
RIPE NCC
B. Ellacott
APNIC

July 20, 2016

RPKI Multiple "All Resources" Trust Anchors Applicability Statement
draft-rir-rpki-allres-ta-app-statement-01

Comments?

Questions?

APNIC 42

COLOMBO, SRI LANKA

28 September – 5 October 2016

#apnic42