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 let’s 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

Signed by foo!
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

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

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

Issued by: GoDaddy Secure Certificate Authority - G2
Expires: Friday, 28 September 2018 at 16:07:39 am Australian Eastern Standard Time
This certificate is valid

When using this certificate: Use System Defaults
Details

Signed by foo!
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
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 transferred 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?
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

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?