APNIC Trial of Certification of IP Addresses and ASes

IETF 66
SIDR BOF

George Michaelson
Geoff Huston

Address and Routing Security

What we have today is a relatively insecure system that is vulnerable to various forms of deliberate disruption and subversion

And it appears that bogon filters and routing policy databases are not, in and of themselves, entirely robust forms of defence against these vulnerabilities

Address and Routing Security

The (very) basic routing security questions that need to be answered are:

- Is this a valid address prefix?
- Who injected this address prefix into the network?
- Did they have the necessary credentials to inject this address prefix?

What would be good …

To use a public key infrastructure to support attestations about addresses and their use:

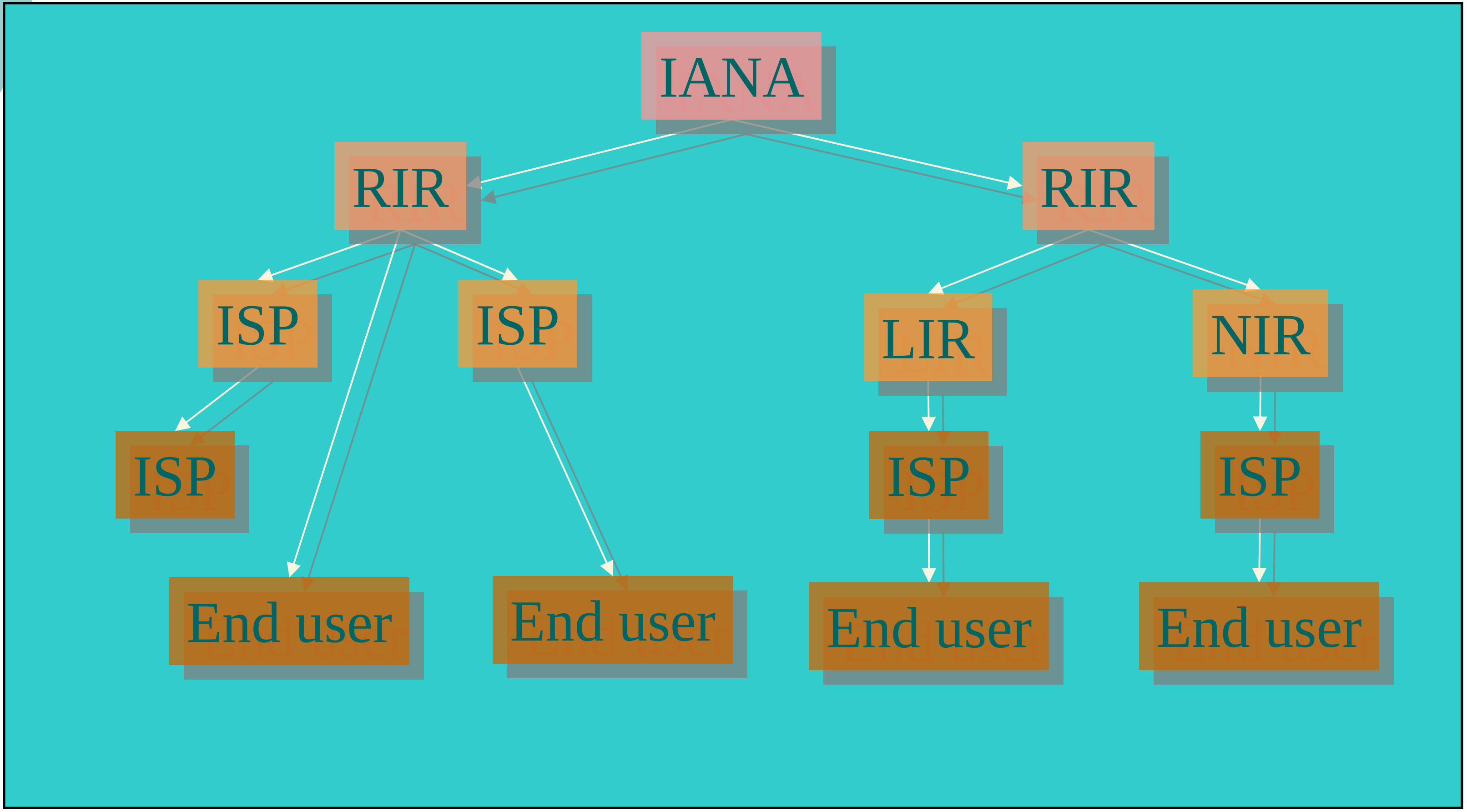
- the **<u>authenticity of the address object</u>** being advertised
- **<u>authenticity of the origin AS</u>**
- the **<u>explicit authority</u>** from the address to AS that permits an original routing announcement to be made by that AS

X.509 Extensions for IP Addresses

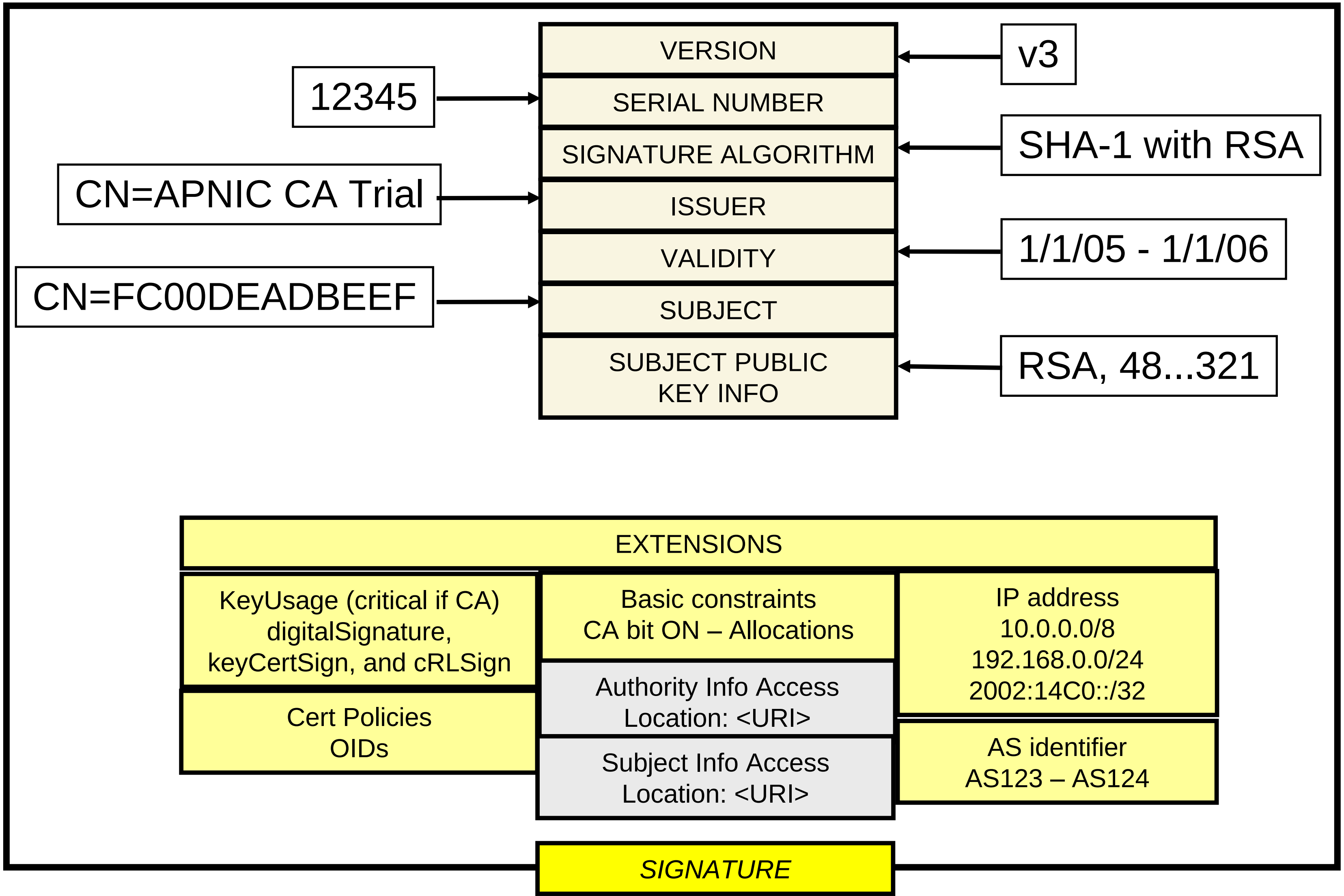
- RFC3779 defines extension to the X.509 certificate format for IP addresses & AS number
- The extension binds a list of IP address blocks and AS numbers to the subject of a certificate
- These extensions may be used to convey the issuer's authorization of the subject for exclusive use of the IP addresses and autonomous system identifiers contained in the certificate extension
- The extension is defined as as a critical extension
  - Validation includes the requirement that the Issuer's certificate extension **must** encompass the resource block described in the extension of the certificated being validated

RFC3779 summary

The certificate chain will reflect the delegation hierarchy, from IANA down to the end users



Certificate Format



VERSION

SERIAL NUMBER

SIGNATURE ALGORITHM

ISSUER

VALIDITY

SUBJECT

SUBJECT PUBLIC KEY INFO

v3

12345

SHA-1 with RSA

CN=APNIC CA Trial

1/1/05 - 1/1/06

CN=FC00DEADBEEF

RSA, 48...321

EXTENSIONS

KeyUsage (critical if CA)
digitalSignature,
keyCertSign, and cRLSign

Basic constraints
CA bit ON – Allocations

IP address
10.0.0.0/8
192.168.0.0/24
2002:14C0::/32

Cert Policies
OIDs

Authority Info Access
Location: <URI>

Subject Info Access
Location: <URI>

AS identifier
AS123 – AS124

SIGNATURE

What is being Certified

- APNIC (the "Issuer") certifies that:

  the certificate "Subject"

  whose public key is contained in the certificate

  is the current controller of a set of IP address and AS resources

  that are listed in the certificate extension

- APNIC is NOT certifying here the identity of the subject, nor their good (or evil) intentions!

What can you do with certificates?

- You can sign routing authorities, routing requests, or IRR submitted objects with your private key.
  - The recipient (relying party) can validate this signature against the matching certificate’s public key, and can validate the certificate in the PKI
- You can use the private key to sign routing information that could be propagated by a routing protocol
- You can issue signed subordinate certificates for any sub-allocations of resources

APNIC Certificate Trial

Trial service provides:

- Issue of RFC3779 compliant certificates to APNIC members
- Policy and technical infrastructure necessary to deploy and use the certificates in testing contexts by the routing community and general public
  - CPS (Certification practice statement)
  - Certificate repository
  - CRL (Certificate revocation list)
- Tools and examples (open source) for
  - downstream certification by NIR, LIR and ISP
  - display of certificate contents
  - encoding certificates

Current Status

- Test Certificates being generated
  - Locally generated key pair
  - Cover all current APNIC membership holdings
  - CRL test
    - Reissue all certificates with explicit revocation on original certificate set
- Example tools being developed
- APNIC Trial Certificate Repository:

  ftp://ftp.apnic.net/pub/test-certs/