

APNIC Trial of Certification of IP Addresses and ASes

RIPE 52 Plenary

George Michaelson
Geoff Huston

Motivation: 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

Motivation: 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?

Can these questions be answered reliably, quickly and cheaply?

What would be good ...

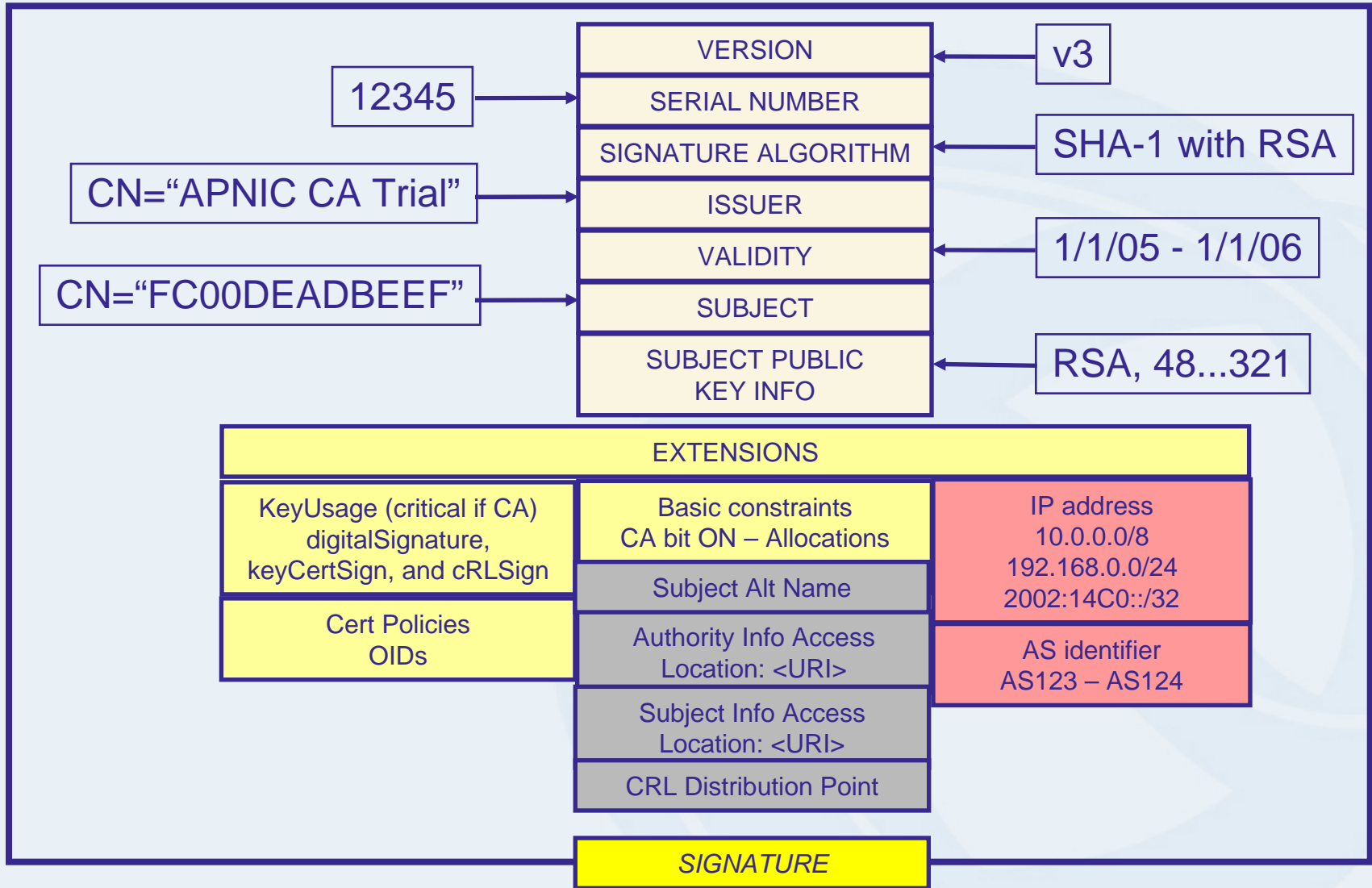
To be able to use a public infrastructure to validate assertions about addresses and their use:

- the **authenticity of the address object** being advertised
- **authenticity of the origin AS**
- the **explicit authority** 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

APNIC Trial Certificate Format



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!
- This is a simple mechanism of using certificates as a means of validation of ‘title’ of current resource control

What could you do with Resource Certificates?

- You could 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 could use the private key to sign routing information that could then be propagated by an inter-domain routing protocol that had validation extensions
- You could issue signed subordinate resource certificates for any sub-allocations of resources, such as may be seen in a LIR context

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

Expected Environment of Use

Service interface via APNIC web portal

- Generate and Sign routing requests

- Validate signed objects against repository

- Manage subordinate certificates

Local Tools – LIR Use

- Synchronize local repository

- Validate signed resource objects

- Generate and lodge certificate objects

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/>

Current APNIC Experiment Program

Now (2006)

- Certificate design
- Tool construction
- Use modelling
- Portal Tools and Local Use Tools

Next (late 2006)

- Review and Evaluation
- Definition Next Steps