# APNIC Trial of Certification of IP Addresses and ASes

RIPE 51
11 October 2005

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 entirely robust forms of defence against these vulnerabilities

# Address and Routing Security

The basic routing payload 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?
- Is the forwarding path to reach this address prefix an acceptable representation of the network's forwarding state?

# What would be good …

To use a public key infrastructure to support attestations 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

# What would also be good…

- If the attestation referred to the address allocation path (IANA to RIR to LIR to…)
  - use of an RIR issued certificate to validate the attestation signature chain
- If the attestation was associated with the route advertisement
  - such attestations to be carried in BGP as an Update attribute
- If validation these attestations was treated as a route object preference indicator
  - attestation validation to be a part of the BGP route acceptance process

# A Starting Point for Routing Security

Adoption of some basic security functions into the Internet's routing domain:

- Injection of reliable trustable data
  - Address and AS certificate PKI as the base of validation of network data
- Explicit verifiable mechanisms for integrity of data distribution
  - Adoption of some form of certification mechanism to support validation of distribution of address and routing information

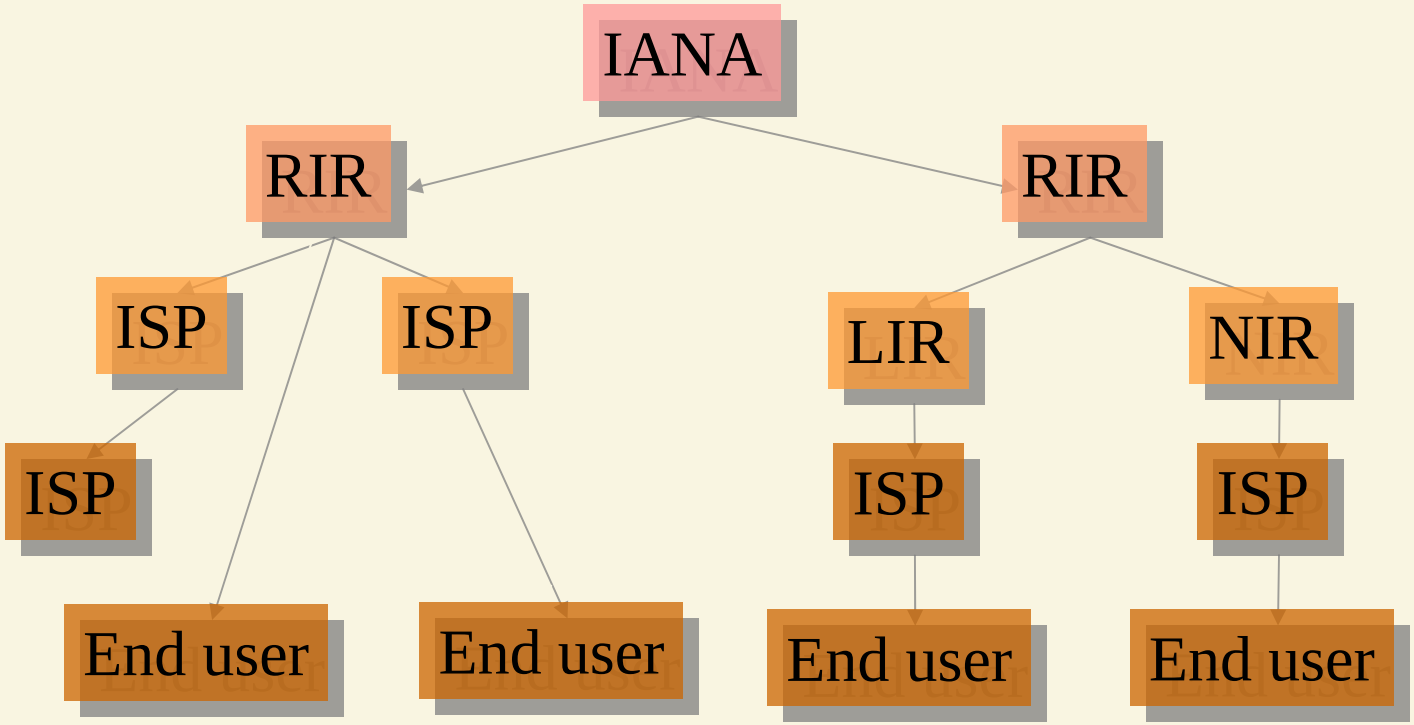


# X.509 Extensions for IP Addresses

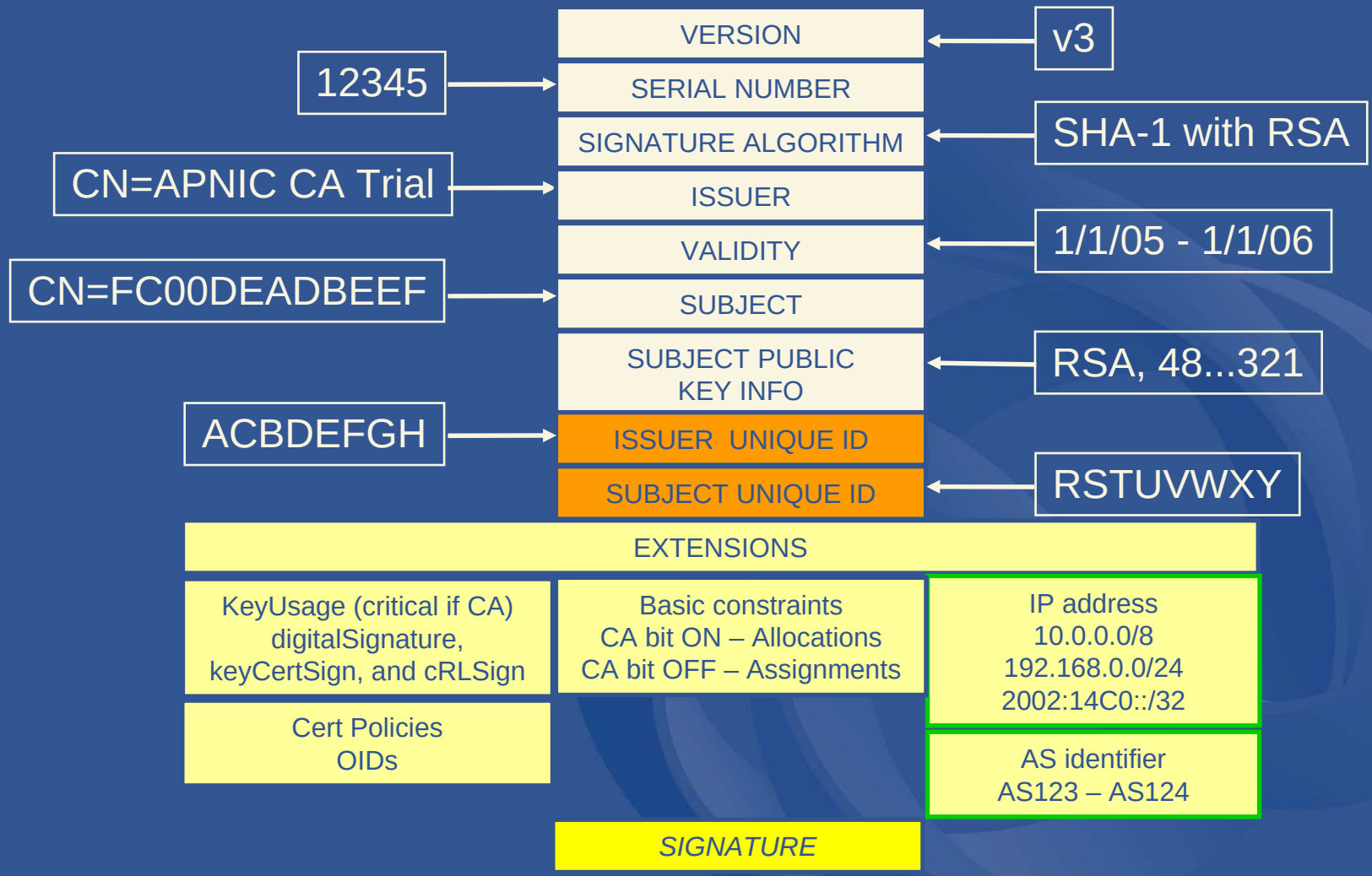
- RFC3779 defines extension to the X.509 certificate format for IP addresses & AS number
- The extension binds a list of IP address blocks and AS numbers to the subject of a certificate
- The extension specifies that the certification authority hierarchy should follow the IP address and AS delegation hierarchy
  - Follows IANA ⇒ RIR ⇒ LIR
    - And all their downstream delegations
- 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

# RFC3779 summary

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



# 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 does NOT certify the identity of the subject, nor their good (or evil) intentions!

# What can you do with certificates?

- You can sign routing authorities or routing requests with your private key. The recipient can validate this signature against the matching certificate's public key
- You can use the private key to sign routing information that is propagated by a routing protocol
- You can issue signed derivative certificates for any sub-allocations of resources



# APNIC Certificate Project Phases

- Trial – 4Q 2005
  - Early adopters, s/w developers, protocol designers
  - Major requirement changes allowed
    - Certificate formats may change
- Pilot – 1Q 2006
  - Input from trial used to test service
  - Wider deployment
  - Minor requirement changes allowed
    - Certificate format should be stable
- Full service – 2Q 2006
  - General service availability
  - Full policy and procedures in place

# 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

# Notes (1)

- APNIC Certificate is an APNIC Member Service
  - Certificates issued as a service to APNIC members
  - Certificate lifetime tied to current membership
- Certificate Subject Name
  - Uses unique HEX string of encoded 40 bit value
    - Constant across various entity name events
    - Consistent label for entity relationship with APNIC
    - Reverse reference to be loaded into WHOIS record (future)
- Not General Purpose Certificates
  - Certificates are not trusted confirmation of identity or bona fides claims
  - Certificates limited to confirmation of association of IP resources with private key holder
- CA Bit is SET
  - Subject may issue sub-certificates describing further sub-allocations of resources

# Notes (2)

- APNIC certify LIR sub-delegations?
  - NO - only warrant relationship with LIR, existance of resource allocation to that LIR from APNIC
- RFC3779 Compliance
  - Use a subset of 3779 options
    - Avoid IP ranges and use only CIDR spanning sets
- APNIC Root CA
  - Current trial uses a certificate root at APNIC
- 2 Certificate Repositories
  - APNIC-Issued Certificates
  - APNIC-Issued plus derived sub-allocation certificates that are lodged with APNIC
  - Access via OCSP, FTP, RSYNC,…
- Compatibility with related work
  - Ensure that these certificates can be used to feed into sBGP or soBGP or ?

# 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/

# Questions?