Summary Report on Resource Certification

February 2007

Geoff Huston
Chief Scientist
APNIC
Objective

• To create a robust framework that allows validation of assertions relating to IP addresses and ASNs and their use

and

• To make it easier for anyone to see if someone is lying about actual control over addresses and/or routing!
Uses

• Signing of IRR entries
  “Yes, I am the right-of-use holder and that’s precisely the information I entered into the IRR.”

• Signing of Routing Origination
  “Yes, I am the right-of-use holder for this address prefix and I am permitting ASx to originate a route to this address prefix.”

• Signing of Route Requests
  “Please route address prefix a.b.c.d/x through customer interface xxx.”
Resources for this work

- APNIC’s allocation database
- Public / Private key technology
- X.509 v3 certificate technology
- IP resource extensions to X.509 v3 certificates
- PKI models and trust relationships
The Overall Objective

• To support a PKI that mirrors the existing resource allocation state
  – Every resource allocation can be attested by a matching certificate that binds the allocated resource with the resource issuer and recipient

• To use these resource certificates to make signed assertions that can be validated through this PKI
Trial Activity Status

- Specification of X.509 Resource Certificates
- Generation of resource certificate repositories aligned with existing resource allocations and assignments
- Tools for Registration Authority / Certificate Authority interaction (undertaken by RIPE NCC)
- Tools to perform validation of resource certificates Extensions to OpenSSL for Resource Certificates (open source development activity, supported by ARIN)

Current Activities
- Tools for resource collection management, object signing and signed object validation (APNIC, and also open source development activity, supported by ARIN)
- LIR / ISP Tools for certificate management
- Testing, Testing, Testing
- Operational service profile specification

Working notes and related material we’ve been working on in this trial activity:
http://mirin.apnic.net/resourcecerts
Focus points for Q1 2007

• Can we design the certificate management subsystem to be an largely automated “slave” of the resource allocation function?
• Provide a toolset to allow IRs to manage certificate issuance
• Use the same toolset to provide “hosted” certificate services
Focus points for Q1 2007

- Defining the components and interactions of a “certificate engine”
Focus points for Q1 2007

• Automated certificate issuance
• Client-side tools that allow certificate management to be ‘out-sourced’
• Considerations of splits, mergers and resource transfers
Next Steps

• Development of the Certificate Engine
• End Entity Certificates
• Tools for Relying Parties
• Evaluation of Progress
Thank You

http://mirin.apnic.net/resourcecerts

Questions?