Progress 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
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  RIPE NCC  ARIN

APNIC  LACNIC

NIR1  NIR2

ISP1  ISP2  ISP3  ISP4  ISP  ISP  ISP
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

NIR1  NIR2

ISP1  ISP2  ISP3  ISP4  ISP  ISP  ISP

Issued Certificates match allocation actions
Resource Certificates

Resource Allocation Hierarchy

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key-pub>
Signed: <apnic-key-priv>
Resource Certificates

Resource Allocation Hierarchy

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key-pub>
Signed: <apnic-key-priv>

Issuer: NIR2
Subject: ISP4
Resources: 192.2.200.0/24
Key Info: <isp4-key-pub>
Signed: <nir2-key-priv>

Issued Certificates
Resource Certificates

Issuer: APNIC
Subject: NIR2
Resources: 192.2.0.0/16
Key Info: <nir2-key>
Signed: <apnic-key-priv>

Issuer: NIR2
Subject: ISP4
Resource: 192.2.200.0/22
Key Info: <isp4-key>
Signed: <nir2-key-priv>

Issuer: ISP4
Subject: ISP4-EE
Resources: 192.2.200.0/24
Key Info: <isp4-ee-key>
Signed: <isp4-key-priv>
Use: Routing Authority

Resource Allocation Hierarchy

IANA

AFRINIC RIPE NCC ARIN

APNIC LACNIC

NIR1 NIR2

Issued Certificates

Route Origination Authority

“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”
Signed Objects

Resource Allocation Hierarchy

IANA

AFRINIC RIPE NCC ARIN

APNIC LACNIC

NIR1 NIR2

ISP3 ISP4 ISP ISP ISP

Issued Certificates

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>
Signed Object Validation

Resource Allocation Hierarchy

IANA

AFRINIC
RIPE NCC
ARIN

APNIC
LACNIC

Issued Certificates

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>

1. Did the matching private key sign this text?
Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>
Signed,
ISP4 <isp4-ee-key-priv>

2. Is this certificate valid?
Signed Object Validation

Resource Allocation Hierarchy

IANA

AFRINIC RIPE NCC ARIN

APNIC LACNIC

APNIC Trust Anchor

Issued Certificates

APNIC Trust Anchor

3. Is there a valid certificate path from a Trust Anchor to this certificate?

Route Origination Authority

“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>
Signed Object Validation

Validation Outcomes

1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a valid address, derived from an APNIC allocation
3. ISP4 holds a current right-of-use of 192.2.200.0/24
4. A route object, where AS65000 originates an advertisement for the address prefix 192.2.200.0/24, has the explicit authority of ISP4, who is the current holder of this address prefix

Resource Allocation Hierarchy

IANA

AFRINIC
RIPE NCC
ARIN
RIPE NCC
LACNIC

LIR1
LIR2

ISP
ISP
ISP
ISP
ISP
ISP
ISP

Route Origination Authority
“ISP4 permits AS65000 to originate a route for the prefix 192.2.200.0/24”

Attachment: <isp4-ee-cert>

Signed,
ISP4 <isp4-ee-key-priv>
Example of a Signed Object

netnum-set: RS-TELSTRA-AU-EX1
descr:      Example routes for customer with space under apnic
members:  58.160.1.0-58.160.16.255, 203.34.33.0/24
tech-c:     GM85-AP
admin-c:    GM85-AP
notify:     test@telstra.net
mnt-by:     MAINT-AU-TELSTRA-AP
sigcert:    rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q/Hc4yxwhTamNXW-cDwtQcmvOVGjU.cer
sigblk:     -----BEGIN PKCS7-----
    MIIBdQYJKoZIhvcNAQcCoIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHA...8KJYFWl7+rQmRf4F0m5oLWBHnjuX2E89q0f2ywvITTNg31ywqBoAqmmDhDy+nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV02I2HbMI1SrXM5nQ0xyYG3Pcxo/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
    -----END PKCS7-----
changed:    test@telstra.net 20060822
source:     APNIC
<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Serial</td>
<td>1</td>
</tr>
<tr>
<td>Issuer</td>
<td>CN=telstra-au</td>
</tr>
<tr>
<td>Validity: Not Before</td>
<td>Fri Aug 18 04:46:18 2006 GMT</td>
</tr>
<tr>
<td>Validity: Not After</td>
<td>Sat Aug 18 04:46:18 2007 GMT</td>
</tr>
<tr>
<td>Subject</td>
<td>CN=An example sub-space from Telstra IANA, E=<a href="mailto:apnic-ca@apnic.net">apnic-ca@apnic.net</a></td>
</tr>
<tr>
<td>Subject Key Identifier g(SKI)</td>
<td>Hc4yxwhTarnXWy-cDwtQcmvOVGjU</td>
</tr>
<tr>
<td>Subject Info Access:</td>
<td>caRepository –</td>
</tr>
<tr>
<td></td>
<td>rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5</td>
</tr>
<tr>
<td></td>
<td>Ck010p5Q/Hc4yxwhTarnXWy-cDwtQcmvOVGjU</td>
</tr>
<tr>
<td>Key Usage</td>
<td>DigitalSignature, nonRepudiation</td>
</tr>
<tr>
<td>CRL Distribution Points:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5</td>
</tr>
<tr>
<td></td>
<td>Ck010p5Q.cr1</td>
</tr>
<tr>
<td>Authority Info Access:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>caIssuers –</td>
</tr>
<tr>
<td></td>
<td>rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5</td>
</tr>
<tr>
<td></td>
<td>Ck010p5Q.cer</td>
</tr>
<tr>
<td>Authority Key Identifier:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck010p5Q</td>
</tr>
<tr>
<td>Certificate Policies:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.3.6.1.5.5.7.14.2</td>
</tr>
<tr>
<td>IPv4</td>
<td>58.160.1.0-58.160.16.255, 203.34.33.0/24</td>
</tr>
</tbody>
</table>
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
  – Query / Response interaction between registry and registry clients:
    • **List**: What resources have been allocated to me and what’s the corresponding state of issued certificates?
    • **Issue**: Here is a certificate request – please issue me with a certificate that matches my allocated resource set
    • **Remove**: Please revoke certificates issued with this public key
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?