Using Resource Certificates
Progress Report on the Trial of Resource Certification

November 2006

Geoff Huston
APNIC
What would be good …

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

- Publish routing authorities authored by a resource holder that cannot be altered or forged

- Allow third parties to authenticate that an address or routing assertion was made by the current right-of-use holder of the number resource
What would be even gooder …

• Is to have a reliable, efficient, and effective way to underpin the integrity of the Internet’s address resource distribution structure and our use of these resources in the operational Internet

• Is to replace various forms of risk-prone assertions, rumours, implicit trust and fuzzy traditions about addresses and their use with demonstrated validated authority
Resource Certificate Trial

Approach:
- Use X.509 v3 Public Key Certificates (RFC3280) with IP address and ASN extensions (RFC3779)

Parameters:
- Use existing technologies where possible
- Leverage on existing open source software tools and deployed systems
- Contribute to open source solutions and open standards

OpenSSL as the foundational platform
- Add RFC3779 (resource extension) support

Design of a Certification framework
- anchored on the IP resource distribution function
Resource Public Key Certificates

The certificate’s Issuer certifies that:

the certificate’s Subject

whose public key is contained in the certificate

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

that are listed in the certificate’s resource extension

This is not an attestation relating to identity or role – it is an attestation that in effect binds a private key to a right-of-use of a number resource collection

This is not an attestation about any form of related routing policies
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

LIR1  LIR2

ISP  ISP  ISP  ISP  ISP  ISP  ISP  ISP
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  RIPE NCC  ARIN

APNIC  LACNIC

NIR1  NIR2

ISP  ISP  ISP  ISP  ISP  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

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>
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC

RIPE NCC

ARIN

APNIC

LACNIC

NIR1

NIR2

ISP

ISP

ISP

ISP

ISP

ISP

ISP

ISP

ISP

ISP

ISP

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

Issuer: NIR2
Subject: ISP4
Resources: 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>
Base Object in a Routing Authority

Context

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

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?
Signed Object Validation

Resource Allocation Hierarchy

IANA

AFRINIC  RIPE NCC  ARIN  APNIC  LACNIC

LIR1  NIR2

ISP  ISP  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>

2. Is this certificate valid?
Signed Object Validation

Resource Allocation Hierarchy

IANA

AFRINIC
RIPE NCC
ARIN

APNIC
LACNIC

LIR1
NIR2

ISP
ISP
ISP
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>

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

Resource Allocation Hierarchy

IANA

AFRINIC

RIPE NCC

ARIN

RIPE NCC

LACNIC

LIR1

LIR2

ISP4

ISP

ISP

ISP

ISP

ISP

Issued Certificates

Resource Allocation Hierarchy

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>

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
### Example of a Signed Object

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>netnum-set</td>
<td>RS-TELSTRA-AU-EX1</td>
</tr>
<tr>
<td>descr</td>
<td>Example routes for customer with space under apnic</td>
</tr>
<tr>
<td>members</td>
<td>58.160.1.0-58.160.16.255,203.34.33.0/24</td>
</tr>
<tr>
<td>tech-c</td>
<td>GM85-AP</td>
</tr>
<tr>
<td>admin-c</td>
<td>GM85-AP</td>
</tr>
<tr>
<td>notify</td>
<td><a href="mailto:test@telstra.net">test@telstra.net</a></td>
</tr>
<tr>
<td>mnt-by</td>
<td>MAINT-AU-TELSTRA-AP</td>
</tr>
<tr>
<td>sigcert</td>
<td>rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q/Hc4yxwhTamNXW-cDWithQcmvOVGjU.cer</td>
</tr>
<tr>
<td>sigblk</td>
<td>-----BEGIN PKCS7-----</td>
</tr>
</tbody>
</table>

```
MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHAQCCBhgMAgEBMBowFTETMBEGA1UEAxMKdGVsc3RY1hdQIBATAJBgUr
DgMCGgUAMAOQCSqGSIb3DQEBAQUABIIBAEZGI2dAG3lAAGi+mAK/S5bsNrgEHOmN
1leJF9aqM+jVO+tiCvRHyPMemPi6yoCm2h5RCR/avP40U4CC3QMhU98tw2Bq0TY
HZvqXfAOVhjD4Ap4xKjiAyr8tfeC7ZDh0+fpvsysdV2XXtHljwjcL4GvM/gES6dJ
KJYFwWr7rPqQmFTFm5oLWBhNjuxZE889qf2ZVizITTN31ynwqBoAqmmDhDy
+nsRVAXax7II2iQDTr/pjI2VWe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV02I2HbMI
1SvRXMx5nQOXyY3G3Px0/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
```

-----END PKCS7-----

<p>| changed     | <a href="mailto:test@telstra.net">test@telstra.net</a> 20060822                                       |
| source      | APNIC                                                           |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version:</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Serial:</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Issuer:</strong></td>
<td>CN=telstra-au</td>
</tr>
<tr>
<td><strong>Validity:</strong>&lt;br&gt;<strong>Not Before:</strong></td>
<td>Fri Aug 18 04:46:18 2006 GMT</td>
</tr>
<tr>
<td><strong>Validity:</strong>&lt;br&gt;<strong>Not After:</strong></td>
<td>Sat Aug 18 04:46:18 2007 GMT</td>
</tr>
<tr>
<td><strong>Subject:</strong></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><strong>Subject Key Identifier g(SKI):</strong></td>
<td>Hc4yxwhTamNXW-cDWtQcmvOVGjU</td>
</tr>
<tr>
<td><strong>Subject Info Access:</strong></td>
<td>caRepository –&lt;br&gt;rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU</td>
</tr>
<tr>
<td><strong>Key Usage:</strong></td>
<td>DigitalSignature, nonRepudiation</td>
</tr>
<tr>
<td><strong>CRL Distribution Points:</strong></td>
<td>rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q.crl</td>
</tr>
<tr>
<td><strong>Authority Info Access:</strong></td>
<td>caIssuers –&lt;br&gt;rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q.cer</td>
</tr>
<tr>
<td><strong>Authority Key Identifier:</strong></td>
<td>Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck010p5Q</td>
</tr>
<tr>
<td><strong>Certificate Policies:</strong></td>
<td>1.3.6.1.5.5.7.14.2</td>
</tr>
<tr>
<td><strong>IPv4:</strong></td>
<td>58.160.1.0-58.160.16.255, 203.34.33.0/24</td>
</tr>
</tbody>
</table>
Trial 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

Current Activities
🌟 Extensions to OpenSSL for Resource Certificates (open source development activity, supported by ARIN)
🌟 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/resoursecerts