Using Resource Certificates
Progress Report on the Trial of Resource Certification

October 2006

Geoff Huston
APNIC
4:30 pm

Mail:

Geoff, mate,

I’ve been dealing with your phone people and I’m getting nowhere – could you route xxx/24 for me this afternoon? I’ve got a customer on my back and I need this done by 5 today, and I’m getting desperate.
Sound Familiar?

4:30 pm
Mail:
Geoff, mate,
I’ve been dealing with your phone people and I’m getting nowhere – could you route xxx/24 for me this afternoon? I’ve got a customer on my back and I need this done by 5 today, and I’m getting desperate.

7:00pm
Trouble Ticket:
Customer complaining that they have been disconnected. The circuit is up, but the customer is complaining that there is no traffic.
4:30 pm
Mail:
  Geoff, mate,
  I’ve been dealing with your phone people and I’m getting nowhere – could you route xxx/24 for me this afternoon? I’ve got a customer on my back and I need this done by 5 today, and I’m getting desperate.

7:00 pm
Trouble Ticket:
  Customer complaining that they have been disconnected. The circuit is up, but the customer is complaining that there is no traffic.

9:30 am
Mail:
  Product Manager:
  We’ve had a complaint with a customer threatening legal action over some kind of address dispute. We have a call with legal this afternoon at 2:00 – details below.
If only….

• I could’ve quickly and accurately figured out who really had the right-of-use of the address block at the time

• I could’ve asked for a signed route origination that gave me (ASx) an authority to route prefix xxx that I could validate independently
Motivation: Address and Routing Security

The (very) basic routing security questions that need to be answered are:

– Is this a valid address prefix?

– Who advertised this address prefix into the network?

– Did they have the necessary credentials to advertise this address prefix?

– Is the advertised path authentic?
What would be good …

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

– Allow third parties to authenticate that an address or routing assertion was made by the current right-of-use holder of the address resource

– Confirm that the asserted information is complete and unaltered from the original

– Convey routing authorities from the resource holder to a nominated party that cannot be altered or forged
What would be good ...

- 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 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
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*
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  APNIC  RIPE NCC  ARIN  LACNIC

LIR1  LIR2

ISP  ISP  ISP  ISP  ISP  ISP  ISP  ISP
Resource Certificates

Resource Allocation Hierarchy

IANA

AFRINIC  APNIC  RIPE NCC  ARIN  LACNIC

ISP  ISP  ISP  ISP  ISP  ISP  ISP  ISP

Issued Certificates match allocation actions
Resource Certificates

Resource Allocation Hierarchy

Issuer: ARIN
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <lir2-key-pub>
Signed: <arin-key-priv>
Resource Certificates

Issuer: ARIN
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <lir2-key-pub>
Signed: <arin-key-priv>

Issuer: LIR2
Subject: ISP4
Resources: 192.2.200.0/24
Key Info: <isp4-key-pub>
Signed: <lir2-key-priv>
Resource Certificates

Resource Allocation Hierarchy

Issuer: ARIN
Subject: LIR2
Resources: 192.2.0.0/16
Key Info: <lir2-key>
Signed: <arin-key-priv>

Issuer: LIR2
Subject: ISP4
Resources: 192.2.0.0/16
Key Info: <isp4-key>
Signed: <lir2-key-priv>

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

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
APNIC
RIPE NCC
ARIN
LACNIC

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>
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?
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
APNIC
RIPE NCC
ARIN
LACNIC
LIR1
LIR2
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>

Validation Outcomes

1. ISP4 authorized this Authority document
2. 192.2.200.0/24 is a valid address
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
What could you do with Resource Certificates?

**Issue** signed subordinate resource certificates for any sub-allocations of resources, such as may be seen in a LIR context

Maintain a certificate collection that matches the current resource allocation state
What could you do with Resource Certificates?

**Sign** routing authorities, routing requests, or WHOIS objects or IR objects with your private key

Use the private key to sign attestations with a signature that is associated with a right-of-use of a resource

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>
What could you do with Resource Certificates?

**Validate** signed objects

*Authentication*: Did the resource holder really produce this document or object?

*Authenticity*: Is the document or object in exactly the same state as it was when originally signed?

*Validity*: Is the document valid today?

– A relying party can:
  • authenticate that the signature matches the signed object,
  • validate the signature against the matching certificate’s public key,
  • validate the certificate in the context of the Resource PKI
Example of a Signed Object

route-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-AUIANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU.cer

sigblk: -----BEGIN PKCS7-----
MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHATGCAUEwggE9AgEBMBowFTETMBEGA1UEAxMKdGVsc3RyYS1hdQIBATAJBgUr
DgMCGgUAMA0GCSqGSIb3DQEBAQUABIIBAEZGI2dAG31AAGi+mAK/S5bsNrgEH0mN
1leJF9aqM+jVO+tiCvRhyPMeBMiP6yoCm2h5RCR/avP40U4CC3QMhU98tw2BqOTY
HZvqXfa0Vhjd4Ap4xKjiAyr8tfeC7ZDho+fpvsydV2XXtHivjwcL4GvM/gES6dJ
KJYFWW1rPqQnfTFMm5oLWBHnJuxX2E89qyQf2YVizITTN3y1nwqBoAqmmDhDy
+nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV0ZI2HbMI
1SvRXMx5nQOXyYG3Pcxo/PAhBbKvkfudLki/IzB3j+4M8KemrnVMRo=
-----END PKCS7-----

changed: test@telstra.net 20060822
source: APNIC
Signer’s certificate

Version: 3
Serial: 1
Issuer: CN=telstra-au
Subject: CN=An example sub-space from Telstra IANA, E=apnic-ca@apnic.net
Subject Key Identifier g(SKI): Hc4yxwhTamNXW-cDWTQcmvOVGjU
Subject Info Access: caRepository –
    rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q/Hc4yxwhTamNXW-cDWTQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
    rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q.crl
Authority Info Access: caIssuers –
    rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5Ck010p5Q.cer
Authority Key Identifier:
    Key Identifier g(AKI): cbh3Sk iwj8Yd8uqaB5Ck010p5Q
Certificate Policies: 1.3.6.1.5.5.7.14.2
IPv4: 58.160.1.0-58.160.16.255, 203.34.33.0/24
Potential Scenarios

Service interface via a Web Portal:
- Generate and Sign routing-related objects
- Validate signed objects against the PKI
- Manage subordinate certificate issuance
  (Automated certificate management processes)

Local Tools – LIR Use
- Local repository management
- Resource object signing
- Generate and lodge certificate objects
Resource Certificate Trial Program

- 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
- Operational service profile specification
Next Steps …

1. Complete current trial activities by EOY 06
2. APNIC Evaluation of Trial activities
   - Status of work items
   - Does this approach meet the objectives?
   - What are the implications of this form of certification of resources?
   - Impact assessment
     • Service infrastructure, operational procedures
     • Utility of the authentication model
     • Policy considerations
   - Recommendations for production deployment
Credit where credit is due…..

• The design and implementation team involved in this trial:
  – George Michaelson
  – Rob Loomans
  – Geoff Huston
  – Randy Bush
  – Rob Austein
  – Rob Kisteleki
  – Steve Kent
  – Russ Housley
Thank You

Questions?