Progress Report on APNIC Trial of Certification of IP Addresses and ASes

APNIC 22
September 2006

Geoff Huston

Motivation: Address and Routing Security

What we have today is a relatively insecure system that is highly vulnerable to various forms of deliberate disruption and subversion

And it appears that bogon filters and routing policy databases are not, in and of themselves, entirely robust forms of defence against these vulnerabilities

Motivation: Address and Routing Security

The (very) basic routing 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?

Can these questions be answered reliably, quickly and cheaply?

What would be good …

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

- Allow third parties to authenticate that an address or routing assertion was made by the 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

General Approach

- Use existing technologies as much as possible
- Leverage on existing open source software tools and deployed systems
- Develop open source solutions
- Contribute to open standards

- Use X.509 Public Key Certificates with IP address extensions, with OpenSSL as the tool foundation

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

- The certificate issuer is NOT certifying here the identity of the subject, nor their good (or evil) intentions!
- This is a simple mechanism of using certificates as a means of validation of a "right-of-use" of a resource collection

What could you do with Resource Certificates?

- Sign routing authorities, routing requests, or WHOIS objects or IR objects with your private key
  - The recipient (relying party) can authenticate the signed object, and then validate this signature against the matching certificate's public key, and can validate the certificate in the context of the Resource PKI
- Issue signed subordinate resource certificates for any sub-allocations of resources, such as may be seen in a LIR context
- 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?

Potential Use Scenario

Service interface via APNIC web portal:

- Generate and Sign routing-related objects
- Validate signed objects against the PKI
- Manage subordinate certificate issuance

Local Tools – LIR Use

- Local repository management
- Resource object signing
- Generate and lodge certificate objects

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-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
             CkO1Op5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU.cer
sigblk:      -----BEGIN PKCS7-----
             MIIBdQYJKoZIhvcNAQcCoIIBZjCCAWICAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
             DQEHATGCAUEwggE9AgEBMBowFTETMBEGA1UEAxMKdGVsc3RyYS1hdQIBATAJBgUr
             DgMCGgUAMA0GCSqGSIb3DQEBAQUABIIBAEZGI2dAG3lAAGi+mAK/S5bsNrgEHOmN
             1leJF9aqM+jVO+tiCvRHyPMeBMiP6yoCm2h5RCR/avP40U4CC3QMhU98tw2Bq0TY
             HZvqXfAOVhjD4Apx4KjiAyr8tfeC7ZDhO+fpvsydV2XXtHIvjwjcL4GvM/gES6dJ
             KJYFWWlrPqQnfTFMm5oLWBUhNjuX2E89qyQf2YZVizITTNg3ly1nwqBoAqmmDhDy
             +nsRVAxax7II2iQDTr/pjI2VWfe4R36gbT8oxyvJ9xz7I9IKpB8RTvPV02I2HbMI
             1SvRXMx5nQOXyYG3Pcxo/PAhbBkVkgfudLki/IzB3j+4M8KemrnVMRo=
             -----END PKCS7-----
changed:     test@telstra.net 20060822
source:      APNIC
```

Signer's certificate

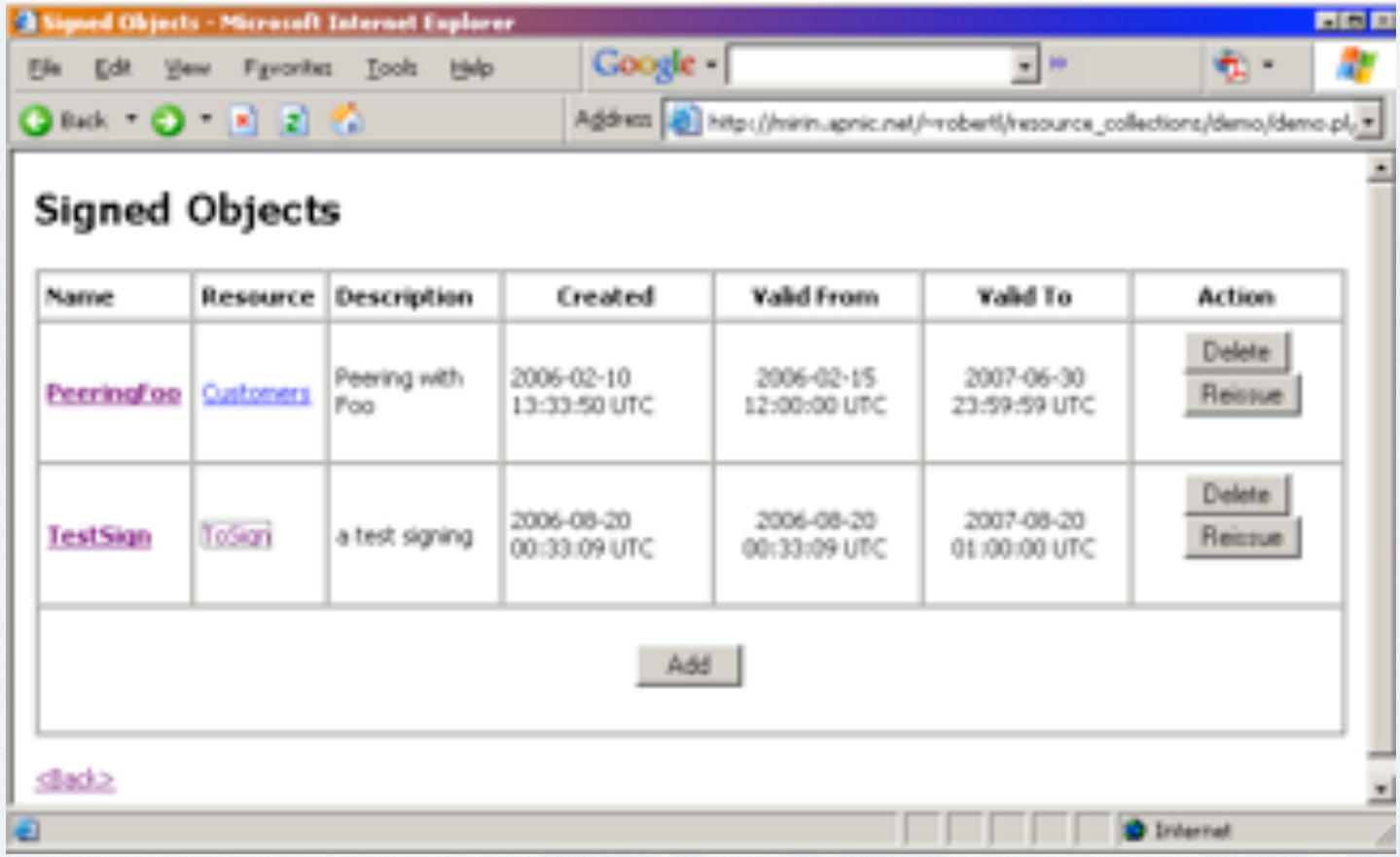
```
Version:   3 (0x3)
Serial:    1 (0x1)
Issuer:    CN=telstra-au
Validity:  Not Before: Fri Aug 18 04:46:18 2006 GMT
Validity:  Not After:  Sat Aug 18 04:46:18 2007 GMT
Subject:   CN=An example sub-space from Telstra IANA, E=apnic-ca@apnic.net
Subject Key Identifier g(SKI): Hc4yxwhTamNXW-cDWtQcmvOVGjU
Subject Info Access: caRepository -
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           Ck01Op5Q/Hc4yxwhTamNXW-cDWtQcmvOVGjU
Key Usage: DigitalSignature, nonRepudiation
CRL Distribution Points:
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           Ck01Op5Q.crl
Authority Info Access: caIssuers -
           rsync://repository.apnic.net/TELSTRA-AU-IANA/cbh3Sk-iwj8Yd8uqaB5
           Ck01Op5Q.cer
Authority Key Identifier:
           Key Identifier g(AKI): cbh3Sk-iwj8Yd8uqaB5Ck01Op5Q
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
```

Resource Signing Tool

Resources can be subdivided into “collections” and each collection can be named. This section of the portal provides tools to manage resource collections

A resource collection is used to sign a document (or any other digital object)

Resource Signing Tool



Documents can be signed with a resource collection, and associated validity dates. Signed objects can also be reissued and deleted

The underlying resource certificate generation and management tasks are not directly exposed in this form of the signing tool

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 (activity supported by ARIN)
- Tools for resource collection management, object signing and signed object validation
- LIR / ISP Tools for certificate management
- Operational service profile specification

Next Steps

- Complete current trial activities
- Review
  - 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