Resource Certificate
Provisioning Protocol

Geoff Huston
IETF 70
December 2007
Problem Statement

- How to automate the process of certificate issuance such that the issued certificate accurately tracks the current resource allocation status.
  - Avoid situations where
    - the issued certificate “overclaims” resources
    - The issued certificate “underclaims” resources
Scenario

Certificate Issuer → Internet Registry
Issues Resource Certificates

Certificate Subject → Resource Holder
Allocates / Assigns Addresses
Scenario

Certificate Issuer

Internet Registry

Issues Resource Certificates

Allocates / Assigns Addresses

Resource Certificate Provisioning Protocol

Certificate Subject

Resource Holder
Protocol Characteristics

- Simple Client / Server protocol using a request / response interaction over a secure reliable channel
Protocol Payload

- **Cryptographic Message Syntax (CMS)**
  - SignedData object type
    - Include Signing Time in the CMS wrapper
    - Include CMS signing cert in the CMS wrapper

- **XML Data Objects**
  - Carried as CMS payload
XML Message Structure

```xml
<?xml version="1.0" encoding="UTF-8"?>
<message xmlns="http://www.apnic.net/specs/rescerts/up-down/"
    version="1"
    sender="sender name"
    recipient = "recipient name"
    type="message type">
    [payload]
</message>
```
Messages

- Query
- Issue
- Revoke
Query Message

- **Request:** type="list"

- **Response:**
  - List of Resource “classes”
    - List of allocated / assigned Number Resources within this class
    - Issued certificate(s) for this class
Issue Message

- **Request:** type="issue"
  - Payload: Resource “class” name
    - PKCS#10 Certificate Request

- **Response:**
  - Payload: Issued certificate
Revoke Message

- **Request:** type="revoke"
  - Payload: Resource “class” name
  - Subject’s public key

- **Response:**
  - Payload: confirmation of revocation
Error Responses

- Error status returned when the request could not be performed
Protocol Specification

Current (unsubmitted) draft is:

http://www.potaroo.net/drafts/draft-ietf-sidr-rescerts-provisioning-00.html
Next Steps

- Adoption of the specification of this provisioning protocol as a SIDR WG Document?