RPKI Standards Activity

Geoff Huston
APNIC
February 2010
IETF Activity

• Secure inter-Domain Working Group (SIDR)
  – chartered April 2006
  – Charter:
    http://www.ietf.org/dyn/wg/charter/sidr-charter.html
  – Focus:
    • formulate an extensible architecture for an interdomain routing security framework
    • Document the use of certification objects within this secure routing architecture
    • Document specific routing functionality modules within this architecture that are designed to address specific secure routing requirements as they are determined by the RPSEC Working Group
SIDR Activities

Architecture

– define the use of X.509 certificates and an associated PKI, and intended uses of this PKI
– Allows third parties to test assertions made about IP addresses and AS numbers and their use through the use of a validation framework relating to the association of the legitimate current holder of the number resource with the assertion

Documents:
draft-ietf-sidr-arch-09.txt

architecture of the PKI
SIDR Activities

Certification Framework

- certificate format
- certificate semantics
- certificate issuance, management and validation
- certificate policy statement
- template certificate practice statements

Documents:

draft-ietf-sidr-res-certs-17.txt
  certificate format, semantics, issuance, management and validation
draft-ietf-sidr-rpki-algs-00.txt
  common algorithm and key size specification
draft-ietf-sidr-ta-02.txt
  proposed structure for publication of trust anchor material
draft-ietf-sidr-cp-08.txt
  certificate policy statement
draft-ietf-sidr-cp-isp-03.txt
  template certificate practice statement: Internet Service Provider
draft-ietf-sidr-cp-irs-04.txt
  template certificate practice statement: Internet Registry
SIDR Activities

Certificate Repository Management

– certificate issuance and management
– certificate publication practice

Documents:

draft-ietf-sidr-rescerts-provisioning-05.txt
  certificate issuance and management protocol specification

draft-ietf-sidr-repos-struct-03.txt
  specification of the structure and contents of certificate repositories

draft-ietf-sidr-rpki-manifests-06.txt
  specification of the manifest structure for certificate repositories
SIDR Activities

**Validation of Route Origination**

- Definition of a signed object that would allow a relying party to determine if the holder of a given address prefix has authorized an AS to originate a route for the prefix

Documents:

- draft-ietf-sidr-roa-format-06.txt
  - syntax of a route origin authorization
- draft-ietf-sidr-roa-validation-03.txt
  - semantics of a route origin authorization object, and validation
SIDR Activities

Validation of *RPSL Objects*

– specification of a Resource PKI signature format that is compatible with the RPSL object format, allowing RPSL objects to be validated against the Resource PKI

Documents:

draft-ietf-sidr-rpsl-sig-01.txt

signature format for RPSL objects
Related Topics in Securing Inter-Domain Routing

In no particular order:

• Securing a BGP session
  – BOP is to use passwords and MD5 on the TCP session, and the issue of MD5 key rollover remains outstanding

• Methods of validating the identity of the remote BGP speaker in a BGP peering session

• A credential framework to allow a BGP speaker to validate that the information contained in the AS PATH attribute of a BGP Update represents the intended forwarding path associated with the Route Object

• Partial Deployment scenarios and forced Relying party assumptions relating to invalidity

• Validation Lifetimes and synchronization of change in validation credentials and route object validity

• Implementing RPSS in RPSL using the RSPL signature mechanism

• *Integrity of intent* vs *Integrity of Protocol Operation* – securing routing policy as distinct from securing routing protocols