# A Profile for Bogon Origin Attestations (BOAs)

draft-huston-sidr-bogons.00.txt

Geoff Huston

SIDR WG IETF 71

March 2008

# Bogons and BOAs

- Currently the Routing table contains over 500 prefixes and 330 AS numbers which have no current authoritative registration record (Bogons)

  [See http://www.cidr-report.org for today's list of Bogons]

- BOAs provide a validated means for a Relying Party to determine whether a given prefix or a given origination AS is a Bogon, and should not be used as part of the local routing set

# Semantic Intent of a BOA

"As the current right-of-use holder of the IP addresses and AS numbers listed here, I attest that **no** party has been authorized to use these resources in the context of the public Internet."

Provides a mechanism for "active denial" of a route object

# Potential BOA Issuers

- IANA: An IANA-issued BOA would contain those resources that have not been allocated to any RIR or for any special use in the public network
- RIRs: Those resources that have not been allocated or assigned to any LIR / NIR or ISP
- NIRs / LIRs: Those resources that have not been assigned to any ISP
- ISP: Those resources that are not announced into the routing system

# BOA Structure

Modelled on a ROA:

- CMS signed-data object
- Payload is a list of IP addresses and AS Numbers
- Signed by an RPKI EE certificate

# BOA Validation

- Syntactic correctness
- IP Resources in EE Certificate precisely match the IP Resources in the BOA
- EE certificate is valid in the context of the RPKI

# BOA Issuance

- Each IR should regularly issue a BOA for all unassigned / unallocated resources
- Each ISP may regularly issue a BOA for all unrouted resources
- The EE Certificate should be a one-off use EE certificate
- Suggest a daily issuance cycle with a 72 hour validity interval for the EE Certificate
- EE Certificate to be revoked upon next regular BOA issuance
- BOAs to be published as a Signed Object in the RPKI Distributed Repository structure

# BOA Interpretation in BGP

- If the originating AS is described in a valid BOA, the the local BGP speaker can regard the route object as failing validation, and take locally-defined actions

- If the originating prefix is described in a valid ROA then ROA validation procedures apply irrespective of a valid BOA
- Otherwise if the prefix is an aggregate that encompasses a prefix described in a BOA, matches a prefix described in a BOA or is a more specific prefix of a prefix described in a BOA, then the local BGP speaker can regard the route object as failing validation, and take locally-defined actions

# BOA Deployment

- No changes to BGP are proposed
- Any RPKI CA may issue a BOA for resources that are not authorized to appear in the routing system
- Any Relying Party may maintain a local cache of BOAs and use the collection of valid BOAs to validate all route objects that are advertised in BGP
- Piecemeal adoption of BOAs by Issuers and Relying Parties is supported

# Questions / Comments?