

STIR Certificates:

Status and Authorization Check Options

STIR WG @ IETF 92
Sean Turner & Jon Peterson

Two sides to every coin

- Sign the call
 - Generate keys
 - Get enrolled
 - Get keys/certificate
- Verify the caller
 - Build a certificate path
 - Do some maths
 - Check the path
 - *Check the status*
 - *Find/retrieve status info*
 - *Check the authorizations*



Status Check Options

- Pay for it upfront or later!
- Gotta find the info:
 - Pointers already defined!
- Which is more painful:
 - Generating key/enrolling/distributing
 - Querying authority
- Options:
 - Short lived certs
 - Query authority
 - CRLs
 - SCVP
 - OCSP

CRLs

- Tried and true
 - Going to be made regardless
- Have a bad rap:
 - Humongous
 - Not online
- Partitioning mechanisms
- Probably shouldn't rely on these for verification of caller

From www.keepcalm-o-matic.co.uk



SCVP/OCSP

- OCSP:
 - More widely deployed
 - Profiled for High-Volume Environments
- SCVP
 - Allows trust decisions to be “off loaded” to a trusted party
- Recommend OCSP:
 - Need to profile in SHA-256



Authorization Check Options

1. For this certificate, is the following number currently in its scope of validity?
2. What are the numbers associated with this certificate?

Option 1: Piggyback

- Reasonable to reuse OCSP?
- Define OCSP extension:
 - OID: from IANA PKIX Arc
 - Criticality: yes
 - Syntax: Any darn thing we want
- Issues:
 - Pre-generate responses?
 - “OCSP stapling”!
 - HVE OCSP profile ☹



From nasa.gov

Option 2: by-Reference

- Embed in certificate:
AIA
- Need our own “access” semantics:
 - Method: Just an OID
 - Location: URI
- Issues:
 - Adds some latency while the query/response completes
 - Privacy concerns

Comments/Questions

- What did I miss?

