draft-huston-sidr-rfc6490-bis

Geoff Huston

draft-~~huston~~ietf-sidr-rfc6490-bis

Geoff Huston

RFC6490

> This document defines a Trust Anchor Locator (TAL) for the Resource Certificate Public Key Infrastructure (RPKI) [RFC6480]. This format may be used to distribute trust anchor material using a mix of out-of-band and online means. Procedures used by Relying Parties (RPs) to verify RPKI signed objects SHOULD support this format to facilitate interoperability between creators of trust anchor material and RPs.

Summary:

- A TAL is a simple text object which is composed of
  - a URI (where self-signed CA can be found)
  - a hash of a public key

Intent:

- To allow a CA to vary the Internet Number Resources in the self-signed CA cert without having to promulgate a new certificate across all Relying Parties

draft-ietf-sidr-multiple-publication-points

"This document addresses this problem [of scalability and diversity] by enabling multiple operators for trust anchor material … by allowing one or more URI for each public key in a TAL file"

Section 3 of the draft describes proposed changes to RFC6490 that would permit the use of multiple URIs in a TAL

Note from SIDR WG Char 6 December:

> Proposes "a "6490-bis" document that obsoletes RFC 6490 with the addition of multiple operators in section 3 of the current document."

draft-~~huston~~ietf-sidr-rfc6490-bis-01.txt

Applies section 3 of draft-ietf-sidr-multiple-publication-points to RFC 6490

- Adds the ability to place multiple URIs in the TAL
- Adds guidelines for Relying Parties

Issues

Discussion issues raised on the SIDR list so far:

- Syntax of a TAL
  - blank line separator between URI(s) and Key?
  - Use "key=val" format?
  - Use JSON?
  - Specify a maximum number of URIs?

- Different certs retrieved from different URI's?
  - Incrementing CA serial numbers?
  - Time limit for CA propagation / removal?
  - Develop a TA change protocol?
  - Publish a TAL lifetime object?
  - What does "Stable URI" mean?