draft-ietf-stir-certificates …

Jon Peterson & Sean Turner
STIR@IETF100

Status (aka I thought we were done with this draft)

In RFC editor's queue: Cluster#318

Martin Thomson sent some comments we feel we need to address see: thread.

Looking for WG approval for five changes that follow.

tl;dr: adopting these changes requires a targeted WGLC/IETF LC

Change #1: TNAuthList in AIA constrains Signer

S10.1 didn’t explicitly state the following but it was always the intention, so the proposal is to add the following to the end of the 2nd paragraph in s10.1:

> As with the certificate extension defined in Section 9, a URI dereferenced from an end entity certificate will indicate the TNs which the caller has been authorized.

Change #2: AIA is on the “critical” path

AIA is a non-critical X.509 extension, but if present we want it processed*.

Propose that we add the following right after where the previously proposed change goes (note the MUST here):

> Verifiers MUST support the AIA extension and the dereferenced URI from a CA certificate limits the the set of TNs for certification paths that include this certificate.

* AIA is supported by implementations to retrieve OCSP responses so this isn’t a “yuge” change.

Change #3: Better specify downloaded AIA format

Propose the following tweak (i.e., we added “DER-encoded):

> The document returned by dereferencing that URI will contain the complete DER encoded TN Authorization List (see Section 9) for the certificate.

Propose that the media type registration on the next page be included in the IANA considerations.

> Note - requires some time for the media-types@iana.org; maximum “some time” in 30 days.

Change #3: media type

Type name: application
Subtype name: tnauthlist
Required parameters: None.
Optional parameters: None.
Encoding considerations: Binary.
Security considerations: See Section 12 of this specification.
Interoperability considerations:
The TN Authorization List inside this media type MUST be DER-encoded TNAuthorizationList.
Published specification: This specification.
Applications that use this media type:
Applications that support [draft-ietf-stir-certificates] certificates.
Fragment identifier considerations: N/A
Additional information:
Magic number(s): None
File extension(s): None
Macintosh File Type Code(s): None
Person & email address to contact for further information:
Jon Peterson <jon.peterson@team.neustar>
Intended usage: COMMON
Restrictions on usage: none
Author: Sean Turner <sean@sn3rd.com>
Change controller: The IESG <iesg@ietf.org>

Change#4: Better specify count field

Count is underspecified WRT “*” and “#” as well as overflow situations (e.g., TN=123 and count=+1000). Adding some extensibility to enable prefix ranges.

Propose the following be added in s9 to item #2 (discusses TN ranges and in the following count, start, and TelephoneNumber refer to the ASN.1 fields):

> The count field is only applicable to start fields’ whose values do not include “*” or “#” (i.e., a TelephoneNumber that does not include “*” or “#”). count never overflows a TelephoneNumber digit boundary (i.e., a TelephoneNumberRange with TelephoneNumber=10 with a count=91 will address numbers 10-99).

Change #5: Beef up Security Consideration

If AIA divulges the entire list of telephone numbers associated with a particular certificate STIR verifiers, information can leak about telephone numbers other than the one associated with the particular call that the verifier is checking.

We’ve danced around this issue with our work on certificate freshness for some time. Trade off is data minimization vs. the RTT.

We will add some text about short-lived certs here and the way they can mitigate the risks