draft-rgaglian-csi-send-name-type-type-registry

Roque Gagliano
Suresh Krishnan
Ana Kukce
SEND Trust Anchor Option:

- Defined in RFC 3971.
- Allows the identification of the TA by the host.
- Part of CPS message and form by:

```
+-----------------+-----------------+-----------------+-----------------+
| Type            | Length          | Name Type       | Pad Length      |
+-----------------+-----------------+-----------------+-----------------+
| Name ...        | ... Padding     |                 |                 |
```

- In RFC 3971 two name types were defined but no registry was created in the IANA section.
TA Across Admin Boundaries.

Administrative Domain (ex. ISP, enterprise)

Host

Local

Certs and CRL Repository.

Public

Certs and CRL Repository.

Host

TA

Administrative Domain

Certs and CRL Repository.
New SKI Name Type

- Subject Names and FQDN may not be unique across different CAs.
- CSI is using RPKI Cert Profiles where subject names are normally meaningless and SKI is mandatory.
- We take the same definition as written in the cert draft:

The Key Identifier used here is the 160-bit SHA-1 hash of the value of the DER-encoded ASN.1 bit string of the subject public key, as described in Section 4.2.1.2 of [RFC5280].
Thanks

and

should the WG adopt this document?