Governance and Policy Considerations for Delegate Certificates

ATIS/SIP Forum IPNNI Task Group

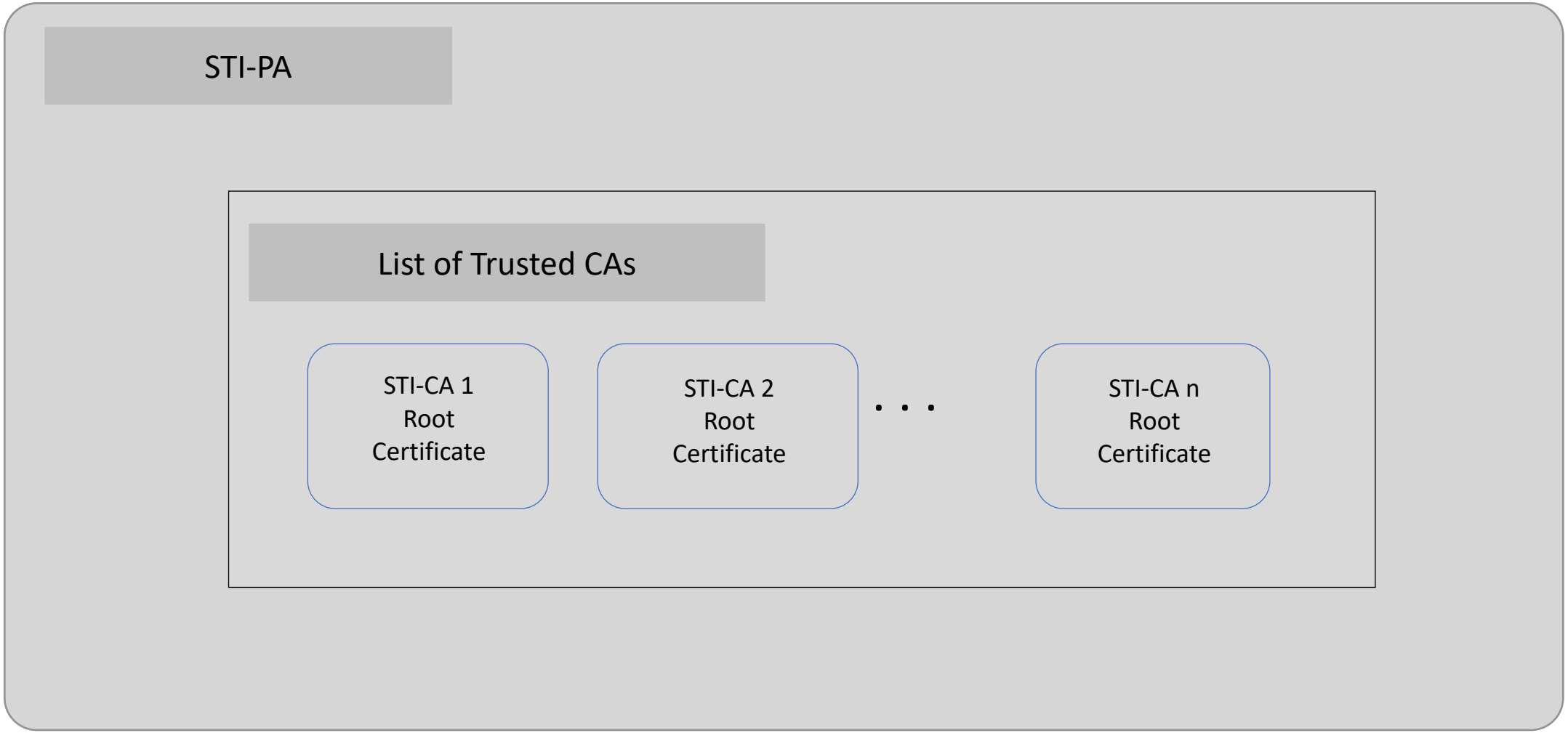
January 24, 2022

Mary Barnes (Neustar, Inc., a Transunion Company)

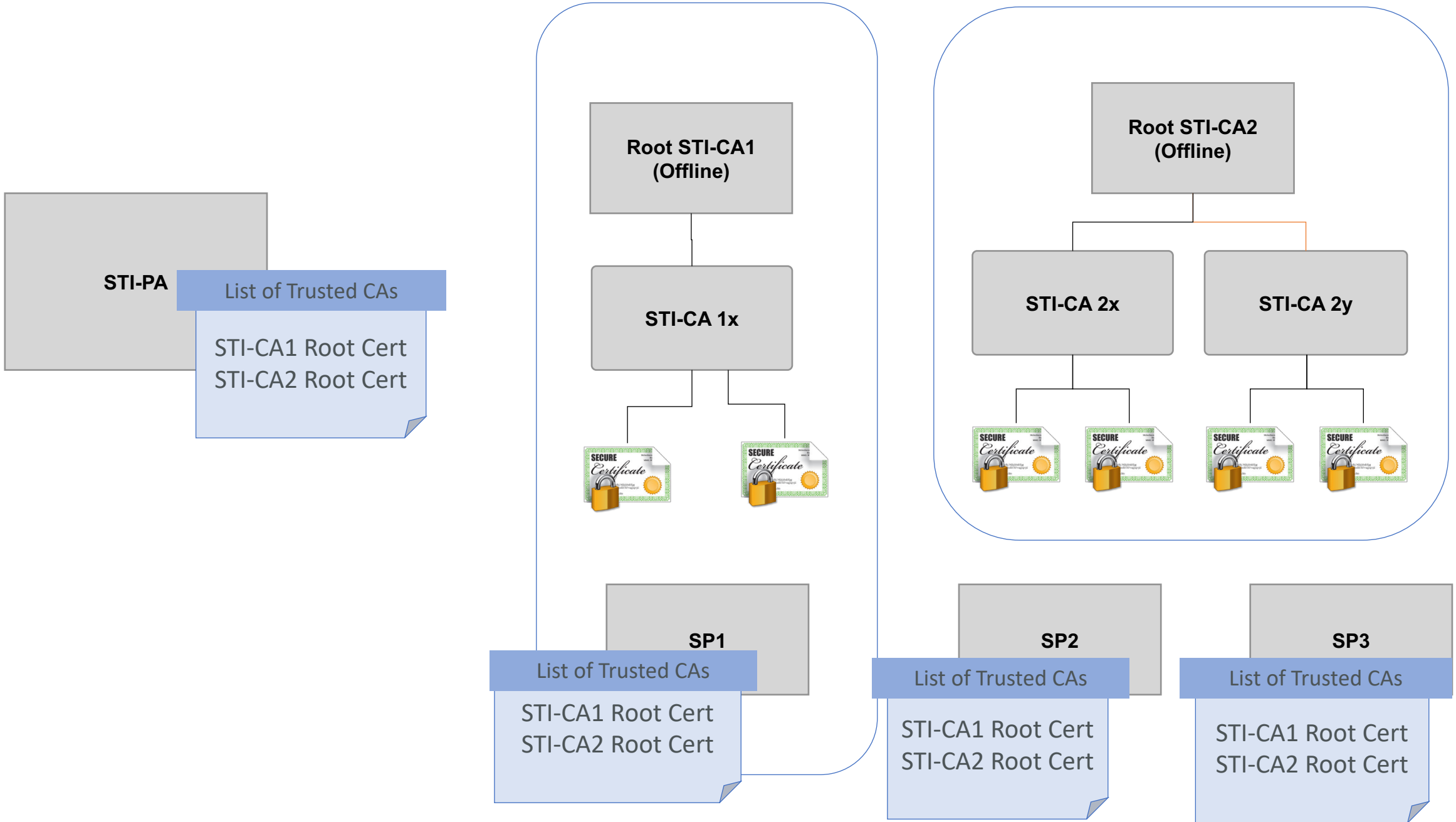
Background

- ATIS-1000092:
  - Describes mechanism authorizing the establishment of an SCA (by an SP) for issuance of delegate certificates
  - Proposes that delegate certs are short lived thus no requirement for support for revocation
  - (S)CA certificate can be revoked using existing PA defined interface
- IPNNI-2021-00015R00:
  - Documents some governance and policy considerations for delegate certs and SCA
  - Proposes that SCA submits a separate CPS

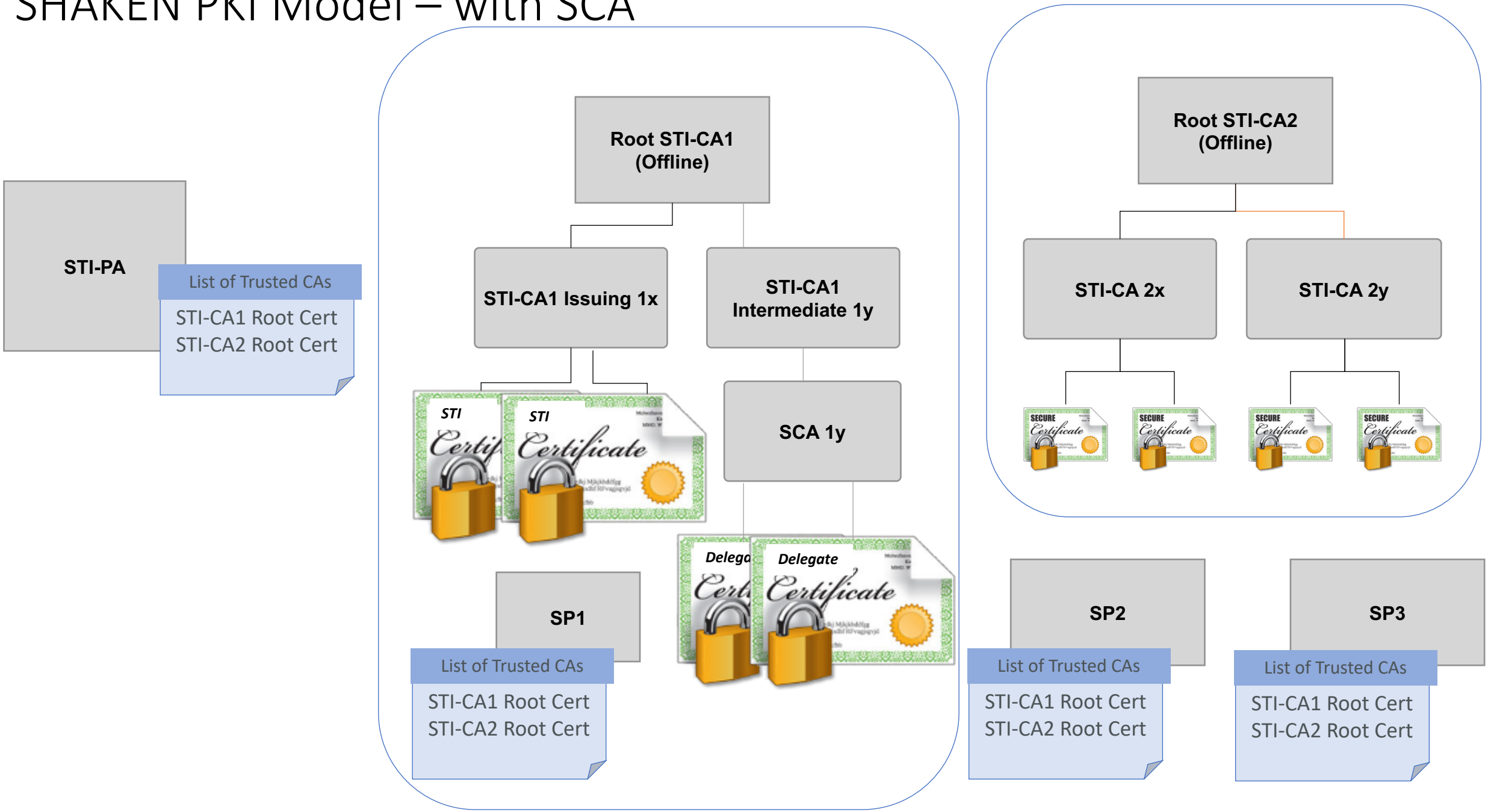
SHAKEN Interdomain PKI Model



SHAKEN PKI Model – ATIS-1000084



SHAKEN PKI Model – with SCA



Trust model considerations with SCAs

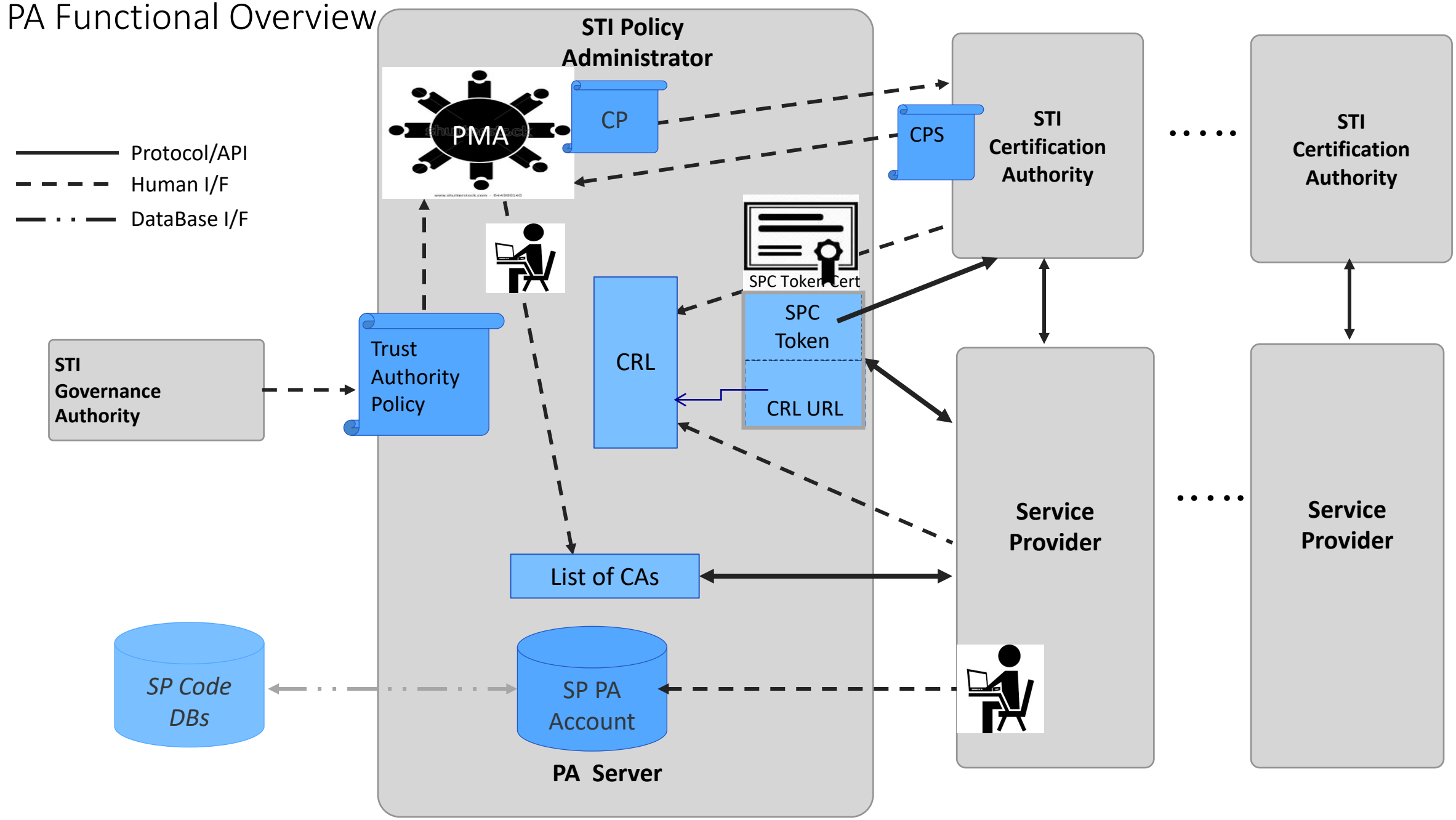
- The addition of an SCA to the SHAKEN architecture in support of Delegate Certificates does (should) not impact core SHAKEN PKI Trust Model:
  - All issued certificates (STI and delegate) MUST chain to a Root certificate in the list of Trusted CAs.
- A CA that issues CA certificates, allowing an SP to host an SCA*, which issues delegate certificates, must have an approved CPS that describes how this is accomplished:
  - The CA must only issue the certificate to an SP that has an SPC Token with CA=true, issued by the PA
  - Whether the delegate certificates can be issued with CA=true should be documented in the CPS.

*Note: SCA can also be hosted by the CA on behalf of the SP.

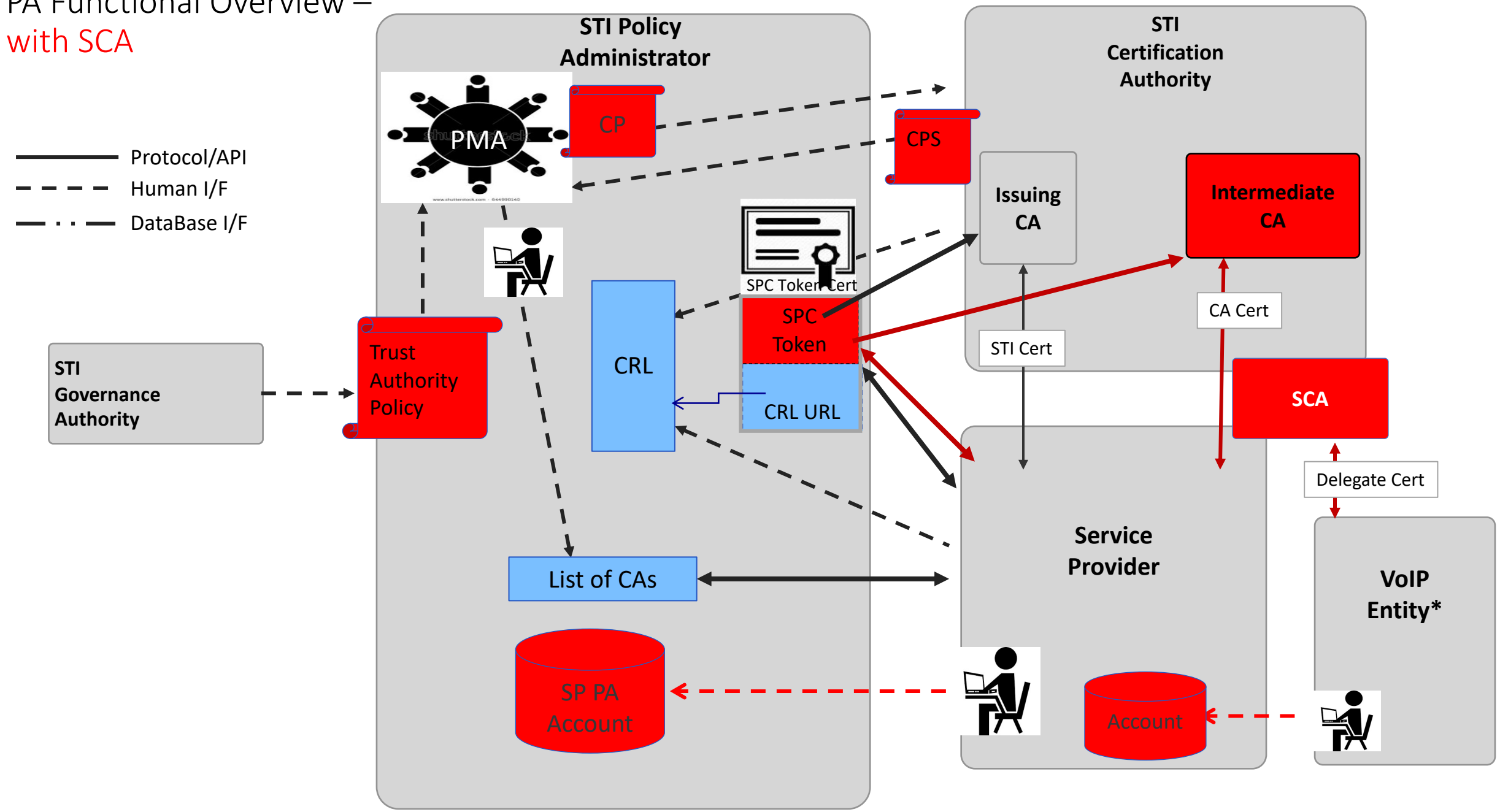
Trust model considerations with SCAs (continued)

- The SP must be approved by the PA to obtain SPC tokens with CA=true (i.e., an SP must be authorized to issue delegate certs to their customer/VoIP entities).
  - Criteria for authorization/approval should be established by the STI-GA, for example:
    - Required information to be gathered and maintained with regards to the VoIP entity (e.g., legal business name, location of business, age of business, any regulatory considerations, etc.)
    - Operational metrics to be maintained such as number of certificates issued and frequency of issuance.
    - Information required for traceback (and criteria for requesting such).
  - Other criteria by which an SP authorizes/pre-approves the VoIP entities to be issued certificates is specific to an SP.

PA Functional Overview



PA Functional Overview – with SCA



*VoIP Entity is pre-authorized to obtain a cert. No tokens/no CRL

Certificate revocation for Delegate certificates

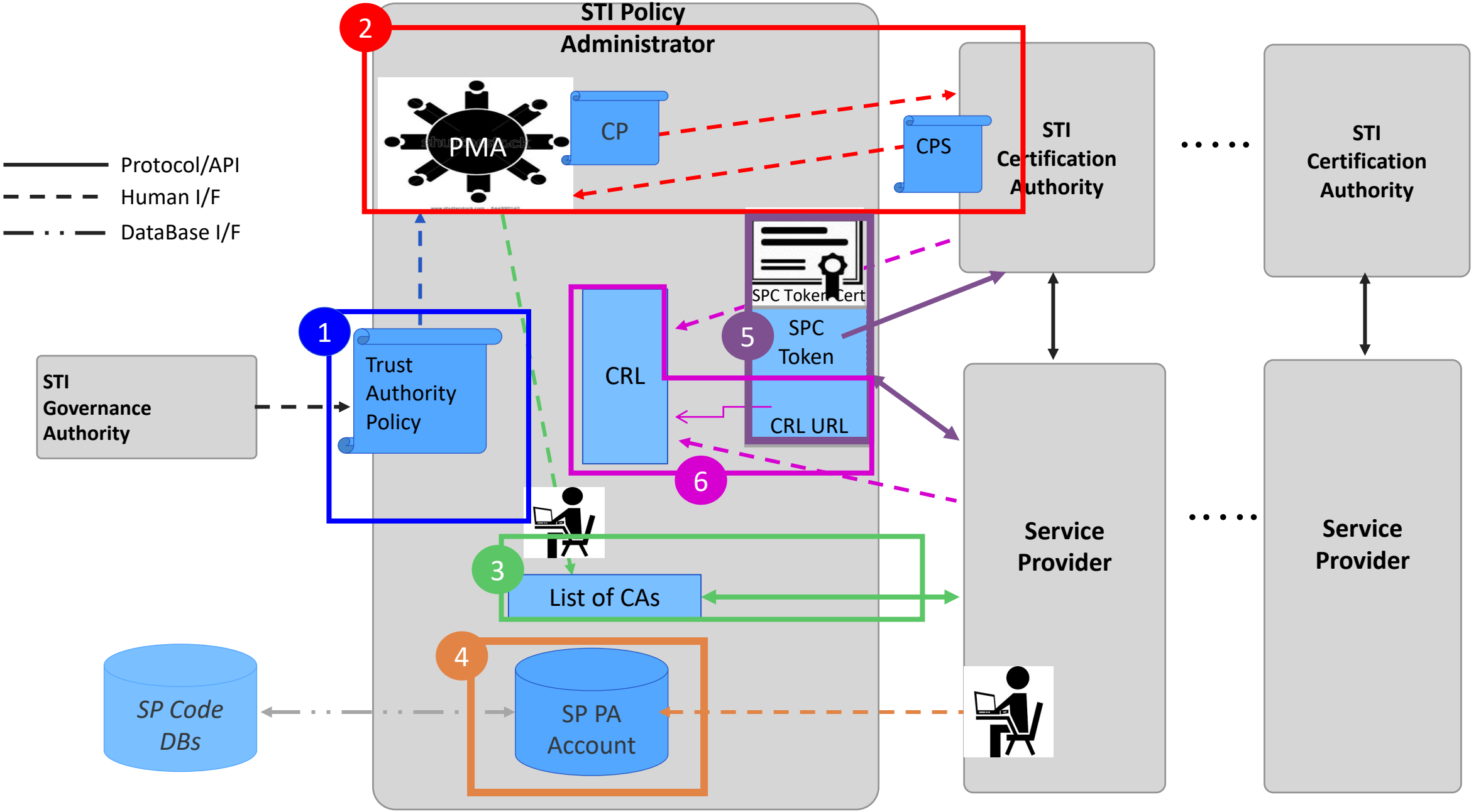
- ATIS-1000072 documents that delegate certs will be short lived and thus no revocation or CRL in the issued certificates is required.
  - Issue: That was the initial premise for ATIS-1000080 and that was not what people intended to implement.
- Premise in ATIS-1000072 is that SCA certificate could be revoked if necessary, following the same procedures as revocation of STI-certificates
  - Issue: This impacts *all* delegate certificates issued by the SCA. There may be scenarios whereby there are still valid delegate certificates outstanding that would fail validation in that case – e.g., in the case that an SP uses the same SCA for multiple customers.

Proposal

- Update ATIS-1000080 and ATIS-1000084 (and ATIS-1000092) to include governance and policy considerations for Delegate Certificates.
  - Describe governance and policy considerations specific to delegate certificates in the context of existing SHAKEN Trust model (pulling some content from IPNNI-2021-00015R001)
  - Detail certificate content requirements for delegate certs within section 6.4 of ATIS-1000080
  - Update (or remove) certificate evolution section (6.3.10) of ATIS-1000080.
  - Detail additional policy considerations for the CP in ATIS-1000084.
  - Describe support for certificate revocation in ATIS-1000080 and ATIS-1000092.

Backup

PA Functions – ATIS 1000080



PA + SCA Functions