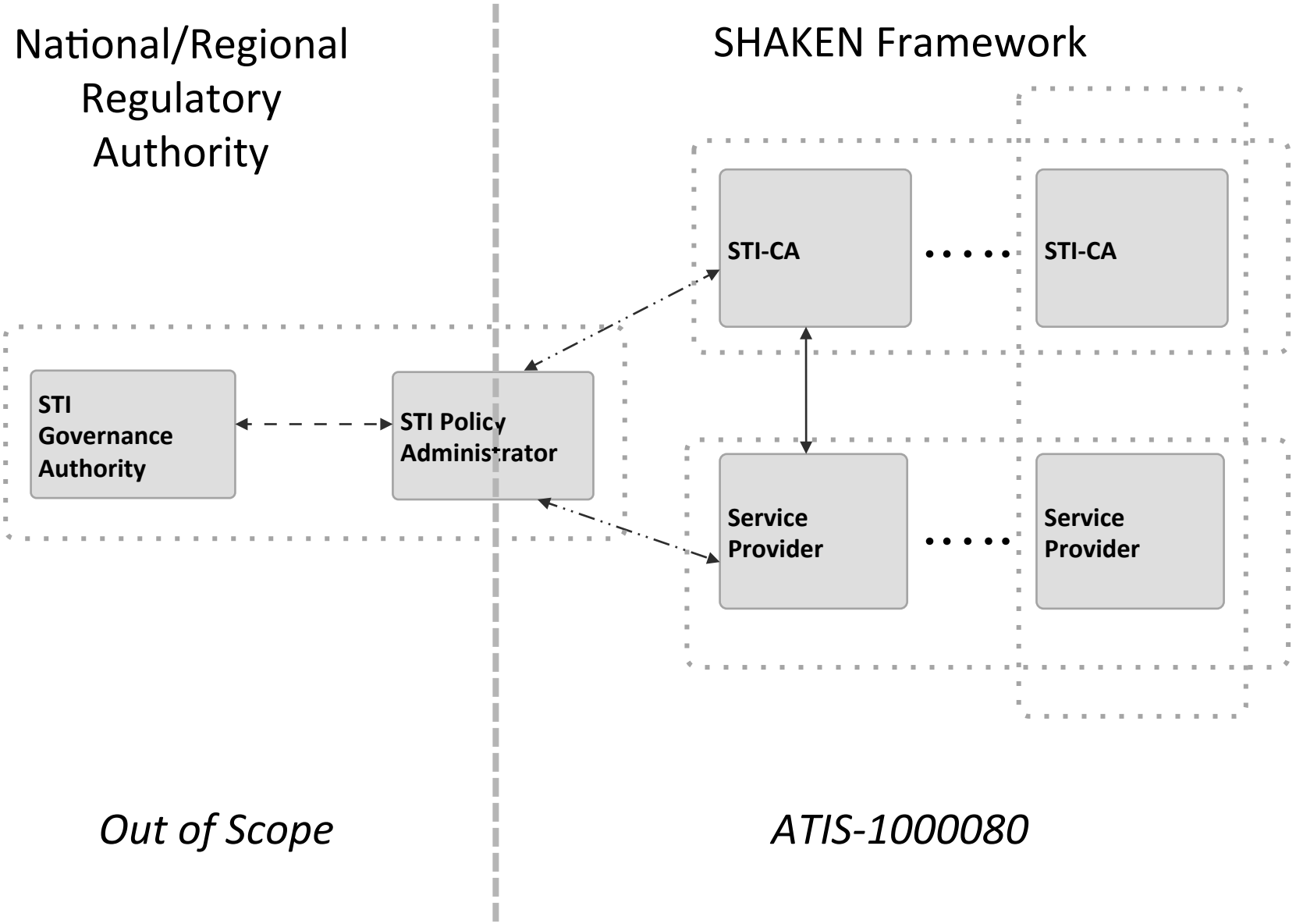
Operational Considerations for SHAKEN STI Certification Authorities and Policy Administrators

based on
ATIS-IPNNI-2017-00051R004.docx

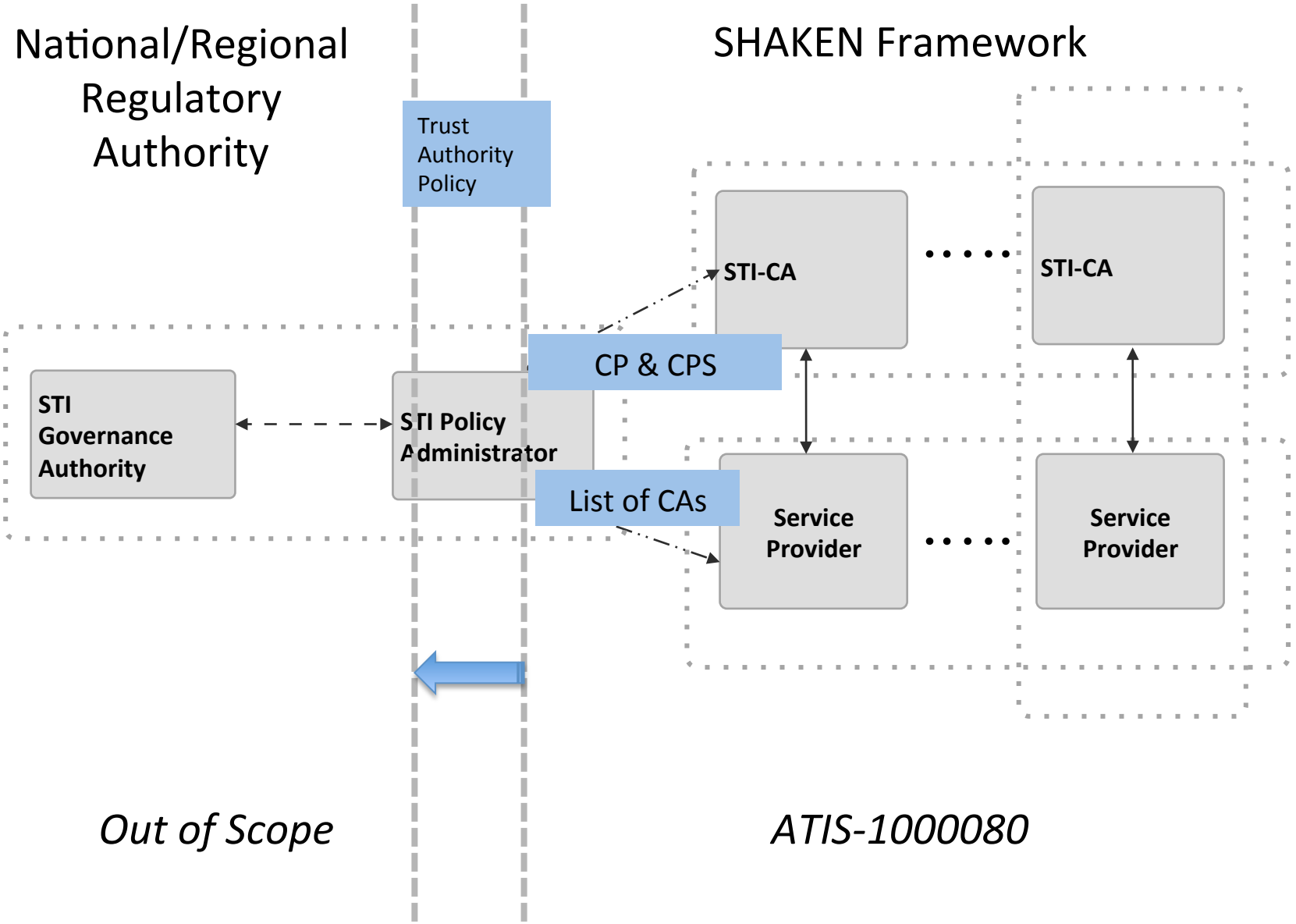
Note: this does not represent a complete set of guidelines – this is a working document subject to change


National/Regional Regulatory Authority
SHAKEN Framework
STI-CA
STI-CA
STI Governance Authority
STI Policy Administrator
Service Provider
Service Provider
Out of Scope
ATIS-1000080

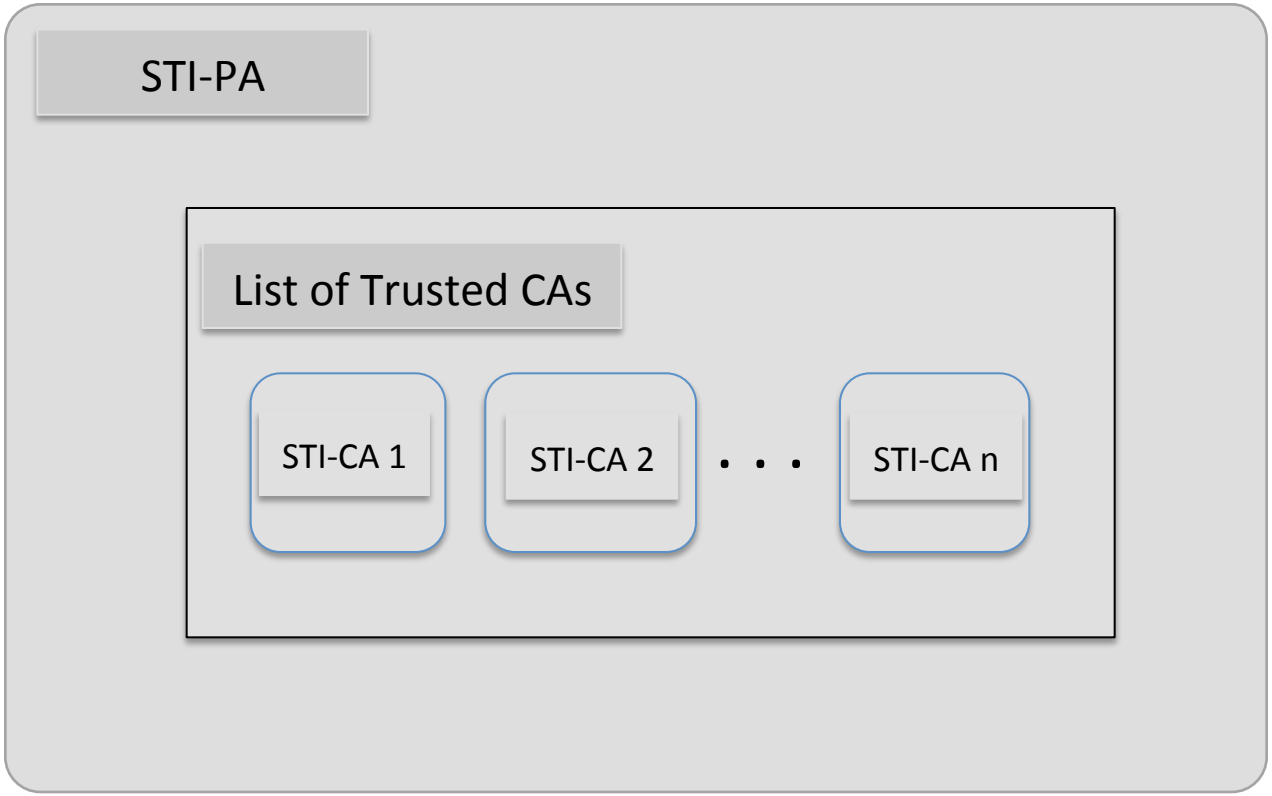
Overview

Describes operational considerations and recommended practices for STI-PA in managing approved STI-CAs and authorized Service Providers:

- Trust Authority Policy
- Certificate Policy & Certification Practice Statements
- Management of List of STI-CAs
- STI-PA Administration of Service Providers


National/Regional Regulatory Authority
SHAKEN Framework
Trust Authority Policy
STI-CA
STI-CA
CP & CPS
STI Governance Authority
STI Policy Administrator
List of CAs
Service Provider
Service Provider
Out of Scope
ATIS-1000080

Trust Authority Model



- STI-PA is external to the PKI – maintains list of Trusted CAs on behalf of the relying parties in the PKI
- STI-PA serves as the Trust Anchor to the relying parties in the PKI
- Each STI-CA must support Certificate Policy (CP) as established by the STI-PA
- STI-PA reviews Certification Practice Statement (CPS) as provided by the STI-CAs to ensure compliance

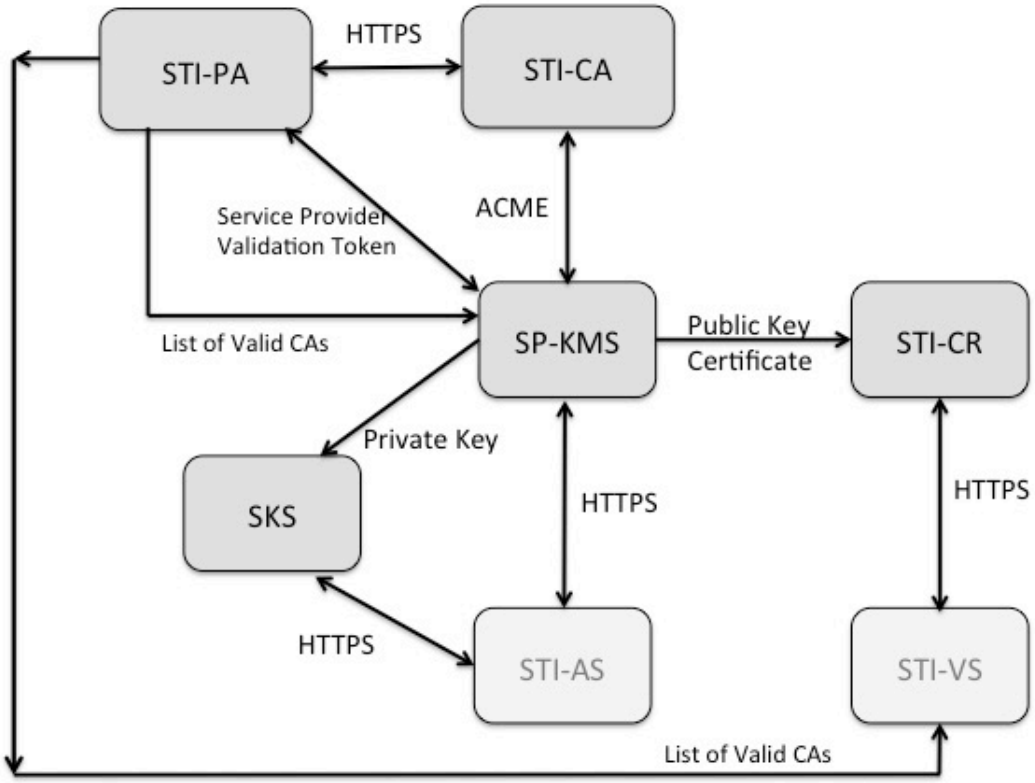
Trust Authority Policy

- STI-PA is the only Trust Authority in the model – STI-CAs should not inherit trust from other CAs (no policy mapping)
- STI-PA can remove an STI-CA from the list of trusted CAs based on pre-established criteria (e.g., failure to comply with the CP established by the STI-PA)
- STI-CA is responsible for the following:
  - Notify STI-PA should it no longer choose to issue STI certificates
  - Notify STI-PA if certificates are revoked
  - Follow recommended procedures for CA key rollover

Certificate Policy

- Standarizes server and CA naming to avoid collisions
- Root CAs should NOT be online – offline CAs should be in a secure vault until a new certificate requires issuance.
- Defines profile for extensions to be supported – e.g., must support TNAuthList extension
- Provides mechanism to support certificate revocation
- Requires provision of secure mechanisms for key recovery and data recovery agents.
- Requires CA to maintain proper system time (e.g. secure NTP).

List of Valid STI-CAs



List of Valid CAs

- STI-PA (administrative body) reviews the CPS of the STI-CA to ensure it is operated to an acceptable level of assurance:
  - Ensures polices per CP are supported
  - Determines that the STI-CA/PKI provides a warranty with regards to issued certificates
  - Periodic audits recommended
- STI-PA periodically distributes/updates list:
  - Mechanism details TBD
  - Periodicity should be shorter than certificate lifetimes
  - Updated list should be distributed if an STI-CA is removed
  - Service Providers can request updated list if it expires

STI-PA Administration of Service Providers

- Existing identifiers (e.g., OCNs), allocated and managed by an entity authorized by an NRAA, are used as Service Provider Codes:
  - Provide uniqueness & accountability
- Prior to requesting a certificate, a Service Provider must:
  - Create an account with the STI-PA
  - Create an account with an STI-CA
  - Obtain a service provider code token from the STI-PA (as Trust Anchor) per the procedures outlined in ATIS-1000080.