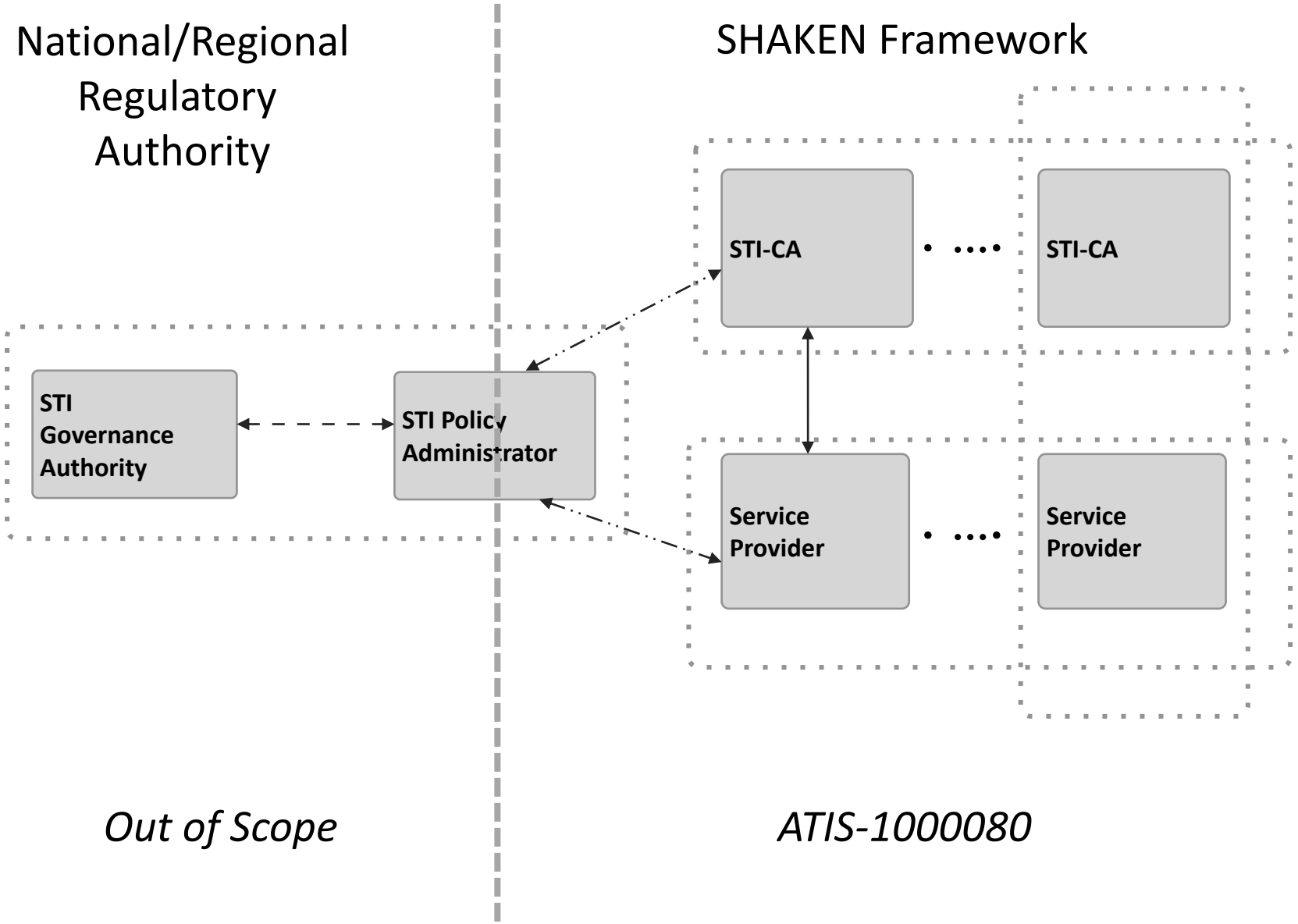
Operational Considerations for SHAKEN STI Certification Authorities and Policy Administrators

based on
ATIS-IPNNI-2017-00051R008.docx

mbarnes@iconectiv.com

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

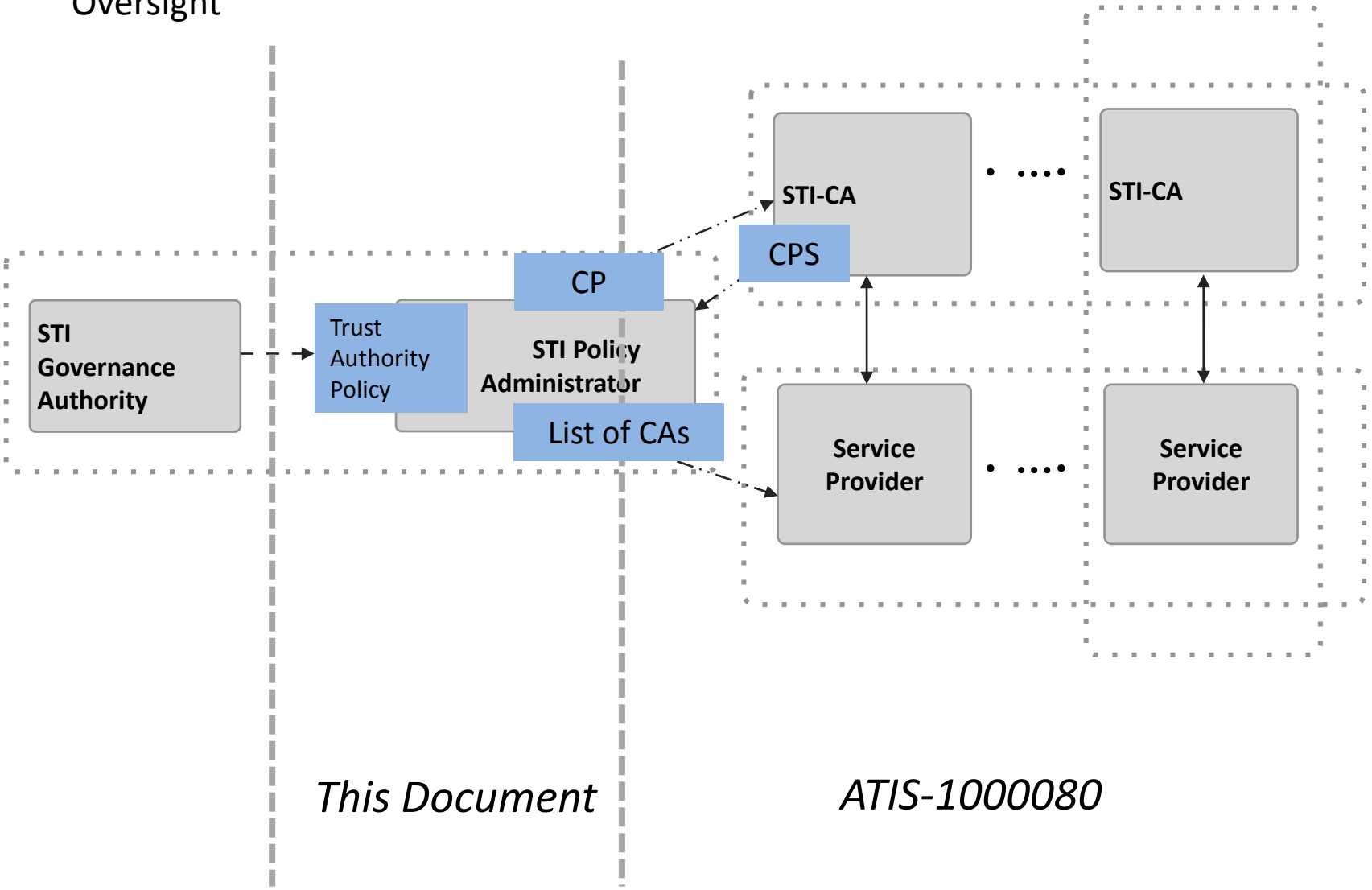
Overview

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

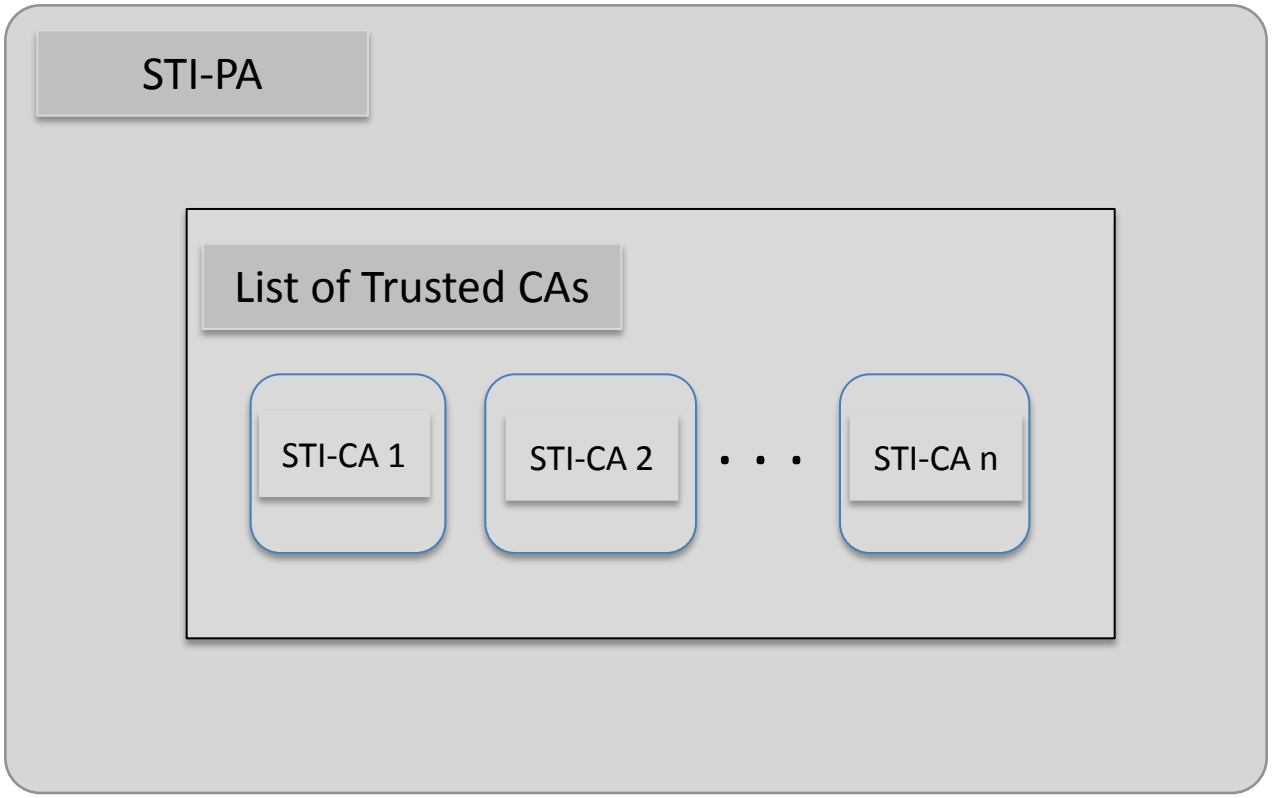
- Trust Authority Model
- Certificate Policy & Certification Practice Statements
- Management of List of STI-CAs
- STI-PA Administration of Service Providers

SHAKEN Certificate Management

National/Regional Regulatory Oversight



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 Model

- Role of the STI-PA is to enforce the criteria as established by the STI-GA:
  - Typically a Policy Management Authority (PMA) comprises a set of people responsible for ensuring that the established policies are being adhered to.
- 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)

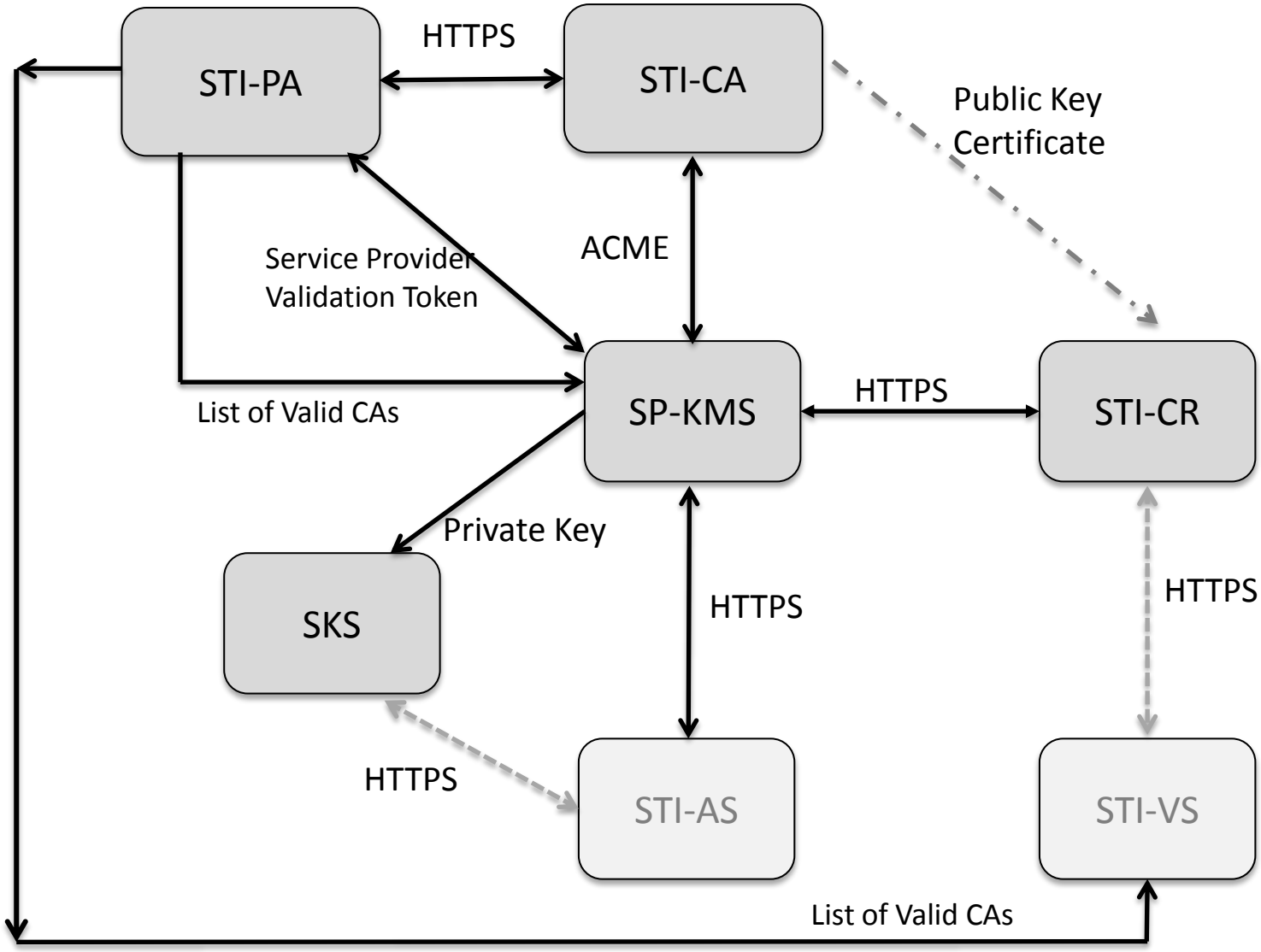
Certificate Policy

- STI-PA imposes a Certificate Policy (CP) on the STI-CAs
- A Certificate Policy (CP) provides a set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements [RFC 3647].
- The CP contains the business, legal, and technical requirements for certificate approval, management, use, revocation, and renewal.
- The Certificate Policy contains policies for the STI-PA, STI-CA, STI-CR, subscribers, and relying parties. [RFC 3647] contains the following outline for the contents of the Certificate Policy:
  1. Introduction
  2. Publication and Repository
  3. Identification and Authentication
  4. Certificate Life-Cycle Operational Requirements
  5. Facilities, Management, and Operational Controls
  6. Technical Security Controls
  7. Certificate, CRL, and OCSP Profile
  8. Compliance audit
  9. Other Business and Legal Matters

Certification Practice Statement

- The Certification Practices Statement (CPS) contains the practices a CA follows when issuing digital certificates.
- The CPS is written by the STI-CA.
- The CPS provides detailed information on how the policy requirements documented in the CP are implemented by the CA.
- It is recommended that the CPS follow the same format as the CP.
  - [RFC 3647] contains the recommended contents of a CP and CPS.

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.