Annex A

Compliance Control Mapping Methodology

Informative – Not Normative

A.1 Purpose and Scope

This annex defines a methodology for mapping the evidence elements produced by the Continuous Remote Attestation Framework to individual technical controls within recognized compliance standards. It is intended to enable organizations to leverage their continuous attestation infrastructure as a source of machine-verifiable compliance evidence.

This annex is informative, not normative. It does not constitute a compliance certification, nor does it assert that implementing the framework satisfies any compliance standard in its entirety. Compliance with any regulatory framework requires meeting all specified controls – including organizational, procedural, and administrative controls that are beyond the scope of machine-verifiable attestation.

The mapping is scoped exclusively to technical controls that can be evidenced through the attestation stack. For each mapped control, the annex identifies which framework evidence elements provide relevant evidence, and the attestation layer from which that evidence originates.

A.1.1 Covered Regulatory Frameworks

This annex provides illustrative mappings to the following regulatory frameworks, selected for their relevance to the primary deployment environments for confidential computing:

Sector	Framework	Version	Relevance
Government / Defense	CMMC 2.0 Level 2 (NIST SP 800-171 Rev. 2)	Rev. 2 (2020)	Required for all DoD contractors handling CUI. CMMC 2.0 Level 2 mandates all 110 NIST 800-171 controls. Mapping uses the underlying 800-171 control IDs as these are what C3PAO assessors evaluate.
Government / Federal	NIST SP 800-53 Rev. 5	Rev. 5 (2020)	Mandatory for federal information systems under FISMA. Provides the most granular control catalog and serves as the foundation for FedRAMP.

Sector	Framework	Version	Relevance
Healthcare	HIPAA Security Rule	45 CFR § 164.302–318	Required for covered entities and business associates handling electronic protected health information (ePHI).
Finance	PCI DSS v4.0.1	v4.0.1 (2024)	Required for any entity that stores, processes, or transmits payment card data.
Cross-Sector (Audit)	SOC 2 Trust Services Criteria	2017 (current)	Widely used for SaaS and cloud service providers demonstrating security, availability, and confidentiality controls.

A.1.2 What This Mapping Does NOT Cover

The following categories of compliance controls are explicitly out of scope for this annex:

- Organizational and governance controls (e.g., security awareness training, personnel background checks, management responsibility)
- Procedural and process controls (e.g., incident response plan documentation, change management board approvals, risk assessment methodologies)
- Physical security controls (e.g., facility access, media destruction, environmental protections)
- Controls that require human judgment or assessment (e.g., security architecture review, penetration testing, risk acceptance decisions)

These controls are essential components of any complete compliance program but cannot be evidenced through a technical attestation stack.

A.2 Mapping Methodology

Each mapping entry follows a consistent structure:

- **Control ID:** The identifier from the source standard (e.g., NIST 800-171 3.1.1, PCI DSS 6.3.2).
- **Control Description:** A brief description of the control requirement.
- **Framework Layer:** The attestation layer (L1, L2, L3, or Protocol) that produces the relevant evidence.
- **Evidence Element(s):** The specific evidence elements from the framework that address the control.
- **Coverage Level: Full.** The framework evidence element directly and completely satisfies the technical requirements of the control as written.

Supplementary identity evidence may also be produced by an implementation's workload identity system. For example, deployments using SPIFFE / SPIRE may generate machine-verifiable evidence of workload registration, credential issuance, credential rotation, and credential revocation. Such evidence is relevant primarily to identity and authentication controls. However, workload identity evidence does not replace attestation evidence and should be treated as complementary unless the implementation can demonstrate that credential issuance and renewal are cryptographically or policy-bound to the current attestation state.

An Appraiser/Publisher implementation may issue individual cryptographically signed compliance control assertions for controls mapped at the Full or Partial coverage level. Each assertion includes the control identifier, the evidence elements that satisfy it, the current epoch_id, a timestamp, and a digital signature. These assertions are designed to be machine-readable for consumption by automated compliance monitoring systems.

Provider Trust Stance Context. Compliance assertions issued under different Provider Trust Stances (main framework Section 5.3) carry different downstream meanings for some controls. Controls that explicitly require evidence independent of the cloud service provider, including selected FedRAMP High requirements, sovereign cloud requirements, and certain CMMC scoping decisions, can only be satisfied by assertions issued under the Provider-Independent stance. Assertions for these controls include the Provider Trust Stance under which they were issued in their metadata (see A.7.1). Assessors and relying parties consuming a compliance assertion stream should verify the stance value alongside the control identifier when interpreting the assertion against control text that conditions on cloud service provider trust assumptions.

A.3 Government and Defense Mappings

A.3.1 CMMC 2.0 Level 2 (NIST SP 800-171 Rev. 2)

CMMC 2.0 Level 2 requires implementation of all 110 security controls from NIST SP 800-171 Rev. 2. As of November 2025, CMMC requirements are appearing in new defense contracts, with third-party C3PAO assessments required from November 2026. The mapping below uses the NIST 800-171 control identifiers, as these are the specific assessment objectives evaluated by C3PAOs during CMMC Level 2 certification assessments.

Controls that are entirely organizational or procedural in nature are omitted. Of the 110 NIST 800-171 controls, the attestation framework provides relevant technical evidence for approximately 21 controls, mapped below.

NIST 800-171 ID	Control Family / Description	Layer	Evidence Element
3.1.13	AC: Employ cryptographic mechanisms for remote access	L1 / Protocol	TLS termination inside TEE with Attested Transport Binding (TB-1 through TB-3), AES-256-GCM encryption
3.1.20	AC: Verify and control connections to external systems	L3.2	eBPF egress filtering, denied_network rules, network connection allowlist
3.3.1	AU: Create and retain audit records	Protocol	Transparency log (append-only Merkle tree), YANG Push event stream with signed epoch_id, appraisal history API
3.4.1	CM: Establish and maintain baseline configurations	L2	Golden Baseline (YAML/CoRIM), composite vendor/tenant baseline, container image digests, IMA hash lists
3.4.2	CM: Establish and enforce security configuration settings	L1 / L2	TPM-verified Secure Boot, IMA policy enforcement (tcb mode), SELinux immutable policy, min_tcb_version enforcement
3.4.3	CM: Track, review, approve, and audit changes	L2 / Protocol	Container digest comparison against baseline, Sigstore signature verification, transparency log of all appraisal decisions

NIST 800-171 ID	Control Family / Description	Layer	Evidence Element
3.4.5	CM: Define, document, and enforce physical and logical access restrictions associated with changes	L1 / L2	TEE hardware memory isolation boundary, vendor baseline immutability (tenant cannot override platform reference values)
3.5.2	IA: Authenticate identities before allowing access	L1 / Protocol	Attested Transport Binding (TB-1, TB-2, TB-3): attestation evidence verified against hardware trust anchor with key commitment and freshness
3.13.1	SC: Monitor, control, and protect communications at system boundaries	L1 / L3.2	TLS termination inside TEE with Attested Transport Binding (TB-1), AES-256-GCM payload encryption, eBPF network monitoring and egress filtering
3.13.8	SC: Implement cryptographic mechanisms to prevent unauthorized disclosure during transmission	L1	TLS 1.3 inside TEE, AES-256-GCM with post-quantum key encapsulation (e.g., ML-KEM per FIPS 203), end-to-end encryption between client and TEE
3.14.2	SI: Provide protection from malicious code	L2 / L3	IMA executable integrity (prevents launch of modified binaries), eBPF behavioral containment, kernel integrity monitoring (KIM)
3.14.6	SI: Monitor the system to detect attacks and indicators of potential attacks	L3.1 / L3.2	Continuous kernel integrity monitoring (syscall table, IDT, module list), eBPF process/network/file behavioral monitoring, IMA runtime measurements
3.14.7	SI: Identify unauthorized use of the system	L3.2	eBPF behavioral profile enforcement (syscalls, network, binaries), IMA runtime measurement of new executables, alert/revoke policy modes

A.3.2 NIST SP 800-53 Rev. 5 (Selected Controls)

The following maps selected NIST 800-53 control families to framework evidence. This is not exhaustive; it focuses on the control enhancements most directly addressed by continuous attestation.

800-53 ID	Control Name	Layer	Evidence Element	Coverage
CA-7	Continuous Monitoring	All	60-second evidence reporting cycle, four-layer continuous appraisal, YANG Push notification stream, transparency log	Full
CM-2	Baseline Configuration	L2	Golden Baseline YAML, composite vendor/tenant baselines, container digests, IMA boot measurements	Full
CM-3	Configuration Change Control	L2 / Protocol	Container digest change detection, Sigstore re-signing required for updates, transparency log of all state changes	Full
CM-6	Configuration Settings	L1 / L2	Secure Boot enforcement, IMA policy (tcb), SELinux immutable config, min_tcb_version, debug status (dbgstat)	Full
IA-3	Device Identification and Authentication	L1	Hardware attestation report, Attested Transport Binding (TB-1, TB-3), platform identity via silicon Root of Trust	Full
SC-7	Boundary Protection	L1 / L3.2	TEE hardware memory encryption boundary, eBPF egress filtering, Attested Transport Binding (TB-1, TB-4)	Full
SC-8	Transmission Confidentiality and Integrity	L1	TLS inside TEE with Attested Transport Binding (TB-1 through TB-3), AES-256-GCM payload encryption. Key protection per TB-5.	Full
SC-12	Cryptographic Key Establishment and Management	L1	Cloud KMS with WIF gating, KMS grant/revoke tied to attestation state, state-gated I/O pattern	Full
SC-13	Cryptographic Protection	L1	AES-256-GCM, NIST-standardized post-quantum signature algorithm (e.g., ML-DSA per FIPS 204), post-quantum key encapsulation (e.g., ML-KEM per FIPS 203). AEAD for AI model weights. Hardware attestation report signatures remain	Full

800-53 ID	Control Name	Layer	Evidence Element	Coverage
			dependent on silicon vendor algorithm support.	
SC-28	Protection of Information at Rest	L1 / L2	TEE memory encryption (hardware), KMS-encrypted storage, AEAD model weight integrity	Full
SI-3	Malicious Code Protection	L2 / L3	IMA prevents launch of modified binaries, eBPF behavioral detection, kernel integrity monitoring	Full
SI-4	System Monitoring	L3.1 / L3.2	Continuous eBPF behavioral monitoring (syscall, network, file), kernel integrity checks every 60s, IMA runtime measurements	Full
SI-7	Software, Firmware, and Information Integrity	L1 / L2 / L3.1	Hardware boot measurement, IMA file integrity, container digest verification, KIM syscall/IDT/module validation, Sigstore signatures	Full

A.4 Healthcare Mapping: HIPAA Security Rule

The HIPAA Security Rule (45 CFR § 164.302–318) establishes standards for protecting electronic protected health information (ePHI). The following maps the Security Rule's technical safeguard standards and implementation specifications to framework evidence elements.

NOTE: HIPAA distinguishes between "Required" and "Addressable" implementation specifications. This mapping focuses on the technical evidence the framework provides; organizational determinations of what is "reasonable and appropriate" remain with the covered entity.

HIPAA Ref.	Standard / Specification	Layer	Evidence Element
§ 164.312(a)(2)(iv)	Encryption and Decryption (A)	L1	AES-256-GCM end-to-end encryption, TEE memory encryption (hardware), KMS-managed keys for data at rest
§ 164.312(b)	Audit Controls (Standard)	Protocol	Transparency log (append-only Merkle tree), YANG Push signed event stream, monotonic epoch_id, appraisal history
§ 164.312(c)(1)	Integrity (Standard)	L2 / L3.1	IMA file integrity, container digest verification, kernel integrity monitoring, Sigstore signatures, SBOM verification
§ 164.312(c)(2)	Mechanism to Authenticate ePHI (A)	L2	Container image digest verification, AEAD integrity for data artifacts, IMA hash comparison at load time
§ 164.312(d)	Person or Entity Authentication (Standard)	L1 / Protocol	Attested Transport Binding (TB-1, TB-2, TB-3): attestation evidence verified against hardware trust anchor with key commitment and freshness
§ 164.312(e)(1)	Transmission Security (Standard)	L1	TLS termination inside TEE with Attested Transport Binding (TB-1), AES-256-GCM payload encryption
§ 164.312(e)(2)(i)	Integrity Controls (A)	L1 / Protocol	TLS integrity (AEAD ciphersuites), signed attestation events, nonce-bound responses preventing replay
§ 164.312(e)(2)(ii)	Encryption (A)	L1	TLS 1.3 with AES-256-GCM, post-quantum key encapsulation (e.g., ML-KEM per FIPS 203). Key protection model per TB-5 disclosure

A.5 Finance Mapping: PCI DSS v4.0.1

PCI DSS v4.0.1 applies to entities that store, process, or transmit cardholder data. The following maps PCI DSS requirements to framework evidence elements where the attestation infrastructure provides directly relevant technical controls.

PCI DSS Req.	Requirement Description	Layer	Evidence Element	Coverage
1.2.1	Restrict inbound and outbound traffic to that which is necessary	L3.2	eBPF egress filtering with explicit allowlist, denied_network rules, network connection monitoring	Full
2.2.1	Develop configuration standards for all system components	L2	Golden Baseline YAML, composite vendor/tenant baselines, container image digests, IMA policy definitions	Full
2.2.7	Encrypt all non-console administrative access	L1	All access via TLS inside TEE with Attested Transport Binding (TB-1 through TB-3), AES-256-GCM payload encryption	Full
3.5.1	Protect stored account data using strong cryptography	L1	TEE memory encryption (hardware), KMS-managed encryption keys, state-gated key release (keys revoked on attestation failure)	Full
4.2.1	Use strong cryptography during transmission of cardholder data over open networks	L1	TLS 1.3 terminating inside TEE with Attested Transport Binding (TB-1, TB-2), AES-256-GCM, post-quantum signatures (e.g., ML-DSA per FIPS 204)	Full
5.2.1	Detect and protect against malicious software	L2 / L3	IMA prevents execution of modified binaries, eBPF behavioral containment, kernel integrity monitoring (KIM)	Full
6.3.2	Maintain an inventory of bespoke and custom software	L2	SBOM (SPDX/CycloneDX) verification, Sigstore/Cosign provenance signatures, container image manifest tracking	Full
10.3.1	Protect audit logs from modification	Protocol	Transparency log (append-only Merkle tree),	Full

PCI DSS Req.	Requirement Description	Layer	Evidence Element	Coverage
			Publisher signatures over events, public auditability	
11.5.1	Implement change-detection mechanisms on critical files	L2 / L3.1	IMA file integrity monitoring, container digest change detection, kernel structure integrity (KIM), runtime IMA measurements	Full

A.6 Cross-Sector Mapping: SOC 2 Trust Services Criteria

SOC 2, based on the AICPA Trust Services Criteria, is widely used by cloud service providers and SaaS companies. The following maps the Common Criteria (CC) and supplemental criteria to framework evidence.

Criteria Description	Layer	Evidence Element	Coverage
Logical and Physical Access Controls: Implement logical access security software, infrastructure, and architectures	L1 / L2 / L3.2	TEE hardware isolation, IMA executable control, eBPF behavioral enforcement, KMS state-gated access, Attested Transport Binding (TB-1 through TB-6)	Full
The entity authorizes, modifies, or removes access based on authorization	L1 / Protocol	KMS grant/revoke based on attestation state, dead man's switch auto-revocation, TTL enforcement on grants	Full
The entity implements logical access security to protect against threats from external sources	L1 / L3.2	Attested Transport Binding (TB-1, TB-4), eBPF egress filtering, TEE boundary protection, denied_network rules	Full
Restrict the transmission, movement, and removal of information to authorized users and processes	L1 / L3.2	End-to-end encryption (AES-256-GCM), eBPF network allowlist, state-gated I/O pattern (keys revoked on FAIL)	Full
To meet its objectives, the entity uses detection and monitoring procedures	L3 / Protocol	Continuous 60s eBPF monitoring, kernel integrity checks, IMA runtime measurements, YANG Push alerting	Full
The entity monitors system components for anomalies indicative of malicious acts	L3.1 / L3.2	eBPF behavioral anomaly detection, kernel integrity monitoring, IMA runtime file change detection	Full
The entity evaluates detected anomalies to determine if they represent security events	Protocol	Appraiser engine (four-layer evaluation), PASS/ALERT/FAIL decision matrix, signed verdicts	Full
Confidentiality: The entity identifies and maintains confidential information	L1	TEE memory encryption (hardware), KMS-managed keys, AEAD for data artifacts, end-to-end encryption	Full

A.7 Implementation Guidance for Compliance Assertions

A.7.1 Compliance Assertion Token Format

When the Appraiser/Publisher issues a compliance control assertion, it SHOULD follow this structure:

Field	Type	Description
control_id	string	The control identifier from the source standard (e.g., "NIST-800-171:3.14.6")
framework_id	string	The compliance framework identifier (e.g., "CMMC-L2", "HIPAA", "PCI-DSS-4.0")
evidence_refs	array	List of evidence element identifiers that satisfy the control
layer_sources	array	Attestation layers from which evidence originates (e.g., ["L2", "L3.2"])
coverage_level	enum	"full", "partial", or "supportive"
cvm_id	string	Target Machine identifier
epoch_id	uint64	Current monotonic epoch from the attestation stream
timestamp	ISO 8601	Time of assertion generation
ttl_seconds	uint32	Assertion validity period (recommended: match attestation report interval)
provider_trust_stance	enum	"inclusive", "limited", or "independent". The Provider Trust Stance under which this assertion was issued (main framework Section 5.3). Required when the relying party's control mapping conditions on cloud service provider trust assumptions.
signature	base64	Post-quantum signature (e.g., ML-DSA per FIPS 204) over all preceding fields using the Publisher's attestation-bound signing key

A.7.2 Assertion Lifecycle

Compliance assertions are ephemeral by design. They represent the compliance posture at a specific point in time, tied to the current attestation epoch. An assertion expires when its TTL elapses, when the underlying attestation state changes (e.g., PASS to FAIL), or when the epoch_id advances beyond the assertion’s epoch.

Enterprise Validators consuming compliance assertions should verify that the epoch_id in the assertion matches or exceeds the last-seen epoch from the YANG Push stream. Assertions with stale epoch_ids should be rejected.

A.7.3 Limitations and Caveats

Organizations and assessors must understand the following limitations:

- This mapping covers technical controls only. A complete compliance program requires organizational, procedural, and physical controls that cannot be evidenced through attestation.

- Coverage levels are assessed against the control text as written. Individual assessors or auditors may interpret control requirements differently. This is meant as an initial foundation for public review.

- The mapping is illustrative. Organizations should perform their own control-by-control assessment to validate applicability to their specific environment and scoping decisions.

- Compliance assertions do not replace formal audits. They provide continuous, machine-verifiable evidence that complements periodic human assessments.

- The FIPS validation status of cryptographic implementations is deployment-specific and must be verified independently of this framework.

- Transport binding evidence references (TB-1 through TB-6) are platform-neutral requirements defined in the main framework. The specific attestation token format and key commitment mechanism vary by TEE platform and cloud provider.

- Workload identity frameworks such as SPIFFE / SPIRE may provide useful identity and authentication evidence, but they do not independently establish hardware trust, image integrity, runtime integrity, or transport binding to an End User session.

- Any compliance mapping that relies on SPIFFE / SPIRE should disclose whether identity issuance and renewal are gated by current attestation verdicts, and whether credential revocation is triggered automatically on FAIL.

A.7.4 Supplementary SPIFFE / SPIRE Identity Evidence Mappings

The following mappings are illustrative and supplementary. They describe where SPIFFE / SPIRE-derived evidence could support compliance assessment when integrated with the framework's attestation pipeline.

Framework / Control	SPIFFE / SPIRE Evidence	Relationship to Attestation	Suggested Coverage
NIST SP 800-171 3.5.1	SPIFFE ID, workload registration record, issued SVID	Supports service/workload identity, but does not establish platform trust by itself	Supportive

Framework / Control	SPIFFE / SPIRE Evidence	Relationship to Attestation	Suggested Coverage
NIST SP 800-171 3.5.2	mTLS using X.509-SVID or JWT-SVID, attestation-gated issuance policy	Stronger if issuance / renewal depends on PASS attestation state	Partial
NIST SP 800-53 IA-3	Workload or node identity issued by SPIRE, registration policy, short-lived credentials	Complements hardware attestation; does not replace it	Partial
HIPAA § 164.312(d)	Service identity credentials and mutual authentication between systems	Supports entity authentication in service-to-service paths	Partial
PCI DSS 8.3.1	Mutual authentication between components using short-lived SVIDS	Useful for internal component authentication; still requires deployment-specific policy	Partial
SOC 2 Logistical Access Controls	Workload identity issuance, rotation, and revocation records	Supports evidence of controlled service authentication and credential lifecycle	Supportive

Where SPIFFE / SPIRE is used, the strongest compliance posture is achieved when only workloads with current PASS verdicts receive or renew credentials, credentials are short-lived, revocation or non-renewal occurs automatically on FAIL, and issuance/revocation events are logged as auditable evidence. Even in such deployments, SPIFFE / SPIRE-derived evidence should be presented as complementary to attestation evidence rather than as a replacement for it.

A.7.5 Example Compliance Control Assertion Tokens

The following examples illustrate machine-readable compliance assertions for controls with full coverage across three distinct compliance frameworks:

Example 1:
CMMC Level 2 / NIST 800-171: Cryptographic Mechanisms for Remote Access

```json
{
 "control_id":      "NIST-800-171:3.1.13",
 "framework_id":    "CMMC-L2",
 "evidence_refs": [
   "tls-1.3-tee-termination",
   "attested-transport-binding:TB-1",
   "attested-transport-binding:TB-2",
   "attested-transport-binding:TB-3",
   "aes-256-gcm-payload-encryption"
 ],
 "layer_sources":   ["L1"],
 "coverage_level":  "full",
 "cvm_id":          "cvm-us-east1-a-7f3b2a",
 "epoch_id":        412,
 "timestamp":       "2026-03-18T14:32:07.491Z",
 "ttl_seconds":     60,
 "signature":       "MEUCIQDk8VqL3nRf...yXwGp4a7T1c="
}
```

Example 2:
NIST SP 800-53 Rev. 5: Software, Firmware, and Information Integrity

```json
{
 "control_id": "NIST-800-53:SI-7",
 "framework_id": "NIST-800-53-R5",
 "evidence_refs": [
   "hw-boot-measurement",
   "ima-file-integrity",
   "container-digest-verification",
   "kim-syscall-table-validation",
   "kim-idt-validation",
   "kim-module-list-validation",
   "sigstore-signature-verification"
 ],
 "layer_sources": ["L1", "L2", "L3.1"],
 "coverage_level": "full",
 "cvm_id": "cvm-us-east1-a-7f3b2a",
 "epoch_id": 413,
 "timestamp": "2026-03-18T14:33:07.491Z",
 "ttl_seconds": 60,
 "signature": "MEQCIHr9TmN0aWvB...Kd2Lx8f0jQw="
}
```

Example 3:
PCI DSS v4.0.1: Protect Audit Logs from Modification

JSON


```
{
 "control_id": "PCI-DSS:10.3.1",
 "framework_id": "PCI-DSS-4.0",
 "evidence_refs": [
   "transparency-log-merkle-tree",
   "publisher-event-signatures",
   "public-auditability-endpoint"
 ],
 "layer_sources": [
   "Protocol",
   "L1"
 ],
 "coverage_level": "full",
 "cvm_id": "cvm-us-east1-a-7f3b2a",
 "epoch_id": 414,
 "timestamp": "2026-03-18T14:34:07.491Z",
 "ttl_seconds": 60,
 "signature": "MEUCIFbWo3Aj7RpQ...Ym5Nv6hS2kE="
}
```

A.8 Future Work

The following extensions to this annex are planned:

- Compute system stack-based model for understanding the application and use of attestation capabilities to IaaS, PaaS, SaaS Providers and Consumers, App Hosters, and Application Consumers.
- Detailed mapping to CMMC 2.0 Level 3 additional controls (based on NIST 800-172).
- Mapping to FedRAMP High baseline controls, including FedRAMP-specific requirements for cloud service providers.
- Development of machine-readable mapping files (JSON/YAML) that can be loaded into Appraiser implementations to enable automated compliance assertion generation.
- Composite posture-level assertions that bundle individual control assertions into a single signed claim (e.g., “CMMC Level 2 – all mapped technical controls PASS”).

A.9 Abbreviations and Acronyms

Term	Definition
AICPA	American Institute of Certified Public Accountants
C3PAO	Certified Third-Party Assessment Organization
CC	Common Criteria
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
DSS	Data Security Standard
ePHI	Electronic Protected Health Information
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act
ID	Identifier
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
SOC 2	System and Organization Controls 2
SP	Special Publication
SPIFFE	Secure Production Identity Framework for Everyone
SPIRE	SPIFFE Runtime Environment
TEE	Trusted Execution Environment
TTL	Time To Live
YAML	YAML Ain't Markup Language
YANG	Yet Another Next Generation