Axis Edge Vault
Certification Practices Statement

March 2023

TABLE OF CONTENTS

1 INTRODUCTION

Axis Communications AB ('Axis') operates a public key infrastructure (PKI) environment, the Axis Product PKI, that provides Certification Authority (CA) services for the signing and issuing of certificates installed in Axis hardware products. The certificates are unique to each product and, by having Axis as the signing authority, their purpose is to provide assurance of the origin of Axis products.

The Certificate Authorities (CAs) within the scope of this Certification Practices Statement (CPS) are those responsible for the signing and issuance of Axis Device ID certificates in accordance with the IEEE 802.1AR standard as well as those for signing and issuing Axis Edge Vault Attestation Certificates to verify the storage location of the Axis Device ID private key.

The Axis Device ID CA is responsible for performing all public key life cycle functions including, but not limited to:

- processing Axis Device ID certificate requests,
- issuing and revoking Axis Device ID certificates,

The Axis Edge Vault Attestation CA is responsible for performing all public key lifecycle functions including, but not limited to:

- processing Axis Edge Vault Attestation certificate requests
- issuing and revoking Axis Edge Vault Attestation certificates

1.1 Overview

This document describes the Certification Practice Statement (CPS) as it applies to the PKI infrastructure used to sign and distribute Axis Device ID and Axis Edge Vault Attestation certificates into Axis hardware products having support for the Axis Edge Vault hardware. This CPS sets forth the specific technical and operational practices for the Axis Device ID CA and Axis Edge Vault Attestation CA. The overarching legal, business and general technical requirements can be found in the accompanying Axis Product PKI Certificate Policy (CP) document.

This document is structured according to RFC 3647 "Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework" [RFC3647]. In accordance with RFC 3647, this CPS is organized using numbered paragraphs. Paragraphs that do not apply to the Axis Device ID CA and Axis Edge Vault CA will be marked with either "Does not apply" or "No additional stipulation". Paragraphs that are addressed in the Axis Product PKI CP document will indicate so with "Details are provided in the corresponding CP". The structure and information included in this document is intended to satisfy the CPS requirements for conformance to the IEEE 802.1AR standard.

Axis' Policy Management Authority (PMA) continuously tracks changes in Axis' policies and incorporates the required changes to updated versions of this document before the proposed changes take effect.

1.2 Document name and identification

1.2.1 Document Identification Number

The OID assigned to Axis Communications by IANA is iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Axis (368).

A special OID arc has been allocated by Axis for Certification Practices Statements.

Iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Axis (368) certificateServices (10) certificationPracticesStatements (2)

The globally unique Identification Number (OID) of the Axis CP (this document is therefore:

1.3.6.1.4.1.368.10.2.1.1.0

OID Arc	Description
1.3.6.1.4.1.368	IANA unique OID for Axis Communications AB
10	Certificate Services
2	Certification Practice Statements
1	CPS-specific Identifier (Axis Edge Vault)
1.0	First and second digit of version number of this document

Version Control

Version	Date	Change Information
1.0	February 8, 2023	First Release

1.2.2 Document Name

The naming of this document as “Axis_EdgeVault_Certification_Practices_Statement” is to assert the application of this CPS to certificates stored and utilized within the ‘AXIS Edge Vault’ secure key store supported in select Axis Hardware products.

1.3 PKI participants

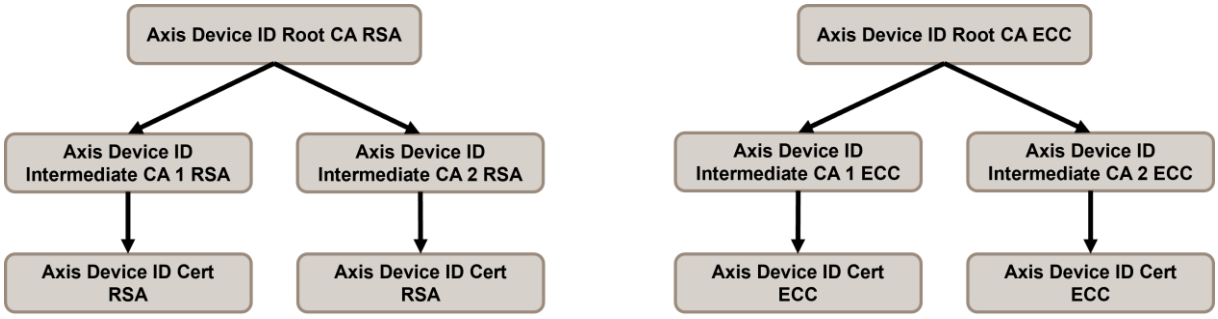
PKI participants include Certification Authorities, Subscribers, End Entities, and Relying Parties.

The Axis Device ID CA hierarchy is intended to be used as a trust anchor for signing Device ID certificates in accordance with requirements set forth in the IEEE 802.1AR standard.

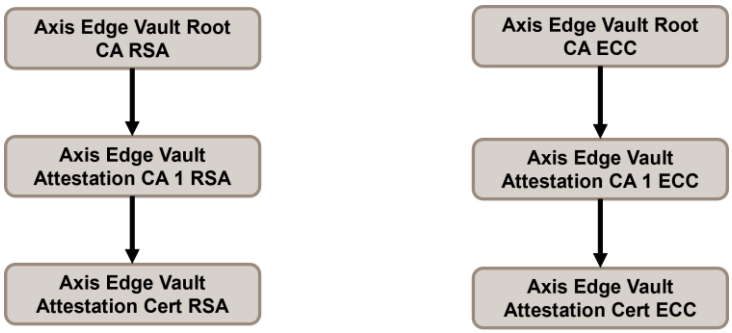
The Axis Edge Vault Attestation CA is intended as a trust anchor to support issuance of signed attestation reports from Axis devices.

The following diagram outlines the PKI hierarchy in scope for this CPS:

Axis Device ID CA hierarchy



Axis Edge Vault CA hierarchy



1.3.1 Certification authorities

This Axis Device ID and Axis Edge Vault Attestation CAs have two-tier CA structures with the Root CA as an offline trust anchor and subordinate Intermediate CAs used to sign the End Entity (Axis Device ID or Edge Vault Attestation) certificates.

- **Axis Device ID/Edge Vault Root CA** – there are both RSA (2048) and ECC (p256) versions of the private key and corresponding public key certificate. The Root CA performs the signing, issuance, and revocation tasks to establish their Intermediate CA counterparts (for RSA and ECC). The private keys are stored offline in a FIPS 140-2 Level 3 hardware security module (HSM) appliance which itself is stored in a secure vault.

- **Axis Device ID/Edge Vault Attestation Intermediate CA** – also exists in RSA (2048) and ECC (P256) versions. The Intermediate CAs sign and issue the Device ID or Edge Vault Attestation certificates which are imported into the Axis device having possession of the corresponding private key. The intermediate CA private keys are stored in a FIPS 140-2 Level 3 network HSM and available online for access to certificate signing functionality during normal operations.

1.3.2 Subscriber

Subscribers are Axis employees (or credentialed employees from manufacturing facilities contracted by Axis) that submit the Certificate Application for End Entity certificates and subsequently ensure the signed End Entity certificate is imported into the appropriate device.

A Subscriber's responsibilities include:

1. provide complete, accurate and truthful information in a Certificate Application,
2. request the revocation of the End Entity certificate when the certificate contains incorrect information or Subscriber's Private Key or the Activation Data controlling its access has been lost or when Subscriber has reason to believe that the Private Key has been accessed by another individual or otherwise compromised,
3. acknowledgement of receipt or assent to Subscriber responsibilities.

1.3.3 End Entities

End entities are the Axis hardware products. They are always:

- named or identified in the respective element of the Certificate issued to this entity

- owner of the private key corresponding to the public key listed in the Certificate

End Entities' responsibilities include:

- protection of the private key information within its secure key store, and
- presenting the public key certificate and CA certificate chain for use in approved use cases.

1.3.4 Relying parties

Relying parties are Axis' customers who install Axis hardware products in their IT infrastructure and require assurance that the product originates from Axis. To facilitate assurance, all CA public key certificates are made publicly available (see Section 2.1). The responsibilities of the relying party include:

1. Using the Certificates only for the applications supported by the CA and defined in the corresponding CPS,
2. use only Key Pairs bound to valid Certificates, and
3. cease use of the Private Key after revocation or expiration of the Certificate

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by the Axis Device ID or Axis Edge Vault Attestation CAs under the guidelines of this CPS and corresponding CP shall only be used for the purposes designated in the Key Usage or Extended Key Usage fields of their respective certificate profiles.

1.4.2 Prohibited certificate uses

All uses not listed 1.4.1 are considered prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

Axis Communications AB
Gränden 1, SE 223 69 Lund, Sweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
Email: support-pki@axis.com
Website: www.axis.com/support/pki-repository

1.5.2 Contact person

Product Owner – Certificate and Key Management
Gränden 1, SE 223 69 Lund, Sweden
Email: support-pki@axis.com

1.5.3 Person determining CPS suitability for the policy

The Commercial IT Capabilities (CITC) group at Axis Communications defines the CP and the suitability of the CPS for the PKI environment scoped in this document.

1.5.4 CPS approval procedures

The procedure for approval includes a risk assessment examining the business requirements, suitability with respect to applicable standards, and the needs of the relying parties. The CP and CPS are reviewed annually for accuracy and to reflect any changes made to the underlying architecture and processes.

This document is accepted and approved by the CIO of Axis Communications AB.

1.6 Definitions and acronyms

1.6.1 Acronyms

Axis – Axis Communications AB

CA – Certificate Authority

CP – Certificate Policy

CPS – Certification Protection Statement

ECC – Elliptic curve cryptography

PKI – Public key infrastructure

RPO - Recovery Point Objective

RSA – Rivest-Shamir-Adelman cryptography

RTO – Recovery Time Objective

TSP – Trust Services Provider

1.6.2 Definitions

AXIS Device ID: a digital identity cryptographically bound to the device and installed in AXIS Edge Vault during production that fulfills the requirements of the IDevID as defined in the IEEE 802.1AR standard.

AXIS Edge Vault: a secure cryptographic compute module (secure module or secure element) in which the Axis device ID is securely and permanently installed and stored.

Certificate: A digitally signed object that binds information identifying an entity that possesses a secret private key to the corresponding public key.

Certificate chain: An ordered list of intermediate certificates that links an end entity certificate (Axis Device ID) to a trust anchor.

Certification authority (CA): An entity that issues X.509 digital certificates.

Public Key Infrastructure: A set of network entities and the roles, policies, and procedures that govern the creation, distribution, use, storage, and revocation of X.509 digital certificates.

Public Key Hierarchy: A relationship between systems supporting a PKI, where systems with a role associated with a tier in the hierarchy can delegate authority to a system or systems whose role is associated with an immediately lower tier.

Secure Key Store – a storage module supporting advanced security functionality for the secure storage of private keys and other secrets.

Trust anchor: A CA that is trusted and for which the trusting party holds information, usually in the form of a self-signed certificate issued by the trust anchor.

Trust Services Provider - is a person or legal entity providing and preserving digital certificates to create and validate electronic signatures and to authenticate their signatories.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Axis provides a publicly accessible webpage at www.axis.com/support/pki-repository that serves as a repository of information relevant to the operation of the Axis Product PKI.

2.2 Publication of certification information

Information published in the repository related to this CPS may include:

- Updated versions of the Axis Product PKI CP and this CPS document,
- Public key certificates for the Axis Device ID and Axis Edge Vault Attestation Root and Intermediate CA's,
- Archived public keys certificates for revoked Root and Intermediate CAs,
- Certificate Revocation information for certificates issued by Axis Device ID and Axis Edge Vault CAs,
- Contact information for responsible parties at Axis Communications.

2.3 Time or frequency of publication

Information is published to the repository as soon as it is made available. The general requirements are:

- All updates to CP and CPS documents shall be published before the changes take effect,
- New public key certificates shall be published before their private keys are activated,
- Certificate revocation information (if applicable) shall be updated at least monthly.

2.4 Access controls on repositories

Repositories are made available on a publicly accessible webpage and exclusively in read-only format.

3 IDENTIFICATION AND AUTHENTICATION (11)

3.1 Naming

3.1.1 Types of names

Specified in the Certificate Policy.

3.1.2 Need for names to be meaningful

Specified in the Certificate Policy.

3.1.3 Anonymity or pseudonymity of subscribers

Specified in the Certificate Policy.

3.1.4 Rules for interpreting various name forms

Specified in the Certificate Policy.

3.1.5 Uniqueness of names

Specified in the Certificate Policy.

3.1.6 Recognition, authentication, and role of trademarks

Specified in the Certificate Policy.

3.2 Initial identity validation

Specified in the Certificate Policy.

3.2.1 Method to prove possession of private key

Specified in the Certificate Policy.

3.2.2 Authentication of organization identity

Specified in the Certificate Policy.

3.2.3 Authentication of individual identity

Specified in the Certificate Policy.

3.2.4 Non-verified subscriber information

Specified in the Certificate Policy.

3.2.5 Validation of authority

Specified in the Certificate Policy.

3.2.6 Criteria for interoperation

Specified in the Certificate Policy.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Specified in the Certificate Policy.

3.3.2 Identification and authentication for re-key after revocation

Specified in the Certificate Policy.

3.3.3 Identification and authentication for revocation request

Specified in the Certificate Policy.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Specified in the Certificate Policy.

4.1.2 Enrollment process and responsibilities

Specified in the Certificate Policy.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Specified in the Certificate Policy.

4.2.2 Approval or rejection of certificate applications

Specified in the Certificate Policy.

4.2.3 Time to process certificate applications

Specified in the Certificate Policy.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Specified in the Certificate Policy.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Specified in the Certificate Policy.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Specified in the Certificate Policy.

4.4.2 Publication of the certificate by the CA

Specified in the Certificate Policy.

4.4.3 Notification of certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.5 4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Specified in the Certificate Policy.

4.5.2 Relying party public key and certificate usage

Specified in the Certificate Policy.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Specified in the Certificate Policy.

4.6.2 Who may request renewal

Specified in the Certificate Policy.

4.6.3 Processing certificate renewal requests

Specified in the Certificate Policy.

4.6.4 Notification of new certificate issuance to subscriber

Specified in the Certificate Policy.

4.6.5 Conduct constituting acceptance of a renewal certificate

Specified in the Certificate Policy.

4.6.6 Publication of the renewal certificate by the CA

Specified in the Certificate Policy.

4.6.7 Notification of certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.7 Certificate re-key

Specified in the Certificate Policy.

4.7.1 Circumstance for certificate re-key

Specified in the Certificate Policy.

4.7.2 Who may request certification of a new public key

Specified in the Certificate Policy.

4.7.3 Processing certificate re-keying requests

Specified in the Certificate Policy.

4.7.4 Notification of new certificate issuance to subscriber

Specified in the Certificate Policy.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Specified in the Certificate Policy.

4.7.6 Publication of the re-keyed certificate by the CA

Specified in the Certificate Policy.

4.7.7 Notification of certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.8 Certificate modification

Specified in the Certificate Policy.

4.8.1 Circumstance for certificate modification

Specified in the Certificate Policy.

4.8.2 Who may request certificate modification

Specified in the Certificate Policy.

4.8.3 Processing certificate modification requests

Specified in the Certificate Policy.

4.8.4 Notification of new certificate issuance to subscriber

Specified in the Certificate Policy.

4.8.5 Conduct constituting acceptance of modified certificate

Specified in the Certificate Policy.

4.8.6 Publication of the modified certificate by the CA

Specified in the Certificate Policy.

4.8.7 Notification of certificate issuance by the CA to other entities

Specified in the Certificate Policy.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Specified in the Certificate Policy.

4.9.2 Who can request revocation

Specified in the Certificate Policy.

4.9.3 Procedure for revocation request

Specified in the Certificate Policy.

4.9.4 Revocation request grace period

Specified in the Certificate Policy.

4.9.5 Time within which CA must process the revocation request

Specified in the Certificate Policy.

4.9.6 Revocation checking requirement for relying parties

Specified in the Certificate Policy.

4.9.7 CRL issuance frequency (if applicable)

Specified in the Certificate Policy.

4.9.8 Maximum latency for CRLs (if applicable)

Specified in the Certificate Policy.

4.9.9 On-line revocation/status checking availability

Specified in the Certificate Policy.

4.9.10 On-line revocation checking requirements

Specified in the Certificate Policy.

4.9.11 Other forms of revocation advertisements available

Specified in the Certificate Policy.

4.9.12 Special requirements re key compromise

Specified in the Certificate Policy.

4.9.13 Circumstances for suspension

Specified in the Certificate Policy.

4.10 Certificate status services

4.10.1 Operational characteristics

Specified in the Certificate Policy.

4.10.2 Service availability

Specified in the Certificate Policy.

4.10.3 Optional features

Specified in the Certificate Policy.

4.11 End of subscription

Specified in the Certificate Policy.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Specified in the Certificate Policy.

4.12.2 Session key encapsulation and recovery policy and practices

Specified in the Certificate Policy.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)

5.1 Physical controls

5.1.1 Site location and construction

Specified in the Certificate Policy.

5.1.2 Physical access

Specified in the Certificate Policy.

5.1.3 Power and air conditioning

Specified in the Certificate Policy.

5.1.4 Water exposures

Specified in the Certificate Policy.

5.1.5 Fire prevention and protection

Specified in the Certificate Policy.

5.1.6 Media storage

Specified in the Certificate Policy.

5.1.7 Waste disposal

Specified in the Certificate Policy.

5.1.8 Off-site backup

Specified in the Certificate Policy.

5.2 Procedural controls

5.2.1 Trusted roles

Specified in the Certificate Policy.

5.2.2 Number of persons required per task

Specified in the Certificate Policy.

5.2.3 Identification and authentication for each role

Specified in the Certificate Policy.

5.2.4 Roles requiring separation of duties

Specified in the Certificate Policy.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Specified in the Certificate Policy.

5.3.2 Background check procedures

Specified in the Certificate Policy.

5.3.3 Training requirements

Specified in the Certificate Policy.

5.3.4 Retraining frequency and requirements

Specified in the Certificate Policy.

5.3.5 Job rotation frequency and sequence

Specified in the Certificate Policy.

5.3.6 Sanctions for unauthorized actions

Specified in the Certificate Policy.

5.3.7 Independent contractor requirements

Specified in the Certificate Policy.

5.3.8 Documentation supplied to personnel

Specified in the Certificate Policy.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Specified in the Certificate Policy.

5.4.2 Frequency of processing log

Specified in the Certificate Policy.

5.4.3 Retention period for audit log

Specified in the Certificate Policy.

5.4.4 Protection of audit log

Specified in the Certificate Policy.

5.4.5 Audit log backup procedures

Specified in the Certificate Policy.

5.4.6 Audit collection system (internal vs. external)

Specified in the Certificate Policy.

5.4.7 Notification to event-causing subject

Specified in the Certificate Policy.

5.4.8 Vulnerability assessments

Specified in the Certificate Policy.

5.5 Records archival

5.5.1 Types of records archived

Specified in the Certificate Policy.

5.5.2 Retention period for archive

Specified in the Certificate Policy.

5.5.3 Protection of archive

Specified in the Certificate Policy.

5.5.4 Archive backup procedures

Specified in the Certificate Policy.

5.5.5 Requirements for time-stamping of records

Specified in the Certificate Policy.

5.5.6 Archive collection system (internal or external)

Specified in the Certificate Policy.

5.5.7 Procedures to obtain and verify archive information

Specified in the Certificate Policy.

5.6 Key changeover

Specified in the Certificate Policy.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Specified in the Certificate Policy.

5.7.2 Computing resources, software, and/or data are corrupted

Specified in the Certificate Policy.

5.7.3 Entity private key compromise procedures

Specified in the Certificate Policy.

5.7.4 Business continuity capabilities after a disaster

Specified in the Certificate Policy.

5.8 CA or RA termination

Specified in the Certificate Policy.

6 TECHNICAL SECURITY CONTROLS (11)

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Root and Intermediate CA key pairs

Key pairs for the Root and Intermediate CA's are generated inside a FIPS 140-2 Level 3 HSM appliance using a "Key Ceremony" procedure under dual supervision to ensure secure generation and storage of the private keys.

6.1.1.2 Axis Device ID and Edge Vault Attestation key pairs

Key pairs for the Axis Device ID and Edge Vault Attestation are generated by the manufacturer of the Axis Edge Vault Secure Element chip during production with the private key remaining on the device and the public key provided to Axis over a secure channel for use in the certificate generation and signing process.

6.1.2 Private key delivery to subscriber

All private keys are generated within the hardware device and are never transmitted outside their secure key store.

6.1.3 Public key delivery to certificate issuer

For the CA components, public keys are provided to the certificate issuer in the form of a PKCS#10 Certificate Signing Request (CSR). The CSRs are generated within the HSM for all subordinate CA certificates as part of the Key Ceremony and subsequently signed by Root certificate.

The RSA and ECC public keys for Device ID and Edge Vault Attestation key pairs are delivered by the manufacturer during production of AXIS Edge Vault hardware modules over an encrypted channel as part of a contracted provisioning service. A PKCS #10 CSR is generated by the Axis Certificate Creation Service (ACCS) using the public key and the certificate template outlined in Section 7.

6.1.4 CA public key delivery to relying parties

The Axis Device ID and Edge Vault Attestation certificate validation chains are made available to relying parties on the Axis public repository specified in Section 2. The certificate validation chains are also stored on the device to support automated verification procedures.

6.1.5 Key sizes

Certificates meet the following requirements for algorithm type and key sizes:

Root CA Certificates	
Algorithm Type	RSA or ECDSA
Digest Algorithm	SHA-256, SHA-384, SHA-512
Minimum RSA modulus size	2048 bits
ECC curve for ECDSA	NIST P-256, P-384, P-512

Intermediate CA Certificates	
Algorithm Type	RSA or ECDSA
Digest Algorithm	SHA-256, SHA-384, SHA-512

Minimum modulus size (RSA)	2048 bits
ECC curve	NIST P-256, P-384, P-512

End Entity Certificates	
Algorithm Type	RSA or ECDSA
Digest Algorithm	SHA-256, SHA-384, SHA-512
Minimum RSA modulus size	2048 bits
ECC curve for ECDSA	NIST P-256, P-384, P-512

6.1.6 Public key parameters generation and quality checking

All asymmetric key pairs for CA signing certificates are generated in FIPS 140-2 Level 3 compliant HSM appliances and subject to signing key parameter checking as outlined in FIPS 186-4 for ECDSA and RSA algorithms used.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Private Keys corresponding to the Root CA certificates are not used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself,
2. Certificates for Subordinate CAs,
3. CRL signing (if applicable)
4. OCSP Response verification (if applicable).

Private keys corresponding to Intermediate CA certificates are used for

1. End Entity certificate signing
2. CRL signing (if applicable)
3. OCSP Response verification (if applicable)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The cryptographic hardware security modules (HSM) used to protect the Axis Device ID and Axis Edge Vault Attestation CA private keys are certified to FIPS 140-2 Level 3.

6.2.2 Private key (n out of m) multi-person control

All generation of the asymmetric key pairs for Root and Intermediate CAs and signing operations using the Root CA private key are performed within the HSM under n of m control where n = 2 and m = 3 (dual control).

6.2.3 Private key escrow

Private key escrow is not implemented in this PKI environment.

6.2.4 Private key backup

Private keys for the Root CA are stored offline on a USB HSM appliance with a mirrored back-up HSM appliance also stored offline. Both the primary and back-up keys are kept in secure storage at separate locations.

Private keys for the Intermediate CA are stored on a network HSM with a back-up stored on a dedicated back-up HSM secured in a separate physical location.

6.2.5 Private key archival

Private key archiving is not implemented for this PKI environment.

6.2.6 Private key transfer into or from a cryptographic module

All private/public key pairs are generated on the HSM appliance where they will be used and are not transferred between cryptographic modules.

6.2.7 Private key storage on cryptographic module

All primary and back-up private keys are stored encrypted on their respective HSM appliance.

6.2.8 Method of activating private key

A Root CA private key can be activated via PED (pin enabled device) authentication under dual control.

6.2.9 Method of deactivating private key

A Root CA private key is de-activated when the PED keys are removed from the appliance.

6.2.10 Method of destroying private key

The Root CA and Intermediate CA private keys are destroyed within the HSM appliance when the private key is no longer needed or the corresponding certificate has expired. Destruction is achieved using a standard delete command within the HSM and is executed in compliance with the FIPS 140-2 standard.

Destruction of CA private keys can only be achieved by authorized staff possessing the required PED key and working under dual control.

6.2.11 Cryptographic Module Rating

The cryptographic module (HSM) operates using firmware certified to FIPS 140-2 Level 3.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys corresponding to revoked private keys are archived and backed-up within the HSM appliance with public key certificates being available for signature validation during the operational lifetime of the end entity certificates. All actively used public certificates are published in the repository described in Section 2.1.

6.3.2 Certificate operational periods and key pair usage periods

The CA certificates are valid for a period of 15 years with the private key having a operational period corresponding to approximately half the certificate validity period.

6.4 Activation data

Activation data in the context of the Axis Device ID and Axis Edge Vault Attestation CAs is in the form of PIN enabled devices (PED) which are used to authenticate users occupying Trusted Roles on the HSM.

6.4.1 Activation data generation and installation

Activation data is generated during initial configuration of the HSM appliance and provided to select administrators occupying Trusted Roles as defined in Section 5.2.1 of the corresponding CP.

6.4.2 Activation data protection

Activation data protection complies with FIPS 140-2 Level 3. Individual users are provided with recommendations on secure storage of activation data but are ultimately responsible for protecting their PIN number and the physical key they are entrusted with.

6.4.3 Other aspects of activation data

No stipulation here.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All computers and physical hardware deployed within the scope of this CPS are subject to the technical security requirements outlined in Axis' ISMS in accordance with ISO 27001.

6.5.2 Computer security rating

No computer security rating is specified.

6.6 Life cycle security controls

6.6.1 System development controls

All system development in the form of software integrations making certificate signing requests to the HSM appliance follows the Axis Security Development Model (ASDM). More information on this model can be found at the following URL: https://www.axis.com/files/manuals/gd_asdm_axis_security_development_model_en_2202_hi.pdf

6.6.2 Security management controls

Security management controls for the operation of Axis' Certificate Authorities are defined in Axis' Lifecycle Management Policy for hardware products, a component of Axis' ISO 27001 certified ISMS.

6.6.3 Life cycle security controls

Security controls are audited annually as part of Axis' ISO 27001 compliance.

6.7 Network security controls

The Axis Device ID and Axis Edge Vault Attestation Root CA are kept offline with no connection to network resources.

6.8 Time-stamping

All hardware device logs, certificate signing processes and key ceremony events are time stamped and stored in a centralized logging database.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate profiles for CA certificates are in the form of X.509 version 3 certificates as described in IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

Axis Device ID certificates follow the X.509 v3 standard and support the relevant fields for conformance with IEEE 802.1AR. For more information regarding the implementation of the Axis Device ID certificate, see Appendix A, “PICS Proforma for IEEE 802.1AR”.

7.1.1 Version number(s)

Only X.509 version 3 certificates are supported.

7.1.2 Certificate extensions

7.1.2.1 Root and Intermediate CA Certificates

The following certificate extensions are supported with their associated criticality

Extension	Criticality
Authority Key Identifier	Non-critical
Subject Key Identifier	Non-critical
Basic Constraints	Critical

7.1.2.2 Device ID and Axis Edge Vault Attestation Certificates

The following extensions are supported with their associated criticality:

Extension	Criticality
Authority Key Identifier	Non-critical
Subject Alternative Name	Non-critical

7.1.3 Algorithm object identifiers

In the “Subject Public Key Info” field the following supported algorithms are defined by the associate OID values:

Algorithm	OID
RSA-2048/SHA-256	1.2.840.113549.1.1.1
ECDSA P-256/SHA-256	1.2.840.10045.3.1.7
ECDSA P-384/SHA-384	1.3.132.0.34

7.1.4 Name forms

Name forms for both CA and Device ID certificates are specified in Section 3.1 of the Certificate Policy. For Device ID certificates, names must follow the convention of:

“axis-<serialNumber>->crytographicSuite>” for example: “axis-accc8e56a87f-eccp256”

7.1.5 Name constraints

No stipulation

7.1.6 Certificate policy object identifier

No stipulation

7.1.7 Usage of Policy Constraints extension

No stipulation

7.1.8 Policy qualifiers syntax and semantics

No stipulation

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation

7.2 CRL profile

Not applicable

7.2.1 Version number(s)

No stipulation

7.2.2 CRL and CRL entry extensions

No stipulation

7.3 OCSP profile

Not applicable

7.3.1 Version number(s)

No stipulation

7.3.2 OCSP extensions

No stipulation

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Specified in the Certificate Policy

9 OTHER BUSINESS AND LEGAL MATTERS

This document is provided “as is” without warranty of any. This document is not intended to, and shall not, create any legal obligation for Axis and/or any of its affiliates. Furthermore, all certificates and any related software and services are provided "as is" and "as available”. To the maximum extent permitted by law, Axis disclaims all express and implied warranties, including all warranties of merchantability, fitness for a particular purpose, and non-infringement. Axis does not warrant that this document or any service or product will meet any expectations or that access to certificates will be timely or error-free.