# Axis Communications
# Product PKI Certificate Policy

March 2023

# TABLE OF CONTENTS

# 1 INTRODUCTION

Axis Communications AB ('Axis') operates a Public Key Infrastructure (PKI) environment, hereby termed 'Axis Product PKI', whose purpose is to serve as a trust anchor for issuing digitally signed public key certificates to Axis' commercial hardware products. The digitally signed certificates serve as cryptographically-bound product identifiers, allowing customers to verify the origin of the products they purchase from Axis prior to installation in their IT environments.

The Certificate Authorities (CAs) within the scope of this document are responsible for performing all public key life cycle functions including, but not limited to:

- processing certificate requests,
- issuing, revoking and renewing digital certificates,
- maintaining and publishing Certificate Revocation Lists (CRLs) for relying parties.

The Axis Product PKI supports the generation of two types of digital certificates for the purposes described above:

- **Axis Device ID certificates**, in conformance with IEEE 802.1AR
- **Axis Edge Vault Attestation certificates**

All certificates are generated by Axis in the role of Trusted Service Provider (TSP) for use in Axis products following the requirements outlined in this Certificate Policy (CP). Further detailed information regarding the practices used for individual certificate types can be found in the corresponding Certification Practices Statements (CPS).

## 1.1 Overview

This document describes the Certificate Policy (CP) as it applies to the lifecycle of the Axis Product PKI environment. This CP sets forth the business requirements, legal requirements as well as the overarching technical and security operations requirements that apply to all certificates issued by the Certificate Authorities within the Axis Product PKI environment. The corresponding Certificate Practices Statements (CPS) complement this document by addressing specific technical and operational practices as they apply to individual certificate use cases.

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 CP is organized using numbered paragraphs. Paragraphs that do not apply to the Axis Product PKI will be marked with either "Does not apply" or "No additional stipulation". Paragraphs that are addressed in the CPS document will indicate so with "Details are provided in the corresponding CPS".

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 Certificate Policy statements:

iso (1) org (3) dod (6) internet (1) private (4) enterprise (1) Axis (368) certificateServices (10) certificatePolicy (1)

The globally unique Identification Number (OID) of this Certificate Policy is therefore:

**1.3.6.1.4.1.368.10.1.1.1.0**

| OID Arc | Description |
|---|---|
| **1.3.6.1.4.1.368** | IANA unique OID for Axis Communications AB |
| **10** | Certificate Services |
| **1** | Certificate Policy |
| **1** | CP-specific identifier (Product PKI) |
| **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_ProductPKI_CertificatePolicy" is to assert that this Certificate Policy applies only to the Product PKI environment whose CA's issue certificates that provide assurance to Relying Parties (customers) that purchase commercial hardware products from Axis. For PKI environments specific to Axis' internal IT systems, wherein the Relying Parties are solely Axis employees or individuals contracted by Axis, a separate CP applies.

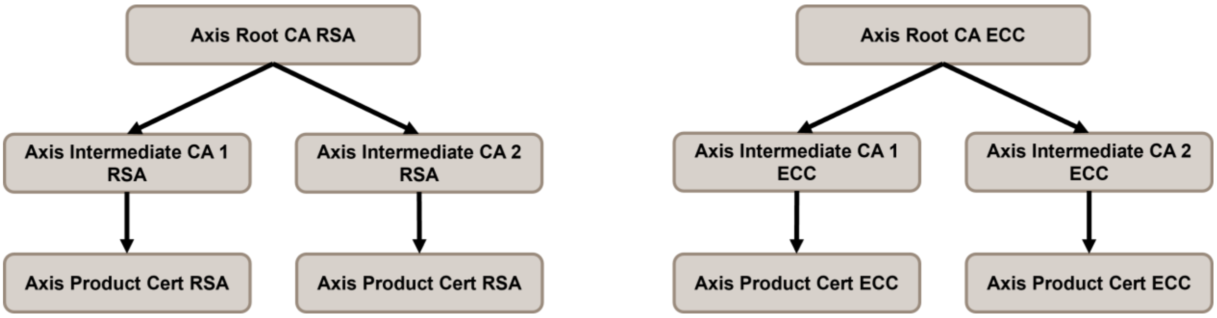
## 1.3 PKI participants

PKI participants include Certification Authorities, Subscribers, End Entities, and Relying Parties. The Axis Product PKI is intended to serve as a trust anchor for certificate signing services used to verify the identity of commercially available hardware products.

Details of the specific PKI hierarchies and certificate use cases in scope are found in the corresponding Certification Practices Statements (CPS).

### 1.3.1 Certification authorities

The Axis Product PKI utilizes a two-tier CA structure with a root CA that is stored offline, and an online Intermediate CA used to sign and issue the End Entity certificates. The diagram below outlines a generic example of the PKI hierarchy.



- **Axis Root CA** – there shall be an RSA, ECC or both versions of the root certificate depending on the needs of the certificate use case. The root private keys perform 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) that is housed in a secure location.

- **Axis Intermediate CA** – may exist in RSA, ECC or both versions depending on format of the Root CA. Intermediate CA private keys sign and issue End Entity certificates at the request of Subscribers. The Intermediate CA private keys are stored in a FIPS 140-2 Level 3 network HSM for online 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 shall 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 Product PKI under the guidelines of this CP and the corresponding CPS 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

Certificates issued by the Axis Product PKI may not be used for any purpose outside of what is listed in its certificate profile.

## 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

IT 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 defines the CP and the suitability of the CPS for the PKI environment scoped in this CP.

### 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 PKI architecture and processes.

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

## 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 to a trust anchor.

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

**Public Key Infrastructure (PKI)**: 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 shall provide 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 shall include, but not be limited to:

- Updated versions of all available CP and CPS documents,
- Public key certificates of all active CA hierarchies,
- Archived public keys certificates for revoked CA hierarchies,
- Certificate Revocation information,
- 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 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

This section outlines the general naming requirements for certificates issued by the Axis Product PKI. A more detailed formula for naming End Entity certificates is documented in Section 7.1.4 of the respective CPS document.

### 3.1.1 Types of names

All Axis Product PKI Certificates adhere to rules for naming and identification and shall require a Distinguished Name that is in compliance with the ITU X.500 standard for Distinguished Names (DN). Names shall be interpreted using the X.500 and RFC822 standards.

### 3.1.2 Need for names to be meaningful

The Common Name (CN) must be stated as the full name of the CA. A CA name indicates its purpose. For example, “Axis Device ID Intermediate CA” is a subordinate CA to the “Axis Device ID Root CA”.

### 3.1.3 Anonymity or pseudonymity of subscribers

The use of pseudonyms for CA or EE names is not permitted.

### 3.1.4 Rules for interpreting various name forms

No special rules

### 3.1.5 Uniqueness of names

Certificate names shall be unique and based on the following rules:

- **Root CA certificates** – named based on functionality and cryptographic suite. For example “Axis Device ID Root CA RSA”.
- **Intermediate CA certificates** – named based on functionality and cryptographic suite and iterated with a number for each generation of CA. For example “Axis Device ID Intermediate CA RSA 2”.
- **End Entity certificates** –the name includes a unique Axis serial number (SN) of the hardware product or a serial number identifying the Axis Edge Vault module installed in the product.

### 3.1.6 Recognition, authentication, and role of trademarks

Axis employees responsible for naming CA or End Entity certificates are prohibited from using names that infringe upon the Intellectual Property Rights of others. If such an issue is identified, contact support-pki@axis.com to report the infringement for investigation. In the case of a legitimate infringement, certificates shall be revoked and replaced with appropriately named certificates.

## 3.2 Initial identity validation

Applicants for certificates are Subscribers. The Subscriber always acts on behalf of the End Entity. A Certificate shall be issued to a Subscriber only when the Subscriber has submitted a Certificate Application in the form of a Certificate Signing Request (CSR) and is able to prove to the CA possession of the corresponding Private Key.

### 3.2.1 Method to prove possession of private key

Certificate Requests are only accepted as PKCS#10 Certificate Signing Requests. Signature verification of a PKCS#10 request constitute sufficient proof of possession of the corresponding Private Key.

If a Key Pair is generated by the manufacturer of the hardware key store, as part of a contracted provisioning service, this requirement shall not be applicable. Please refer to the CPS for Axis Device ID for further information on the provisioning service.

### 3.2.2 Authentication of organization identity

Only employees of Axis Communications or employees of manufacturing facilities under contract with Axis shall be authorized to submit a Certificate Application on behalf of Axis. No other organization name shall appear in a Certificate Application.

### 3.2.3 Authentication of individual identity

Individual Subscribers are Axis employees and employees of manufacturing facilities under contract with Axis. The employees have known and verified identities based on their employment status. Conditions of employment include identity verification by means of a government issued ID presented in person to HR upon commencement of employment.

Authentication for End Entity Certificate Applications to the CA shall be managed through employee permissions with individual subscribers being identified as administrators in their particular domain and authenticated as such when submitting an application.

In the case of registering a new Root CA or Intermediate CA, only employees with defined Trusted Roles (Section 5.2.1) within the HSM, performing tasks in an M of N manner, shall be able to submit a request.

### 3.2.4 Non-verified subscriber information

Not applicable

### 3.2.5 Validation of authority

Validation of authority shall be achieved through role-based permissions and the associated Axis employee credentials.

### 3.2.6 Criteria for interoperation

Not applicable.

## 3.3 Identification and authentication for re-key requests

Re-keying (sometimes called reissuing) refers to the creation of an entirely new certificate, using some or all of the information submitted for an existing certificate and containing a newly generated public key.

### 3.3.1 Identification and authentication for routine re-key

Not supported. The key validity periods are designed to outlive the product’s useful lifespan.

### 3.3.2 Identification and authentication for re-key after revocation

If an End Entity certificate is revoked, a new certificate with an updated key pair based on a PKCS#10 CSR shall be issued.  Identification and authentication shall be performed as described in Section 3.2.

### 3.3.3 Identification and authentication for revocation request

The identification and authentication procedures for a revocation request of End Entity Certificates shall be the same as for initial identity validation as described in Section 3.2.

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)

This section describes the administration of Axis Root CA and Axis Intermediate CA key pairs throughout their operational lifecycle. This includes how:

- the Public and Private keys are generated and / or regenerated (re-keying)
- the Private keys are stored, secured and destroyed
- the Public keys are distributed and archived.

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application?

#### *4.1.1.1 Root CA*

Select Axis employees, having management roles within their respective business areas, shall be assigned Trusted Roles within the HSM to be able to submit a Certificate Application to the Root CA for the purpose of issuing a new Intermediate CA. Applications to issue a new Intermediate CA shall always performed under dual control.

#### *4.1.1.2 Intermediate CA*

Axis employees, or employees of a manufacturing facility under contract to Axis, shall be provided Trusted Roles within the HSM to submit a Certificate Application only to the Intermediate CA designated for their business area.

### 4.1.2 Enrollment process and responsibilities

The enrollment process consists of the subscriber generating the key pair and the CSR within their hardware or software system. If the subscriber possesses the necessary authentication credentials and sufficient permissions, they may submit a Certificate Application to an Intermediate CA designated for their business area and subsequently receive the signed End Entity certificates for the commercial products they are responsible for.

It is the responsibility of the subscriber to ensure that the information included in the CSR is accurate and consistent with that defined in the Certificate Profile as outlined in Section 7 of the CPS that applies to their CA hierarchy.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

All subscribers shall be authenticated through the Axis Corporate IAM prior to submitting Certificate Applications to their respective Intermediate CA.

### 4.2.2 Approval or rejection of certificate applications

Certificate Applications shall be verified against a template of expected parameters to ensure the accuracy of the resulting certificates. Any deviation from this template shall result in the application being rejected.

### 4.2.3 Time to process certificate applications

No additional stipulation.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

If a PKCS#10 format CSR is made, the CA shall verify the digital signature prior to signing and subsequently issue the signed public key certificate.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

Depending on the system submitting the application and the needs of the subscriber they may be notified in the user interface to download the certificate, or the certificate may be automatically uploaded to the End Entity.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

#### *4.4.1.1 Root CA*

Acceptance of the certificate shall take place as part of, or as a result of, the CA Creation Key Ceremony

#### *4.4.1.2 Intermediate CA*

Download and subsequent usage of the issued certificate shall be deemed sufficient to indicate acceptance by the subscriber.

### 4.4.2 Publication of the certificate by the CA

The public key certificate of the Root CA and any other CA certificates in the certificate chain shall be published in a public repository, as described in Section 2, to support verification of the signature in the End Entity certificate.

### 4.4.3 Notification of certificate issuance by the CA to other entities

No other entities shall be notified of certificate issuance by the CA.

## 4.5 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

Subscribers shall only use End Entity private keys and certificates for the intended purposes specified in the certificate.

### 4.5.2 Relying party public key and certificate usage

Relying parties shall only use the public keys and published certificates for verification of the End Entity certificate including:

- Validation of the certificate signing chain
- Determining revocation status of the certificate (if available)

## 4.6 Certificate renewal

Certificate renewal involves issuing a new certificate with extended validity without changing the corresponding private and public key.

Certificate renewal shall not be supported within Axis' Product PKI infrastructure.

### 4.6.1 Circumstance for certificate renewal

Not applicable.

### 4.6.2 Who may request renewal

Not applicable.

### 4.6.3 Processing certificate renewal requests

Not applicable.

### 4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

### 4.6.6 Publication of the renewal certificate by the CA

Not applicable.

### 4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

## 4.7 Certificate re-key

Certificate re-keying is the process of creating a new certificate with a new key pair while retaining the contents and naming of the previous certificate. Changes to the certificate reflect the new public key, key identifiers, validity period and potentially CRL link.

After re-keying, the subscriber may or may not revoke the previous certificate but must not re-key, renew or modify it further. Certificate re-keying follows the same practices as in Section 4.3: Certificate Issuance. Previously validated information must not be re-validated.

### 4.7.1 Circumstance for certificate re-key

Re-keying may be performed:

- in response to the potential compromise of the private key leading to revocation of the public key certificate
- in response to revocation of an up-stream CA certificate thus invalidating the certificate signing chain.

### 4.7.2 Who may request certification of a new public key

No additional stipulation

### 4.7.3 Processing certificate re-keying requests

No additional stipulation

### 4.7.4 Notification of new certificate issuance to subscriber

No additional stipulation

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

No additional stipulation

### 4.7.6 Publication of the re-keyed certificate by the CA

No additional stipulation

### 4.7.7 Notification of certificate issuance by the CA to other entities

No additional stipulation

## 4.8 Certificate modification

Certificate modification involves modifying parameters of a valid certificate such as the subject name or domain name without changing the key.

Certificate modification is not supported in Axis’ Product PKI.

### 4.8.1 Circumstance for certificate modification

Not applicable.

### 4.8.2 Who may request certificate modification

Not applicable.

### 4.8.3 Processing certificate modification requests

Not applicable.

### 4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

### 4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

### 4.8.6 Publication of the modified certificate by the CA

Not applicable.

### 4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

## 4.9 Certificate revocation and suspension

### 4.9.1 Circumstances for revocation

Certificates may be revoked for the following circumstances:

- Evidence that the private key corresponding to the certificate has been or could be compromised
- Evidence that the private key is based on insecure or outdated cryptographic algorithms
- Revocation of upstream CA certificate due to potential compromise of the CA private key or planned changes to the CA hierarchy.

### 4.9.2 Who can request revocation

For End Entity certificates, a revocation may be requested and performed by the CA in response to changes in the CA hierarchy or requested by subscribers and/or relying parties in response to concerns around a particular private key's security.

### 4.9.3 Procedure for revocation request

Revocation requests are made by the subscriber directly to the CA or by a relying party by contacting Axis Technical Support. Revocation requests are investigated for the validity of the request and, if deemed necessary, revocation is carried out.

### 4.9.4 Revocation request grace period

Revocation requests shall be submitted by the requestor as soon as they believe there is cause to do so.

### 4.9.5 Time within which CA must process the revocation request

The CA shall process the revocation request and produce a report within 72 hours of the request being submitted.

### 4.9.6 Revocation checking requirement for relying parties

Relying parties may check the revocation status of their certificates by contacting Axis Technical Services and submitting a request ticket.

### 4.9.7 CRL issuance frequency (if applicable)

Not applicable. Axis does not currently maintain a CRL for public use.

### 4.9.8 Maximum latency for CRLs (if applicable)

Not applicable

### 4.9.9 On-line revocation/status checking availability

Not applicable

### 4.9.10 On-line revocation checking requirements

Not applicable

### 4.9.11 Other forms of revocation advertisements available

None

### 4.9.12 Special requirements re key compromise

If the Root CA has cause to believe the private key has been compromised, Axis will contact relying parties by way of established means outlined in Section 9.11.

### 4.9.13 Circumstances for suspension

Certificate suspension is not supported.

## 4.10 Certificate status services

No certificate status services are currently being offered.

### 4.10.1 Operational characteristics

Not applicable

### 4.10.2 Service availability

Not applicable

### 4.10.3 Optional features

Not applicable

## 4.11 End of subscription

Subscribers are internal employees and systems, not external parties so no subscription mechanisms are present.

## 4.12 Key escrow and recovery

Not applicable. Key escrow is not currently offered.

### 4.12.1 Key escrow and recovery policy and practices

Not applicable

### 4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)

The management and operation of Axis' Product PKI environment is in accordance with Axis' Information Security Management System ("ISMS"), which supports the requirements of this CP. Axis' ISMS is ISO27001 compliant. The ISO certificate can be found at the following link.

https://www.axis.com/dam/public/34/25/e9/axis-iso-27001-certificate-en-US+sv-SE-362978.pdf

## 5.1 Physical controls

Physical controls refer to the controls deployed to protect physical access to the HSM appliance(s) and the secrets stored within. These secrets may include private keys from Root and Intermediate CA's, symmetric keys, or any other secrets that require protected storage.

### 5.1.1 Site location and construction

All HSM appliances shall be housed in specialized server rooms designed for the secure storage of hardware servers and network appliances.

### 5.1.2 Physical access

Physical access shall be controlled via physical and logical access control systems with two factor authentication (badge and pin) to gain access. Authorization shall require "server room" access permissions provided to trusted employees by the responsible area owner. All server room access shall be supported by video surveillance to monitor physical access with video surveillance data stored for a minimum of 90 days.

### 5.1.3 Power and air conditioning

All server rooms shall have cooling systems suitable for the size of the room to provide optimal temperature and humidity for the operation of the devices. Back-up cooling systems shall also exist to ensure operation in the event of a system failure. A system to monitor temperature and humidity shall also be in place.

All server rooms shall be supplied with power from multiple circuits and backed up with an Uninterrupted Power Source (UPS) suitable for the power requirements of the room. A system to monitor the UPS hardware shall exist and the system shall be tested at least monthly with full maintenance performed at least yearly.

### 5.1.4 Water exposure

All HSM appliances shall be housed in server racks that are well clear of the ground to minimize the effect of potential water exposure due to leakage or seepage. Water-based fire suppression systems shall not be deployed in server rooms housing HSM appliances.

### 5.1.5 Fire prevention and protection

Fire suppression systems suitable for the size of the room shall be installed. The system shall be tested according to the manufacturer's instructions on a yearly basis. A system to monitor hardware problems in the fire suppression system shall also exist.

### 5.1.6 Media storage

All media containing sensitive or secret information shall be stored in secure locations within Axis or at secure off-site facilities in the case of back-ups. All locations shall be secured with physical and logical controls to limit access to only authorized individuals and to protect media from physical harm or destruction.

### 5.1.7 Waste disposal

All sensitive information shall be handled using the recommended de-commissioning procedures for the type of media in question and the level of secrecy.  All sensitive paper documents shall be shredded in accordance with DIN 66933.  Media used to collect or transmit sensitive information shall be rendered unreadable via physical destruction. Cryptographic devices shall be physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

### 5.1.8 Off-site backup

Off-site backups shall exist for all media storing Root CA or Intermediate CA private keys.  The backups shall be stored in secure locations subject to all physical and logical security requirements stated for the primary locations.

Off-site backup of audit logs and other sensitive information shall be performed as part of centralized handling of IT logs.

## 5.2 Procedural controls

### 5.2.1 Trusted roles

Trusted roles for Axis' Product PKI operations includes all individuals with access to administrative and operational tasks within the "backend" PKI infrastructure.  The backend infrastructure consists of physical HSM appliances as well as integrations to supporting systems.  The backend infrastructure is that which is capable of:

- Creation and secure storage of Root and Intermediate CA key pairs and enrollment of CA certificates.
- Validation of information in End Entity Certificate Applications
- Acceptance or rejection of End Entity Certificate Applications, Re-Key or Revocation requests.
- Issuance or Revocation of End Entity Certificates

Trusted roles for administrative tasks within the backend infrastructure shall include:

- Security Officers (SO)
- Partition Officers (PO)
- Auditors (AU)

Trusted roles for operational tasks within the backend infrastructure shall include:

- Cryptography Officers (CO)
- Cryptography Users (CU)

### 5.2.2 Number of persons required per task

Several tasks within the backend infrastructure require multiple persons working in an M of N formulation.  These required tasks shall include:

- Physical access to hardware HSM appliances
- Global configuration of the HSM appliances such as initial set-up, maintenance and licensing
- Creation, modification and deletion of Certificate Authority cryptographic objects within the HSM appliance

### 5.2.3 Identification and authentication for each role

Identification and authentication of administrative roles within the HSM shall be performed with the support of a Pin enabled device (PED) key and, in some cases, an additional password. Physical controls are implemented to protect against equipment, information, media and software being taken off-site without authorization.

### 5.2.4 Roles requiring separation of duties

Within the backend infrastructure separation of duties shall be applied between the administrative tasks that define the global parameters of the HSM and the operational tasks that create the cryptographic material and issue certificates.  As an example, based on the roles defined in Section 5.2.1, a “Security Officer” cannot be the same person as a “Cryptography Officer”.

## 5.3 Personnel controls

### 5.3.1 Qualifications, experience, and clearance requirements

Persons entering into Trusted Roles within the PKI environment must have the requisite background, credentials and experience to perform their respective job responsibilities competently.

### 5.3.2 Background check procedures

Background checks on candidates for employment shall be carried out in accordance with local laws and regulations.  The level of scrutiny shall be proportional to level of responsibility with respect to the classification of the data to be accessed and the business requirements surrounding the role.

Any personnel who fail a background check for any reason shall not be allowed to serve in any Trusted Role.

### 5.3.3 Training requirements

Training requirements for personnel in Trusted Roles within the PKI shall include:

- General Information Security Awareness Training
- Role-specific training regarding the specialized duties they are to perform and the required security protocols
- Software and hardware training on the infrastructure components of their environment
- Disaster recovery and business continuity procedures for their environment.

### 5.3.4 Retraining frequency and requirements

Re-training shall be performed as required based on changes to the underlying roles or infrastructure or to maintain a desired level of proficiency to perform the assigned tasks.

General information security awareness training shall be refreshed periodically as required by Axis' ISMS.

### 5.3.5 Job rotation frequency and sequence

No additional stipulation

### 5.3.6 Sanctions for unauthorized actions

Personnel performing unauthorized actions within the PKI environment shall be subject to sanctions up to and including termination of employment depending on the severity of the infraction.

### 5.3.7 Independent contractor requirements

No independent contractors shall be employed to fill Trusted roles within the Axis Product PKI environment.

If independent contractors or consultants are given access to backend infrastructure for the purpose of maintenance or other necessary tasks, they shall be escorted and supervised at all times by an authorized Axis employee in a Trusted Role.

### 5.3.8 Documentation supplied to personnel

All Axis employees shall be provided access to the "Information Security User Handbook" which outlines best practices for handling confidential and non-confidential data within Axis' IT systems.

Further documentation supporting Trusted Roles administering and using the Axis Product PKI infrastructure shall be provided by their Managers.

## 5.4 Audit logging procedures

Audit logging on the primary hardware components of the PKI is performed to track both administrative changes to the configuration of the systems as well as the cryptographic operations performed by the systems.

When possible, data shall be automatically collected in the HSM appliances and sent to a dedicated logging system for storage, management and processing of the logs. Where not possible, a digital logbook or other mechanism is deployed.

### 5.4.1 Types of events recorded

The CA shall record at least the following events:

1. CA certificate and key lifecycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction,
    - Certificate requests, renewal, and re-key requests, and revocation,
    - Approval and rejection of certificate requests,
    - Cryptographic device lifecycle management events,
    - Generation of Certificate Revocation Lists and OCSP entries (when applicable),
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. CA and Subscriber lifecycle management events, including:

- Certificate requests, renewals, re-key requests, and revocation,
- All verification activities stipulated in this document and the CA's Certification Practice Statement (CPS),
- Acceptance and rejection of certificate requests,
- Issuance of certificates,
- Generation of Certificate Revocation Lists and OCSP entries (when applicable).

3. Security events, including:

- Successful and unsuccessful system access attempts,
- PKI and security system actions performed,
- Security profile changes,
- System crashes, hardware failures, and other anomalies,
- Firewall and router activities,
- Entries to and exits from the server room housing the CA hardware components

### 5.4.2 Frequency of processing log

No additional stipulation.

### 5.4.3 Retention period for audit log

Performance and hardware maintenance audit logs shall be retained for a minimum of six months with operational audit logs (as described in Section 5.4.1) retained for a period of two years. All audit logs shall be made available to a Qualified Auditor upon request.

### 5.4.4 Protection of audit log

The digital audit logs shall be protected from modification and destruction and maintained in an encrypted format.

Access control to the digital audit logs shall be provided by Axis' role based IAM system.

Axis Communications shall decide whether to make the audit logs available to other parties and the circumstances under which the information is shared.

### 5.4.5 Audit log backup procedures

All audit logs shall be backed up every 30 hours by capturing a snapshot and storing it in a separate location.

### 5.4.6 Audit collection system (internal vs. external)

Audit logs shall be collected in external systems un-related to the operation of the PKI systems and the components generating the logs.

### 5.4.7 Notification to event-causing subject

Does not apply

### 5.4.8 Vulnerability assessments

Axis Communications shall perform yearly vulnerability assessments covering all systems and process related to the operation of the Axis Product PKI as stipulated in Axis' ISO27001 conformant ISMS.

Vulnerability assessments shall also be performed in response to:

- Changes in the physical infrastructure components of the CA
- Changes to processes that define how the CA operates

## 5.5 Records archival

### 5.5.1 Types of records archived

All administrative and operational audit logs and device events described above shall be archived.

### 5.5.2 Retention period for archive

Archives shall be retained for a period of 6 months (administrative) and 2 years (operational).

### 5.5.3 Protection of archive

Archives shall be exported into an external log management system, processed, and stored in protected filesystems accessible in a read-only format.

### 5.5.4 Archive backup procedures

Archives shall be back-ed up via snapshots taken daily and stored in a separate, secure location.

### 5.5.5 Requirements for time-stamping of records

All audit logs shall be time-stamped when created and the time-stamp shall be maintained during subsequent storage archiving and back-up procedures.

### 5.5.6 Archive collection system (internal or external)

The archive collection system shall be external to the operational systems of the Product PKI but operated and managed by Axis.

### 5.5.7 Procedures to obtain and verify archive information

Verification of archived back-ups are performed periodically as part of the Disaster Recovery portion of the Life Cycle Management plan.  Obtaining access to back-up files and other archived data is limited to employees filling Trusted Roles within the Product PKI as defined in Section 5.2.1.

## 5.6 Key changeover

Root CA private keys expire at the same time as their associated certificates.  Key changeover must occur before the expiration of the certificate and is performed manually using the same “Key Ceremony” performed to create the initial key pair.  The key validity and operational periods are as defined in the table below.

| Certificate Authority | Key Validity Period | Key Operational Period (Stop issuance date) |
|---|---|---|
| **Axis Device ID Root CA** | 15 years | 8 years |
| **Axis Edge Vault Root CA** | 15 years | 8 years |
| **Axis Operations Root CA** | 15 years | 8 years |

The “stop issuance date” defines the date that CA and EE certificates are no longer signed with the existing Root private key. The private key of a newly issued Root CA will take over signing responsibilities starting with issuing new subordinate CA certificates. The private key for the old Root CA will be destroyed at this time. The public key certificate for the old CA will remain to verify previously existing signatures until key validity date is reached.

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

When emergency incidents and compromises occur during operation of the CA, an Emergency Team is established in accordance with the ISMS. This Emergency Team gathers information, assesses the risks, develops a procedure, and proposes and implements that procedure with approval from Axis’ CIO.

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

Should computing resources, software or data become corrupted, existing back-ups of both the issuing CA’s and/or the Root CA’s, in the form of mirrored HSM appliances, can be utilized to continue operations while the primary HW is brought back online, the software is re-installed, or the data is recovered.

### 5.7.3 Entity private key compromise procedures

Should the private key of any CA entity become compromised, it will be destroyed and its corresponding public key certificate revoked. All downstream certificates will also be revoked and subsequently re-issued by the CA replacing the compromised entity.

### 5.7.4 Business continuity capabilities after a disaster

Business continuity (BC) and disaster recovery (DR) plans for the CA are included in the scope of Axis’ ISMS and organizational BC & DR plans. The PKI infrastructure issuing EE certificates carries a RTO of 48 hours and an RPO of 1 week.

## 5.8 CA or RA termination

Should a CA require termination for any reason, all relying parties will be informed using established communication means outlined in Section 9.11, and a termination plan followed to ensure minimal disruption to relying parties. The termination plan shall include provisions to:

- Publish notifications in advance of termination to all affected parties
- Revocation of certificates issued to Intermediate CA’s capable of issuing EE certificates
- Preservation of the CA’s archives and records for the time period defined in the CPS
- Customer support and Help Desk services during transition
- Continuation of revocation services for existing EE certificates
- Destruction of the Root CA’s private key
- Provisions to transition to a new CA if applicable

# 6 TECHNICAL SECURITY CONTROLS (11)

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

Details are described in the corresponding CPS

### 6.1.2 Private key delivery to subscriber

Details are described in the corresponding CPS

### 6.1.3 Public key delivery to certificate issuer

Details are described in the corresponding CPS

### 6.1.4 CA public key delivery to relying parties

Details are described in the corresponding CPS

### 6.1.5 Key sizes

Details are described in the corresponding CPS

### 6.1.6 Public key parameters generation and quality checking

Details are described in the corresponding CPS

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

Details are described in the corresponding CPS

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

Details are described in the corresponding CPS

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

Details are described in the corresponding CPS

### 6.2.3 Private key escrow

Details are described in the corresponding CPS

### 6.2.4 Private key backup

Details are described in the corresponding CPS

### 6.2.5 Private key archival

Details are described in the corresponding CPS

### 6.2.6 Private key transfer into or from a cryptographic module

Details are described in the corresponding CPS

### 6.2.7 Private key storage on cryptographic module

Details are described in the corresponding CPS

### 6.2.8 Method of activating private key

Details are described in the corresponding CPS

### 6.2.9 Method of deactivating private key

Details are described in the corresponding CPS

### 6.2.10 Method of destroying private key

Details are described in the corresponding CPS

### 6.2.11 Cryptographic Module Rating

Details are described in the corresponding CPS

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

Details are described in the corresponding CPS

### 6.3.2 Certificate operational periods and key pair usage periods

Details are described in the corresponding CPS

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

Details are described in the corresponding CPS

### 6.4.2 Activation data protection

Details are described in the corresponding CPS

### 6.4.3 Other aspects of activation data

Details are described in the corresponding CPS

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

Details are described in the corresponding CPS

### 6.5.2 Computer security rating

Details are described in the corresponding CPS

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

Details are described in the corresponding CPS

### 6.6.2 Security management controls

Details are described in the corresponding CPS

### 6.6.3 Life cycle security controls

Details are described in the corresponding CPS

## 6.7 Network security controls

Details are described in the corresponding CPS

## 6.8 Time-stamping

Details are described in the corresponding CPS

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profile

Certificate profiles are specified within the applicable CPS documents for the PKI environment in question.

### 7.1.1 Version number(s)

Details are described in the corresponding CPS

### 7.1.2 Certificate extensions

Details are described in the corresponding CPS

### 7.1.3 Algorithm object identifiers

Details are described in the corresponding CPS

### 7.1.4 Name forms

Details are described in the corresponding CPS

### 7.1.5 Name constraints

Details are described in the corresponding CPS

### 7.1.6 Certificate policy object identifier

Details are described in the corresponding CPS

### 7.1.7 Usage of Policy Constraints extension

Details are described in the corresponding CPS

### 7.1.8 Policy qualifiers syntax and semantics

Details are described in the corresponding CPS

### 7.1.9 Processing semantics for the critical Certificate Policies extension

Details are described in the corresponding CPS

## 7.2 CRL profile

### 7.2.1 Version number(s)

Details are described in the corresponding CPS

### 7.2.2 CRL and CRL entry extensions

Details are described in the corresponding CPS

## 7.3 OCSP profile

### 7.3.1 Version number(s)

Details are described in the corresponding CPS

### 7.3.2 OCSP extensions

Details are described in the corresponding CPS

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Axis operates the Product PKI to act as a Root of Trust when signing certificates installed in Axis products. As Axis does not sell CA services to external parties, nor enter into any contractual obligations with 3rd parties, there are currently no plans to pursue formal compliance. Axis is committed to following best practices and, as such, have designed the Product PKI to align with industry standards such as IEC/EN 319 411-1 and the CA/Browser forum recommendations.

Additionally, Axis performs internal audits on the underlying systems to ensure they function as expected and align with the security baselines defined in Axis' ISO27001-compliant ISMS. If there are any questions surrounding Axis' approach to compliance for the Product PKI, please send your inquiries to support-pki@axis.com.

## 8.1 Frequency or circumstances of assessment

Assessments of the Axis Product PKI in conformance with the information described in this Certificate Policy is carried out by internal auditors as part of Axis' ISO 27001 certification.

## 8.2 Identity/qualifications of assessor

The assessor is an internal IT auditor whose role is to assess compliance of Axis' systems with the requirements set forth in this CP as well as Axis' ISO 27001 Security Baseline.

## 8.3 Assessor's relationship to assessed entity

The assessor is an employee of Axis.

## 8.4 Topics covered by assessment

The topics covered follows the major themes of this Certificate Policy and the technical requirements outlined in the applicable CPS.

## 8.5 Actions taken as a result of deficiency

Deficiencies are recorded, assessed and acted upon based on prioritizations factoring in business risk, business impact and available resources.

## 8.6 Communication of results

Results are communicated internally

# 9 OTHER BUSINESS AND LEGAL MATTERS

This document is provided “as is” without warranty of any kind. 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 CP or any service or product will meet any expectations or that access to certificates will be timely or error-free.

## 9.1 Fees

Certificates within Axis’ external PKI environments are issued by Axis to other Axis systems for the purpose of providing relying parties with a method of verifying that the product or system does indeed originate from Axis. Therefore, no fees are charged and there are no contractual obligations attached to the operation of this PKI environment.

### 9.1.1 Certificate issuance or renewal fees

Not applicable

### 9.1.2 Certificate access fees

Not applicable

### 9.1.3 Revocation or status information access fees

Not applicable

### 9.1.4 Fees for other services

Not applicable

### 9.1.5 Refund policy

Not applicable

## 9.2 Financial responsibility

### 9.2.1 Insurance coverage

Not applicable

### 9.2.2 Other assets

Not applicable

### 9.2.3 Insurance or warranty coverage for end-entities

Not applicable

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

Not applicable

### 9.3.2 Information not within the scope of confidential information

Not applicable

### 9.3.3 Responsibility to protect confidential information

Not applicable

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

Not applicable

### 9.4.2 Information treated as private

Not applicable

### 9.4.3 Information not deemed private

Not applicable

### 9.4.4 Responsibility to protect private information

Not applicable

### 9.4.5 Notice and consent to use private information

Not applicable

### 9.4.6 Disclosure pursuant to judicial or administrative process

Not applicable

### 9.4.7 Other information disclosure circumstances

Not applicable

## 9.5 Intellectual property rights

Not applicable

## 9.6 Representations and warranties

### 9.6.1 CA representations and warranties

Not applicable

### 9.6.2 RA representations and warranties

Not applicable

### 9.6.3 Subscriber representations and warranties

Not applicable

### 9.6.4 Relying party representations and warranties

Not applicable

### 9.6.5 Representations and warranties of other participants

Not applicable

## 9.7 Disclaimers of warranties

Not applicable

## 9.8 Limitations of liability

Not applicable

## 9.9 Indemnities

Not applicable

## 9.10 Term and termination

### 9.10.1 Term

Not applicable

### 9.10.2 Termination

Not applicable

### 9.10.3 Effect of termination and survival

Not applicable

## 9.11 Individual notices and communications with participants

Communication with relying parties is managed through registration to the Axis Security Notification Service, https://www.axis.com/stay-secure and, in select cases, publishing of information directly on www.axis.com.

## 9.12 Amendments

### 9.12.1 Procedure for amendment

The CP is amended in response to planned changes / upgrades in the PKI environments or their underlying policies. These changes / upgrades can be performed on an ad hoc basis or via yearly reviews of the CP and corresponding CPS documents.

### 9.12.2 Notification mechanism and period

If the proposed changes affect the assurance procedures adopted by relying parties, then they shall be notified of changes to the CP by the means described in Section 9.11. The CP shall be updated prior to the proposed changes taking effect.

### 9.12.3 Circumstances under which OID must be changed

The OID must be changed if a new version of this CP is released which has enough material changes to the content to warrant a new versioning number of the document.

## 9.13 Dispute resolution provisions

Not applicable

## 9.14 Governing law

Not applicable

## 9.15 Compliance with applicable law

Not appliable

## 9.16 Miscellaneous provisions

### 9.16.1 Entire agreement

Not applicable

### 9.16.2 Assignment

Not applicable

### 9.16.3 Severability

Not applicable

### 9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable

### 9.16.5 Force Majeure

Not applicable

## 9.17 Other provisions

### 9.17.1 Order of Precedence of the CP

This CP is written with the intention that its contents outline the overarching business, legal and operational requirements for Certificate Authorities operating within the Axis Product PKI environment.

Individual CPS documents are provided for each Certificate Authority trust chain under the scope of this CP to augment the requirements and practices found here with more specific information related to the Certificate use case.  If there are any disputes between the contents of a CPS and the over-arching CP document, the CP takes precedence.