IoT Electrolux Certification Authority

Root CA Certificate Policy and Certification Practice Statement

Version 1.0

Table of Content

1 INTRODUCTION 7

1.1 OVERVIEW 7
1.2 DOCUMENT NAME AND IDENTIFICATION 7
1.2.1 Policy Name 7
1.2.2 Object Identifiers 7
1.3 PKI PARTICIPANTS 7
1.3.1 Certification authorities 7
1.3.2 Registration authorities 7
1.3.3 Subscribers 7
1.3.4 Relying parties 8
1.3.5 Other participants 8
1.4 CERTIFICATE USAGE 8
1.4.1 Appropriate certificate uses 8
1.4.2 Prohibited certificate uses 8
1.5 POLICY ADMINISTRATION 8
1.5.1 Organization administering the document 8
1.5.2 Contact person 8
1.5.3 Person determining CPS suitability for the policy 8
1.5.4 CPS approval procedures 8
1.6 DEFINITIONS AND ACRONYMS 8

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 10

2.1 REPOSITORIES 10
2.2 PUBLICATION OF CERTIFICATION INFORMATION 10
2.3 TIME OR FREQUENCY OF PUBLICATION 10
2.4 ACCESS CONTROLS ON REPOSITORIES 10

3 IDENTIFICATION AND AUTHENTICATION 11

3.1 NAMING 11
3.1.1 Types of names 11
3.1.2 Need for names to be meaningful 11
3.1.3 Anonymity or pseudonymity of subscribers 11
3.1.4 Rules for interpreting various name forms 11
3.1.5 Uniqueness of names 11
3.1.6 Recognition, authentication, and role of trademarks 11
3.2 INITIAL IDENTITY VALIDATION 11
3.2.1 Method to prove possession of private key 11
3.2.2 Authentication of organization identity 11
3.2.3 Authentication of individual identity 11
3.2.4 Non-verified subscriber information 12
3.2.5 Validation of authority 12
3.2.6 Criteria for interoperation 12
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 12
3.3.1 Identification and authentication for routine re-key 12
3.3.2 Identification and authentication for re-key after revocation 12
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 12

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 13

4.1 CERTIFICATE APPLICATION 13
4.1.1 Who can submit a certificate application 13
4.1.2 Enrollment process and responsibilities 13
4.2 CERTIFICATE APPLICATION PROCESSING 13
4.2.1 Performing identification and authentication functions 13
4.2.2 Approval or rejection of certificate applications 13

4.3 CERTIFICATE ISSUANCE 13
4.3.1 CA actions during certificate issuance 13
4.3.2 Notification to subscriber by the CA of issuance of certificate 13
4.4 CERTIFICATE ACCEPTANCE 13
4.4.1 Conduct constituting certificate acceptance 13
4.4.2 Publication of the certificate by the CA 13
4.4.3 Notification of certificate issuance by the CA to other entities 13
4.5 KEY PAIR AND CERTIFICATE USAGE 13
4.5.1 Subscriber private key and certificate usage 13
4.5.2 Relying party public key and certificate usage 13
4.6 CERTIFICATE RENEWAL 14
4.6.1 Circumstance for certificate renewal 14
4.6.2 Who may request renewal 14
4.6.3 Processing certificate renewal requests 14
4.6.4 Notification of new certificate issuance to subscriber 14
4.6.5 Conduct constituting acceptance of a renewal certificate 14
4.6.6 Publication of the renewal certificate by the CA 14
4.6.7 Notification of certificate issuance by the CA to other entities 14
4.7 CERTIFICATE RE-KEY 14
4.7.1 Circumstance for certificate re-key 14
4.7.2 Who may request certification of a new public key 14
4.7.3 Processing certificate re-keying requests 14
4.7.4 Notification of new certificate issuance to subscriber 14
4.7.5 Conduct constituting acceptance of a re-keyed certificate 14
4.7.6 Publication of the re-keyed certificate by the CA 14
4.7.7 Notification of certificate issuance by the CA to other entities 14
4.8 CERTIFICATE MODIFICATION 14
4.8.1 Circumstance for certificate modification 14
4.8.2 Who may request certificate modification 15
4.8.3 Processing certificate modification requests 15
4.8.4 Notification of new certificate issuance to subscriber 15
4.8.5 Conduct constituting acceptance of modified certificate 15
4.8.6 Publication of the modified certificate by the CA 15
4.8.7 Notification of certificate issuance by the CA to other entities 15
4.9 CERTIFICATE REVOCATION AND SUSPENSION 15
4.9.1 Circumstances for revocation 15
4.9.2 Who can request revocation 15
4.9.3 Procedure for revocation request 15
4.9.4 Revocation request grace period 16
4.9.5 Time within which CA must process the revocation request 16
4.9.6 Revocation checking requirement for relying parties 16
4.9.7 CRL issuance frequency (if applicable) 16
4.9.8 Maximum latency for CRLs (if applicable) 16
4.9.9 On-line revocation/status checking availability 16
4.9.10 On-line revocation checking requirements 16
4.9.11 Other forms of revocation advertisements available 16
4.9.12 Special requirements re-key compromise 16
4.9.13 Circumstances for suspension 16
4.9.14 Who can request suspension 16
4.9.15 Procedure for suspension request 16
4.9.16 Limits on suspension period 16
4.10 CERTIFICATE STATUS SERVICES 16
4.10.1 Operational characteristics 16
4.10.2 Service availability 16
4.10.3 Optional features 16
4.11 END OF SUBSCRIPTION 16
4.12 KEY ESCROW AND RECOVERY 17

4.12.1 Key escrow and recovery policy and practices 17
4.12.2 Session key encapsulation and recovery policy and practices 17

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 18

5.1 PHYSICAL CONTROLS 18
5.1.1 Site location and construction 18
5.1.2 Physical access 18
5.1.3 Power and air conditioning 18
5.1.4 Water exposures 18
5.1.5 Fire prevention and protection 18
5.1.6 Media storage 18
5.1.7 Waste disposal 18
5.1.8 Off-site backup 18
5.2 PROCEDURAL CONTROLS 18
5.2.1 Trusted Roles 18
5.2.2 Number of persons required per task 19
5.2.3 Identification and authentication for each role 19
5.2.4 Roles requiring separation of duties 19
5.3 PERSONNEL CONTROLS 19
5.3.1 Qualifications, experience, and clearance requirements 19
5.3.2 Background check procedures 19
5.3.3 Training requirements 19
5.3.4 Retraining frequency and requirements 20
5.3.5 Job rotation frequency and sequence 20
5.3.6 Sanctions for unauthorized actions 20
5.3.7 Independent contractor requirements 20
5.3.8 Documentation supplied to personnel 20
5.4 AUDIT LOGGING PROCEDURES 20
5.4.1 Types of events recorded 20
5.4.2 Frequency of processing log 21
5.4.3 Retention period for audit log 21
5.4.4 Protection of audit log 21
5.4.5 Audit log backup procedures 21
5.4.6 Audit collection system (internal vs. external) 21
5.4.7 Notification to event-causing subject 21
5.4.8 Vulnerability assessments 21
5.5 RECORDS ARCHIVAL 21
5.5.1 Types of records archived 21
5.5.2 Retention period for archive 21
5.5.3 Protection of archive 21
5.5.4 Archive backup procedures 21
5.5.5 Requirements for time-stamping of records 21
5.5.6 Archive collection system (internal or external) 21
5.5.7 Procedures to obtain and verify archive information 22
5.6 KEY CHANGEOVER 22
5.7 COMPROMISE AND DISASTER RECOVERY 22
5.7.1 Incident and compromise handling procedures 22
5.7.2 Computing resources, software, and/or data are corrupted 22
5.7.3 Entity private key compromise procedures 22
5.7.4 Business continuity capabilities after a disaster 22
5.8 CA OR RA TERMINATION 22

6 TECHNICAL SECURITY CONTROLS 24

6.1 KEY PAIR GENERATION AND INSTALLATION 24
6.1.1 Key pair generation 24
6.1.2 Private key delivery to subscriber 24
6.1.3 Public key delivery to certificate issuer 24

6.1.4 CA public key delivery to relying parties 24
6.1.5 Key sizes 24
6.1.6 Public key parameters generation and quality checking 24
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 24
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 24
6.2.1 Cryptographic module standards and controls 24
6.2.2 Private key (n out of m) multi-person control 24
6.2.3 Private key escrow 24
6.2.4 Private key backup 24
6.2.5 Private key archival 24
6.2.6 Private key transfer into or from a cryptographic module 24
6.2.7 Private key storage on cryptographic module 24
6.2.8 Method of activating private key 25
6.2.9 Method of deactivating private key 25
6.2.10 Method of destroying private key 25
6.2.11 Cryptographic module rating 25
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 25
6.3.1 Public key archival 25
6.3.2 Certificate operational periods and key pair usage periods 25
6.4 ACTIVATION DATA 25
6.4.1 Activation data generation and installation 25
6.4.2 Activation data protection 25
6.4.3 Other aspects of activation data 25
6.5 COMPUTER SECURITY CONTROLS 25
6.5.1 Specific computer security technical requirements 25
6.5.2 Computer security rating 25
6.6 LIFE CYCLE TECHNICAL CONTROLS 25
6.6.1 System development controls 25
6.6.2 Security management controls 26
6.6.3 Life cycle security controls 26
6.7 NETWORK SECURITY CONTROLS 26
6.8 TIMESTAMPING 26

7 CERTIFICATE, CRL, AND OCSP PROFILES 27

7.1 CERTIFICATE PROFILE 27
7.1.1 Version number(s) 27
7.1.2 Certificate extensions 27
7.1.3 Algorithm object identifiers 27
7.1.4 Name forms 27
7.1.5 Name constraints 28
7.1.6 Certificate policy object identifier 28
7.1.7 Usage of Policy Constraints extension 28
7.1.8 Policy qualifiers syntax and semantics 28
7.1.9 Processing semantics for the critical Certificate Policies extension 28
7.2 CRL PROFILE 28
7.2.1 Version number(s) 29
7.2.2 CRL and CRL entry extensions 29
7.3 OCSP PROFILE 29
7.3.1 Version number(s) 29
7.3.2 OCSP extensions 29

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 30

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 30
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 30
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 30
8.4 TOPICS COVERED BY ASSESSMENT 30
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 30

8.6 COMMUNICATION OF RESULTS 30

9 OTHER BUSINESS AND LEGAL MATTERS 31

9.1 FEES 31
9.1.1 Certificate issuance or renewal fees 31
9.1.2 Certificate access fees 31
9.1.3 Revocation or status information access fees 31
9.1.4 Fees for other services 31
9.1.5 Refund policy 31
9.2 FINANCIAL RESPONSIBILITY 31
9.2.1 Insurance coverage 31
9.2.2 Other assets 31
9.2.3 Insurance or warranty coverage for end-entities 31
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 31
9.3.1 Scope of confidential information 31
9.3.2 Information not within the scope of confidential information 31
9.3.3 Responsibility to protect confidential information 31
9.4 PRIVACY OF PERSONAL INFORMATION 31
9.4.1 Privacy plan 31
9.4.2 Information treated as private 32
9.4.3 Information not deemed private 32
9.4.4 Responsibility to protect private information 32
9.4.5 Notice and consent to use private information 32
9.4.6 Disclosure pursuant to judicial or administrative process 32
9.4.7 Other information disclosure circumstances 32
9.5 INTELLECTUAL PROPERTY RIGHTS 32
9.6 REPRESENTATIONS AND WARRANTIES 32
9.6.1 CA representations and warranties 32
9.6.2 RA representations and warranties 32
9.6.3 Subscriber representations and warranties 32
9.6.4 Relying party representations and warranties 32
9.6.5 Representations and warranties of other participants 33
9.7 DISCLAIMERS OF WARRANTIES 33
9.8 LIMITATIONS OF LIABILITY 33
9.9 INDEMNITIES 33
9.10 TERM AND TERMINATION 33
9.10.1 Term 33
9.10.2 Termination 33
9.10.3 Effect of termination and survival 33
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 33
9.12 AMENDMENTS 33
9.12.1 Procedure for amendment 33
9.12.2 Notification mechanism and period 33
9.12.3 Circumstances under which OID must be changed 33
9.13 DISPUTE RESOLUTION PROCEDURES 33
9.14 GOVERNING LAW 33
9.15 COMPLIANCE WITH APPLICABLE LAW 33
9.16 MISCELLANEOUS PROVISIONS 34
9.16.1 Entire agreement 34
9.16.2 Assignment 34
9.16.3 Severability 34
9.16.4 Enforcement (attorneys' fees and waiver of rights) 34
9.16.5 Force Majeure 34
9.17 OTHER PROVISIONS 34

BIBLIOGRAPHY 35

1 Introduction

1.1 Overview

This document is the Certificate Policy and Certification Practice statement followed by the Root CA when issuing and managing public key certificates.

This document is formatted according to RFC 3647 [RFC3647]. There are some sections that are maintained for compatibility although they do not apply exactly to the services required by this Certificate Policy. These sections contain the text “No stipulation”.

Within this document the words ‘MUST’, ‘MUST NOT’, ‘REQUIRED’, ‘SHALL’, ‘SHALL NOT’, ‘SHOULD’, ‘SHOULD NOT’, ‘RECOMMENDED’, ‘MAY’, ‘OPTIONAL’ are to be interpreted as in RFC 2119 [RFC2119].

1.2 Document name and identification

1.2.1 Policy Name

This document is Root CA Certificate Policy and Certification Practice Statement version 1.0.

1.2.2 Object Identifiers

This document is uniquely identified by the following identifier: 1.3.6.1.4.1.38884.3.1.1.1.0.

ISO assigned	1
ISO Identified organization	3
US Department of Defense	6
Internet	1
Internet Private	4
IANA registered private enterprises	1
Electrolux	38884
PKI	3
Electrolux Connected Appliances CP/CPS	1
Electrolux Connected Appliances High Assurance	1
Major Version	1
Minor Version	0

1.3 PKI participants

1.3.1 Certification authorities

The Root CA is an offline Certification Authority issuing certificates to Certificate Authorities operated by Electrolux AB.

1.3.2 Registration authorities

The Root CA SHALL be operated directly by the CA administrators. No Registration Authorities SHALL be deployed.

1.3.3 Subscribers

The Root CA SHALL issue certificates only to other Certificate Authorities operated by Electrolux AB.

1.3.4 Relying parties

This CP/CPS does not limit the community of relying parties.

1.3.5 Other participants

No stipulations.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by the Root CA MUST be used in compliance with this CP/CPS.

1.4.2 Prohibited certificate uses

Certificates issued by the Root CA MUST NOT be used for securing financial transactions.

1.5 Policy administration

1.5.1 Organization administering the document

This CP/CPS is administered by the Electrolux AB.
Electrolux AB
Göransgatan 143
SE 105 45 Stockholm
Sweden

1.5.2 Contact person

Policy Administrator is appointed by Electrolux AB. Contact details are published at the Electrolux PKI repository (see Section 2.1).

1.5.3 Person determining CPS suitability for the policy

CPS suitability for the CP is determined by the Policy Administrator (see Section 1.5.2).

1.5.4 CPS approval procedures

Proposed changes to this CP/CPS MUST be delivered to the Policy Administrator. The Policy Administrator informs the requester about the review results within one month.

1.6 Definitions and acronyms

Certificate subject

The entity (person, organization, or server) whose public key is certified in the certificate.

Certification Authority (CA)

An authority trusted by one or more users to create and assign public key certificates.

CA-certificate

A certificate for one CA's public key issued by another CA.

Certificate policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certification path

An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS)

A statement of the practices which a certification authority employs in issuing certificates.

Certificate revocation list (CRL)

A time stamped list identifying revoked certificates which is signed by a CA.

Issuing certification authority

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Public Key Certificate

A data structure containing the public key of an end-entity and some other information, which is digitally signed with the private key of the CA which issued it.

Registration authority (RA)

An entity that is responsible for identification and authentication of certificate subjects and for accepting revocation requests, but that does not sign or issue certificates (i. e., an RA is delegated certain tasks on behalf of a CA).

Relying party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms 'certificate user' and 'relying party' are used interchangeably.

Subject certification authority

In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate

Subscriber

In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject. For certificates issued to other CAs, the entity operating the respective CA.

2 Publication and repository responsibilities

2.1 Repositories

The Root CA SHALL publish its certificates, Certificate Revocation Lists (CRLs), and relevant public documentation in the Electrolux PKI Repository. The repository SHALL be accessible at http://ioteca.electrolux.com.

2.2 Publication of certification information

The Root CA SHALL make publicly available, in the Electrolux AB repositories:

1. the current version of this CP/CPS,
2. all previous versions of the CP, CPS, and CP/CPS that were in effect for issuing certificates,
3. the current version of CRL.

2.3 Time or frequency of publication

All documents SHALL be published in the Electrolux PKI Repository after their approval by the Policy Administrator. CRLs SHALL be published in regular intervals
not longer then 365 days.

2.4 Access controls on repositories

Information listed in Section 2.2 SHALL be publicly available.

The information published in the repository SHALL be protected against any unauthorized modification.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The Root CA assigns each entity a non-empty X.501 Distinguished Name (DN) which serves as a unique identifier of the entity. The DN is inserted in the subject field of the certificate(s) issued to the entity.

Both Issuer and Subject in the RootCA are filled with following attributes:

Attribute	Meaning	Value
CN	CommonName – distinguished name of certification authority	Root CA
OU	Organization Unit	Connected Appliances
O	Organization	Electrolux

3.1.2 Need for names to be meaningful

The names contained in a certificate MUST be meaningful in the sense that the Root CA has proper evidence of the existent association between these names and the subscriber.

3.1.3 Anonymity or pseudonymity of subscribers

Usage of anonymous and pseudonymous names in DN is not permitted. Issuance of anonymous certificates is not permitted.

3.1.4 Rules for interpreting various name forms

Names in certificates SHOULD be interpreted according to RFC 5280 [RFC5280].

3.1.5 Uniqueness of names

Every Subject DN SHALL be associated with exactly one entity.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The requester MUST prove possession of the private key which corresponds to the public key in the certificate request. The possession SHAL be proved by submitting a digitally signed PKCS#10 request or by providing another cryptographically equivalent demonstration.

3.2.2 Authentication of organization identity

The Root CA SHALL issue certificates only to CAs operated by Electrolux AB.

3.2.3 Authentication of individual identity

Subject CAs certified by the Root CA are operated by members of the Electrolux

AB team. These operators are personally known or identical to the operators of the Root CA.

3.2.4 Non-verified subscriber information

None. All information elements in certificates issued by Root CA MUST be validated.

3.2.5 Validation of authority

See Section 3.2.3.

3.2.6 Criteria for interoperation

No stipulations.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Identification and authentication for routine re-key SHALL be accomplished using the same procedures as for initial registration.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication for re-key after revocation SHALL be accomplished using the same procedures as for initial registration.

3.4 Identification and authentication for revocation request

A request for revocation of a certificate issued by the Root CA SHALL be made by a member of the Electrolux AB team or any entity who can prove possession of the private key corresponding to the certificate.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certificate application MUST be submitted by a member of the Electrolux AB team.

4.1.2 Enrollment process and responsibilities

No stipulations.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

A certificate application SHALL be delivered personally by the requester to the Root CA Security Officer using a secure off-line media.

4.2.2 Approval or rejection of certificate applications

Root CA Security Officer SHALL accept a certificate application only when the following conditions are met:

1. The application has been delivered by a member of the Electrolux AB team.
2. The public key in the application has been verified not to be a known weak key.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

No stipulations.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Root CA SHALL convey the issued certificate personally to the Subject CA Security Officer.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulations.

4.4.2 Publication of the certificate by the CA

The Root CA SHALL publish the issued certificates on request of the Subject CA Security Officer.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulations.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Subject CA private key and certificate usage SHALL be specified by the respective CA CP.

4.5.2 Relying party public key and certificate usage

The usage of the Subject CA public key and certificate by relying parties SHALL be specified by the respective CA CP.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

The Root CA does not support certificate renewal.

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

4.7.1 Circumstance for certificate re-key

The Root CA SHALL re-key a Subject CA certificate on request made by a Security Officer of the respective Subject CA.

4.7.2 Who may request certification of a new public key

Only a Security Officer of a Subject CA may request a re-keying of the respective CA certificate.

4.7.3 Processing certificate re-keying requests

A re-keying request SHALL be processed using the same procedures as for initial certificate issuance.

4.7.4 Notification of new certificate issuance to subscriber

The Root CA SHALL convey the issued certificate personally to the Subject CA Security Officer.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulations.

4.7.6 Publication of the re-keyed certificate by the CA

The Root CA SHALL publish the issued certificate on request of the respective Subject CA Security Officer.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulations.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

The Root CA SHALL modify a Subject CA certificate on request made by a Security Officer of the respective CA.

4.8.2 Who may request certificate modification

Only a Security Officer of a Subject CA may request modification of the respective CA certificate.

4.8.3 Processing certificate modification requests

A modification request SHALL be processed using the same procedures as for initial certificate issuance.

4.8.4 Notification of new certificate issuance to subscriber

The Root CA SHALL convey the issued certificate personally to the Subject CA Security Officer.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulations.

4.8.6 Publication of the modified certificate by the CA

The Root CA SHALL publish the issued certificate on request of the respective Subject CA Security Officer.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulations.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate SHALL be revoked when any of the following circumstances occurs:

- the private key corresponding to the certificate is compromised or suspected to be compromised or lost;
- the respective Subject CA has ceased its operations;
- the certificate has not been issued in accordance with this CP/CPS;
- a Security Officer of the respective Subject CA requests the revocation;

4.9.2 Who can request revocation

Any entity who can prove an occurrence of any of the circumstances for revocation as listed in Section 4.9.1 MUST request revocation of the pertinent certificate.

A Security Officer of a Subject CA MAY request revocation of the respective CA's certificate.

4.9.3 Procedure for revocation request

The party requesting a certificate revocation SHALL submit the revocation request to the Root CA.

On reception of a certificate revocation request, the Root CA SHALL:

1. verify the circumstances for revocation
2. verify the identity of the revocation requester in accordance with Section 4.9.2.

If all conditions for revocation are met, the Root CA SHALL revoke the certificate.

4.9.4 Revocation request grace period

Any party that becomes aware of circumstances for revocation SHALL request a revocation as soon as possible but not later than within one business day.

4.9.5 Time within which CA must process the revocation request

The Root CA SHALL act on a revocation request immediately after its reception.

4.9.6 Revocation checking requirement for relying parties

Relying parties MUST check the revocation status of a certificate on which they are relying.

4.9.7 CRL issuance frequency (if applicable)

The Root CA SHALL issue a CRL immediately after a certificate revocation or at least every 13 months.

4.9.8 Maximum latency for CRLs (if applicable)

The Root CA SHALL publish a new CRL immediately after its issuance.

4.9.9 On-line revocation/status checking availability

No stipulations.

4.9.10 On-line revocation checking requirements

No stipulations.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements re-key compromise

No stipulations.

4.9.13 Circumstances for suspension

The Root CA SHALL NOT support certificate suspension.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The Root CA SHALL issue direct, full and complete CRLs, i. e. every CRL contains serial numbers of all non-expired revoked certificates issued by the Root CA.

4.10.2 Service availability

The current CRL SHALL be available for download continuously.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

A Subject CA Security Officer MAY request end of the CA subscription at his/her

own discretion.

On receiving a subscription end request, the Root CA SHALL revoke all valid certificates issued to the subscriber and cease providing services to the subscriber.

4.12 Key escrow and recovery

The Root CA SHALL NOT provide key escrow service.

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

5.1 Physical Controls

5.1.1 Site location and construction

Systems of the Root CA SHALL be located and operated at a dedicated closed, secure and safe location.

5.1.2 Physical access

The software of the Root CA SHALL be stored on an off-line, secure, bootable removable media.

Physical access to systems of the Root CA SHALL be monitored and restricted to authorized personnel only.

5.1.3 Power and air conditioning

No stipulations.

5.1.4 Water exposures

Systems of the Root CA SHALL be located and operated at a location outside of a flood zone.

5.1.5 Fire prevention and protection

Fire prevention and protection of the Root CA site is covered by the Electrolux AB fire prevention policy.

5.1.6 Media storage

The media with the Root CA software SHALL be stored in a safe deposit box in Electrolux AB premises. Access to the safe deposit box is continually monitored. Access codes required to open the safe deposit box are known only to the Root CA Security Officers.

5.1.7 Waste disposal

The Root CA SHALL dispose its waste using procedures preventing using the waste to access any operational information, namely:

- all paper waste SHALL be shredded,
- all magnetic, optical or flash media SHALL be physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

Backup of critical part of the Root CA systems SHALL be stored in a secure place off-site.

5.2 Procedural controls

5.2.1 Trusted Roles

Root CA shall distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of CA operations. Senior management of the Issuer CA shall be responsible for appointing individuals to trusted roles. A list of such personnel shall be maintained and reviewed annually.

Responsibilities at the Root CA be divided among different trusted roles:

5.2.1.1 Security Officer

The Security Officer is responsible for ensuring physical access to the external media storage devices on which the image of virtual machine with Root CA is stored.
The request for an access to this media can come from CA Administrator or from Auditor.

The Security Officers also ensures that security policies are followed.

5.2.1.2 CA Administrator

The CA Administrator is responsible for installing and configuring CA system hardware, operating system (including installation of software patches and other maintenance needed for system stability and recoverability), installation and configuration of the CA software, including key generation, management of the CA accounts, audit parameters, key backup, and key management. The CA Administrator is responsible for performing and securely storing regular system backups of the CA system. Root CA backup SHALL be performed by CA Administrator every time when any change to the Root CA occurs (e.g. new CRL is issued, new SubCA certificate is signed etc.). CA Administrator may not issue certificates to end users.

All operations with a certification authority especially those involving operation with the private key SHALL be performed under the direct and physical supervision of at least one Security Officer.

5.2.1.3 Auditor

The Auditor is responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if the Root CA is operating in accordance with this CP. Security Officer and CA Administrator will provide access to the Root CA's logs on request of Auditor.

5.2.2 Number of persons required per task

Booting the Root CA system and activation of the Root CA signing key SHALL require supervison of at least one Security Officer.

5.2.3 Identification and authentication for each role

CA Administrator SHALL be authenticated with a user name and password.
Security Officer SHALL be authenticated with a personal PIN.

5.2.4 Roles requiring separation of duties

No stipulations.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The personnel of the Root CA SHALL be technically and professionally competent.

5.3.2 Background check procedures

No stipulations.

5.3.3 Training requirements

The Root CA personnel SHALL be trained in:

- basic PKI concepts,
- the use and operation of the Root CA software,
- the relevant documentation including the CP/CPS,
- computer security.

5.3.4 Retraining frequency and requirements

Training SHALL be provided to the personnel at least annually.

Training in the use and operation of the Root CA software SHALL be provided whenever the software is updated or changed.

Any change in CP/CPS SHALL be communicated to the Root CA personnel as soon as possible.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

Root CA or RA employees failing to comply with this CP, whether through negligence or malicious intent, shall be subject to administrative or disciplinary actions, including termination of employment or criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management reviews and discusses the incident with the trusted personnel, management may reassign the employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

The Root CA personnel SHAL be supplied with documentation required for their operation including but not limited to:

- the relevant CP/CPS
- documentation of the Root CA software.

5.4 Audit Logging Procedures

5.4.1 Types of events recorded

The Root CA SHALL record the following events:

- access to the Root CA safe deposit box,
- registration of a subscriber,
- certificate applications,
- certificate issuance,
- certificate revocation requests,
- certificate revocation,
- CRL issuance,
- initiation of the CA systems.

5.4.2 Frequency of processing log

Logs SHALL be processed monthly or immediately after discovering a security incident.

5.4.3 Retention period for audit log

Logs SHALL be retained for at least five years.

5.4.4 Protection of audit log

Access to logs SHALL be restricted to authorized personnel only. Logs SHOULD be protected against lost and modification.

5.4.5 Audit log backup procedures

Audit logs are SHALL be backed up with other CA data.

5.4.6 Audit collection system (internal vs. external)

The audit collection system is internal to the Electrolux AB.

5.4.7 Notification to event-causing subject

The subjects causing an audit event are generally not notified.

5.4.8 Vulnerability assessments

Audit logs SHALL be regularly monitored to find potential security incidents and non-standard events.

5.5 Records archival

5.5.1 Types of records archived

The Root CA SHALL archive:

- the Root CA software,
- the CA certificate,
- issued certificates,
- issued CRLs,
- audit logs,
- all implemented CPs and CPSs,
- operational documentation.

5.5.2 Retention period for archive

The Root CA SHALL archive items listed in Section 5.5.1 for at least five years.

5.5.3 Protection of archive

Archived information SHALL be accessible to authorized personnel only.

5.5.4 Archive backup procedures

Archive records SHALL be regularly moved to an archive media. The media SHALL be stored in a secure place.

5.5.5 Requirements for time-stamping of records

No stipulations.

5.5.6 Archive collection system (internal or external)

The Root CA SHALL collect archive information internally.

5.5.7 Procedures to obtain and verify archive information

Access to archive SHALL be recorded.

5.6 Key changeover

The following steps SHOULD be taken when re-keying the signing key of the Root CA:

1. A new certificate with the new key for the CA SHALL be issued.
2. The new certificate SHALL be published in accordance with Section 2.2.
3. The new certificate is used for issuing certificates. Both the new and the old certificate may be active at the same time. The old key SHALL be used as long as all certificates signed by it have not expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In case of an incident that might lead to compromising integrity of a CA system, the CA personnel SHALL initiate the incident analysis immediately. Further steps depend on the outcome of the analysis.

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

In case of hardware corruption, the system SHALL be recovered from backup to a new hardware and brought into operation.

In case of software or data corruption, the system SHALL be recovered from backup and brought into operation.

5.7.3 Entity private key compromise procedures

When the signing key of the Root CA is compromised, the CA SHALL:

1. immediately revoke the corresponding certificate,
2. stop accepting certificate applications,
3. inform users about the incident,
4. eliminate the circumstances that lead to the compromise,
5. generate a new key pair,
6. request a new certificate for the CA,
7. restart the CA operations with the new certificate.

5.7.4 Business continuity capabilities after a disaster

After a disaster, the Root CA SHALL recover its systems from backup and restart operations. The outage SHOULD NOT take longer than 30 business days.

5.8 CA or RA Termination

The Root CA SHALL announce its intent to terminate its operation at least 12 months in advance.

Before terminating its operations Root CA SHALL:

- revoke all issued certificates,
- request its certificate revocation
- destroy the private keys in possession of the CA,

- archive all relevant information in accordance with Section 5.5.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The Root CA SHALL generate its private keys in an off-line software security module by the Root CA *Security Officers*.

6.1.2 Private key delivery to subscriber

The Root CA SHALL NOT generate private keys for subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers SHALL deliver their public keys in a form of PKCS#10.

6.1.4 CA public key delivery to relying parties

The Root CA SHALL publish its certificates in its repository (see Section 2.2).

6.1.5 Key sizes

An RSA signing key of the Root CA SHALL be at least 4096 bits long.

6.1.6 Public key parameters generation and quality checking

The Root CA SHOULD refuse to certify public keys not matching its quality requirements.

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

6.2 Private key protection and cryptographic module engineering controls

Certificates and private keys MUST be used only in accordance with this policy and for the purpose specified in the KeyUsageextension.

6.2.1 Cryptographic module standards and controls

No stipulations.

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

Every usage of the Root CA signing key SHALL recorded in the key usage log book. These records SHALL contain the date, time and purpose of the key usage and signatures of at least two Security Officers presented at the operation requiring the use of the private key.

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

The backup copy of the Root CA private key SHALL be stored in a safe deposit box in an off-site location.

6.2.5 Private key archival

The Root CA SHALL NOT archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

Not applicable.

6.2.8 Method of activating private key

The Root CA private key SHALL be activated automatically by Root CA.

6.2.9 Method of deactivating private key

The Root CA private key SHALL be automatically deactivated after every signature operation.

6.2.10 Method of destroying private key

The Root CA private key SHOULD be physically destroyed in all media holding the Root CA private key.

6.2.11 Cryptographic module rating

Not applicable.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Root CA SHALL archive its public keys and all public keys submitted as part of a certificate application.

6.3.2 Certificate operational periods and key pair usage periods

The CA-Certificate of the Root CA SHALL be valid for 24 years. Operational period of Subject CA certificates SHALL be at most 12 years.

Key pair usage period is identical to the operational period of the corresponding certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulations.

6.4.2 Activation data protection

No stipulations.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Root CA computer systems SHALL satisfy the following requirements:

- The issuing system SHALL be loaded only on a dedicated off-line computer hardware.
- No software not required for the CA operation SHALL be installed on the issuing system.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle technical controls

6.6.1 System development controls

Significant modification of CA systems SHALL be developed and tested on a separated development system.

6.6.2 Security management controls

No stipulations.

6.6.3 Life cycle security controls

No stipulations.

6.7 Network security controls

The issuing system SHALL be loaded only on a dedicated off-line computer hardware.

6.8 Timestamping

No stipulations.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate Profile

The Root CA SHALL issue certificates in accordance with RFC 5280 [RFC5280].

7.1.1 Version number(s)

The Root CA SHALL issue certificates X.509 version 3.

7.1.2 Certificate extensions

The CA certificate of the Root CA SHALL use the following extensions:

1. Basic Constraints (critical)

   CA: true
2. Key Usage

   Certificate Sign, *CRL Sign*
3. Subject Key Identifier

   key identifier of the CA
4. Authority Key Identifier

   key identifier of the CA

Subject CA certificates SHOULD typically use the following extensions:

1. Basic Constraints (critical)

   CA: true
2. Key Usage

   Certificate Sign, CRL Sign
3. Subject Key Identifier

   key identifier of the subscriber
4. Authority Key identifier

   key identifier of the Root CA signing key
5. Authority Information Access

   CA Issuers: URI: locator of the Root CA certificate
6. CRL Distribution Point

   URI: locator of the current Root CA CRL

7.1.3 Algorithm object identifiers

The Root CA SHOULD sign certificates with the following cryptographic algorithm:

SHA256 with RSA Encryption – OID *1.2.840.113549.1.1.11*

7.1.4 Name forms

Subject names of all certificates issued in compliance with this CP/CPS SHALL be constructed according to Section 3.1.

The subject name of the Root CA is

CN=Root CA

OU = Connected Appliances

O=Electrolux

7.1.5 Name constraints

The Root CA SHALL NOT support the Name Constraints extension.

7.1.6 Certificate policy object identifier

This CP/CPS is identified by the OID defined in Section 1.2.2.

7.1.7 Usage of Policy Constraints extension

The Root CA SHALL NOT support the Policy Constraintsextension.

7.1.8 Policy qualifiers syntax and semantics

The Root CA SHOULD NOT support the Policy Qualifierfield of the Certificate Policies extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

The Root CA SHOULD NOT mark the Certificate Policies extension as critical.

7.2 CRL Profile

Lists of revoked certificates published by Root CA SHOULD contain following information:

Attribute	Vaule	Meaning
Version	2	CRL version
Signature Algorithm	Signature algorithm	Algorithm used for CRL signature
Issuer	CA Name	DN of CA
Last Update	UTC time	Time of CRL issuance
Next Update	UTC Time	The latest time of next CRL issuance
CRL extensions	See Chap. 7.2.2	Extensions presented in CRL
Revoked Certificates	See Chap. 4.9	List of revoked certificates

Lists of revoked certificates SHOULD contain following CRL Extensions:

Extension	Value	Meaning
X509v3 CRL Number	Positive integer	sequential number of the CRL
X509v3 Authority Key Identifier	Key fingerprint	key identifier of the Root CA signing key

7.2.1 Version number(s)

The Root CA SHALL issue CRLs version 2 as defined in RFC 5280 [RFC5280].

7.2.2 CRL and CRL entry extensions

The CRL entry SHALL contain following attributes and extensions:

Extension	Value	Meaning
Serial Number	Positive integer	Certificate serial number
Revocation Date	UTC Date and Time	Date and time of certificate revocation
CRL entry extensions	See next table	Extension of the entry

Every CRL entry SHOULD contain following extensions:

Extension	Value	Meaning
X509v3 CRL Reason Code	String	The reason of certificate revocation

7.3 OCSP Profile

7.3.1 Version number(s)

No stipulations.

7.3.2 OCSP extensions

No stipulations.

8 Compliance audit and other assessment

8.1 Frequency or circumstances of assessment

The Root CA SHALL perform an annual compliance audit.

8.2 Identity/qualifications of assessor

The regular audit SHALL be performed by the Root CA *Auditor*.

The Root CA SHALL enable an audit by a third party when required for its operation support and acceptance. In such case, the entire costs of the audit SHALL be covered by the entity requesting the audit.

8.3 Assessor's relationship to assessed entity

See Section 8.2

8.4 Topics covered by assessment

The audit SHALL verify the compliance of the CA operations with this CP/CPS.

8.5 Actions taken as a result of deficiency

If any deficiency is discovered, the Root CA SHALL take actions needed to bring the documentation, operational procedures and configuration into compliance.

8.6 Communication of results

Results of an audit SHALL be considered private to the Root CA.
The Root CA MAY release audit results to third parties at its discretion.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulations.

9.1.2 Certificate access fees

No stipulations.

9.1.3 Revocation or status information access fees

No stipulations.

9.1.4 Fees for other services

No stipulations.

9.1.5 Refund policy

No stipulations.

9.2 Financial responsibility

Certificates issued under this CP/CPS SHALL NOT be used for securing financial transactions.

9.2.1 Insurance coverage

The Root CA operations are not covered by any insurance.

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

Not supported.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The Root CA SHALL keep the following information confidential:

- private keys of all participants
- other cryptographic data used for CA operations
- all personal data except for those included in certificates
- internal CA documentation except for audit reports published at the discretion of the CA

9.3.2 Information not within the scope of confidential information

Information included in certificates and CRLs SHALL NOT be considered confidential.

9.3.3 Responsibility to protect confidential information

The Root CA SHALL NOT disclose confidential information to any third party, except when required by law enforcement officials who exhibit regular warrant.

9.4 Privacy of personal information

9.4.1 Privacy plan

Root CA will not process any personal information.

9.4.2 Information treated as private

Any information that is not publicly accessible or available through the content of a certificate, a CRL, or an OCSP response SHALL be treated as private information.

9.4.3 Information not deemed private

Any information that is publicly accessible or available through the content of a certificate, a CRL, or an OCSP response SHALL NOT be deemed private.

9.4.4 Responsibility to protect private information

All members of the Electrolux AB team SHALL protect such information from compromise and disclosure to third parties.

9.4.5 Notice and consent to use private information

No stipulations.

9.4.6 Disclosure pursuant to judicial or administrative process

The Root CA MAY disclose any confidential or private information to law enforcement officials who exhibit regular warrant.

9.4.7 Other information disclosure circumstances

No stipulations.

9.5 Intellectual property rights

Electrolux AB owns all intellectual property rights associated with this CP/CPS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The Root CA SHALL provide PKI services in compliance with this CP/CPS.

9.6.2 RA representations and warranties

Not applicable.

9.6.3 Subscriber representations and warranties

A subscriber SHALL in particular:

- provide correct and accurate information to the CA,
- immediately inform the CA about any change of information that has been submitted to the CA,
- act in accordance with this policy,
- use certificates and other services of the CA only for legal purposes,
- use certificates only for purposes for which they were issued,
- protect their private keys from compromise, loss, disclosure, or any unauthorized use,
- immediately request revocation of a certificate when it is suspected to have been misused.

9.6.4 Relying party representations and warranties

Before relying on a certificate to verify a digital signature, relying parties SHALL check that at the time of the creation of the signature the certificate was valid, has not been revoked and was issued for the given purpose.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of Warranties

No stipulations.

9.8 Limitations of Liability

The Root CA SHALL NOT be held responsible for circumstances originated in breaching this CP/CPS by subscribers or relying parties.

9.9 Indemnities

No stipulations.

9.10 Term and Termination

9.10.1 Term

This CP/CPS shall become effective seven days after its publication and shall become effective until terminated in accordance with Section 9.10.2.

9.10.2 Termination

This CP/CPS shall remain effective until replaced with a newer version.

9.10.3 Effect of termination and survival

No stipulations.

9.11 Individual notices and communications with participants

No stipulations.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CP/CPS MUST be approved by the Policy Administrator (see Section 1.5.2).

9.12.2 Notification mechanism and period

Any new version of this certificate policy SHALL be published at the CA repository at least 7 days before becoming effective.

9.12.3 Circumstances under which OID must be changed

Small changes that will not change the meaning of the certificate policy MAY be applied without changing the policy OID.

Other changes require assigning a new OID for the CP/CPS.

9.13 Dispute resolution procedures

All disputes SHOULD be solved by agreement of the disputing parties. The supreme authority for solving disputes is the director of the Electrolulx AB.

9.14 Governing law

The Root CA operations SHALL be governed by the law of Kingdom of Sweden.

9.15 Compliance with applicable law

No stipulations.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulations.

9.16.2 Assignment

No stipulations.

9.16.3 Severability

If any of the provisions of this CP/CPS is found to be invalid or unenforceable, the remainder of this CP/CPS SHALL remain effective.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulations.

9.16.5 Force Majeure

No stipulations.

9.17 Other provisions

No stipulations.

Bibliography

[RFC3647]: S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, *Internet X.509 Public KeyInfrastructureCertificatePolicyandCertificationPractices Framework*. November 2003

[RFC2119]: S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*. March 1997

[RFC5280]: D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. May 2008