Private PKI 1 Certification Practice Statement

1.3.171.5.2.1.2.1.1

Version: 1.1
Classification: Unclassified

Document history and validation cycle

Version	Description	Author	Reviewer	Document Status	Date of publication
1.0	Initial release of the document.	*Karim Nehari*	*Benoit Poletti*	*Published*	*20/07/2017*
1.1	Minor updates	Karim Nehari	Benoit Poletti	*Published*	12/10/2017

Table of content

1 INTRODUCTION

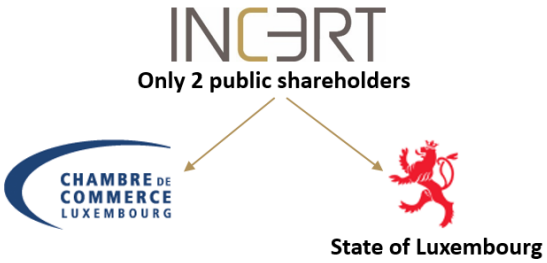
This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which this CPS is targeted.

This document follows the framework and structure outlined in the Internet Engineering Task Force's RFC 3647.

1.1 Overview

INCERT GIE has been founded in August 2012 by the State of Luxembourg and the Luxembourg Chamber of Commerce, and has initiated its establishment in January 2013 by integrating existing IT infrastructures within its organization and by deploying new ones.

Our current shareholding structure brings insurance to the continuity of our business services:



Within the aim to constantly improve its information security and operational activities, INCERT GIE has established since the end of year 2013 the requirements defined in ISO/IEC 27001:2013 standard for all its business and internal services.

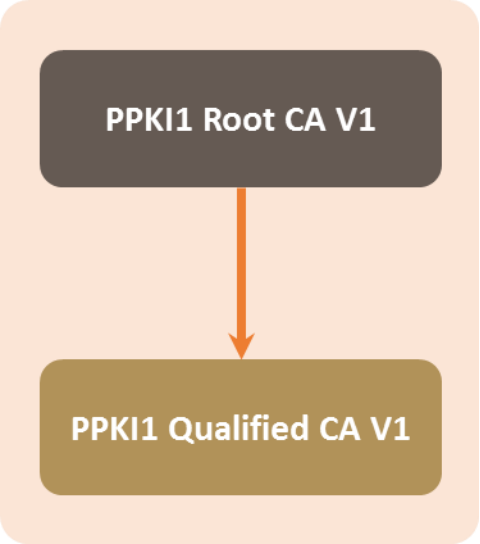
The Private Public Key 1 ("PPKI 1"), has been established by INCERT to enable reliable and secure identity authentication, and to facilitate the preservation of confidentiality and integrity of data in electronic transactions.

This CPS defines the procedures and controls that INCERT requires participants comply with when issuing and managing X.509 certificates under the private public key infrastructure 1 (PPKI1).

This PKI is used to manage the Private PKI1 Root CA V1 and its sub-CA named Private PKI1 Qualified CA V1 (PPKI1 QCA) which issues qualified certificates for natural person.

The PPKI1 QCA provides CRLs and an OCSP service. The key used to sign the OCSP requests is a specific key and the related certificate is signed by the PPKI1 QCA.

This CA is signed by the PPKI1 Root CA which is a self-signed CA and can be used to verify the certification chain. This Root CA is also managed by INCERT.



1.2 Document Name and Identification

The official name of this document is the "Private PKI 1 Certification Practice Statement" (PPKI1 CPS) and it is owned and managed by INCERT.

The OID management rules are described in the document "OID management procedure" (Document J). According to these rules, the identification OID of this document is:

1.3.171.5.2.1.2.1.0

{INCERT OID root}.{PKI}.{Root CA}.{CPS}.{version}.{subversion}

The certificate profiles can be consulted in the Naming and profile document.

1.3 PKI Participants

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI.

This organization described below is only for the proof of concept and audit purposes. In a real case, this PKI would serve to the customer which will be the CA and the registration authorities (RA) will be defined by the customer. INCERT will be only the technical trust infrastructure provider but not the CA.

1.3.1 Certification Authorities

The entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization and this hierarchy is described in section 1.1.

The Private PKI 1 Root CA. The PPKI1 architecture is based on a two-tier CA structure. This architecture allows the Root CA to be stored offline. The Root CA of the Private PKI 1 is called the Private PKI 1 Root CA and it only issues CA certificates. The Root CA is also used for signing the ARL.

The Private PKI 1 Qualified CA. The PPKI1 Qualified CA issues certificates to end entities, manages and revokes end entities certificates. The Qualified CA is also used for signing CRL.

1.3.2 Registration Authorities

These entities are responsible for:

- establishing enrollment procedures for end-user certificate applicants;
- performing identification and authentication of certificate applicants;
- initiating or passing along revocation requests for certificates;
- approving applications for renewal or re-keying certificates on behalf of a CA; and
- establishing an environment and procedure for distributing to subjects their activation data, key pairs and certificate on media (PSE).

RAs may be external to the CA. For person related certificates, the PPKI1 CA may delegate registration of end entities to customer RAs generally for identification and authentication of initial certificate applicants.

1.3.3 Subscribers (End Entities)

The subscribers who may receive certificates from the issuing CA include:

- Physical persons (for example employees, customers of INCERT);
- Device or application (for example OCSP application).

Subscribers must have a valid contractual relationship with INCERT and shall comply with the requirements related to the section 4.

1.3.4 Relying Parties

Relying Parties are entities that act in reliance on a certificate and/or digital signature issued by the Issuer CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

1.3.5 Other Participants

The CA must contractually obligate each RA and subcontractor to comply with all applicable requirements in this CPS and to perform them as required of the CA itself. The CA shall enforce these obligations and may internally audit each RA's, and subcontractor's compliance with these requirements on an annual basis.

External services or qualified electronic signature creation device providers support the CA activities under a signed contractual agreement.

1.4 Certificate Usage

This subcomponent contains:

- A list or the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and a travel order, and/or
- A list or the types of applications for which use of the issued certificates is prohibited.

A certificate is formatted data that cryptographically binds an identified subscriber with a public key and allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1 Appropriate Certificate Uses

All certificates issued within the Private PKI 1 hierarchy shall have key usage extensions and may have enhanced key usage extensions, as defined within RFC 5280 that defines acceptable usage of and provide a basis for reliance upon, the private key corresponding to the public key that is contained within the certificate. These key usage and enhanced key usage extensions are described in the "PPKI1 – Naming and profile document".

Root CA certificate – This certificate is signed by the Root CA certificate itself and only approved for signing the CA certificates of issuing CA (Qualified CA) and the ARL.

Qualified CA certificate – This certificates is signed by the Root CA certificate and is approved only for the signing of the end entity certificates, the Qualified CA's CRL and OCSP signer certificates.

End entity signing certificates – These certificates are approved only for digital signature (authenticity, integrity and non-repudiation usages).

1.4.2 Prohibited Certificate Uses

Other uses of digital certificates issued under this CPS unless specified in previous section 1.4.1 "Appropriate Certificate Uses" are prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS and the documents referenced herein are maintained and administered by INCERT which can be contacted at:

INCERT GIE,
IVY Building, 13-15 Parc d'activités,
L-8308 Capellen
Grand-Duchy of Luxembourg

E-mail: ppki@incert.lu
Web site: https://www.incert.lu
LinkedIn: https://www.linkedin.com/company/incert-gie

1.5.2 Contact Person

Questions regarding this CPS shall be directed to the Security and operations manager or another member of his department:

Security and operations manager
INCERT GIE
IVY Building, 13-15 Parc d'activités,
L-8308 Capellen
Grand-Duchy of Luxembourg

E-mail: ppki@incert.lu
Tel: (352) 273 267 1

1.5.3 Person Determining CPS Suitability for the Policy

The Security and operations manager approves the CPS which is subordinate to the CP.

1.5.4 CPS approval procedures

The director of INCERT and the Security and operations manager review any modifications, additions or deletions to this CPS and determine if these changes are acceptable. At their sole discretion, they must approve or reject any proposed changes of this CPS.

1.6 Definitions and Acronyms

This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the document and their meanings.

1.6.1 Definitions

1.6.2 Acronyms

ARL
Authority Revocation List

CA
Certification Authority

CDP
CRL Distribution Point

CP
Certificate Policy

CPS
Certification Practice Statement

CRL
Certificate Revocation List

CSS
Certificate Status Service

DN
Distinguished Name

ECDSA
Elliptic Curve Digital Signature Algorithm

FIPS
Federal Information Processing Standards

HTTP
Hypertext Transfer Protocol

IEC
International Electrotechnical Commission

IETF
Internet Engineering Task Force

LDAP
Lightweight Directory Access Protocol

LRA
Local Registration Authority

ISO
International Organization for Standardization

ITU
International Telecommunications Union

ITU-T
International Telecommunications Union – Telecommunications Sector

NIST
National Institute of Standards and Technology

OCSP
Online Certificate Status Protocol

OID
Object Identifier

PIN
Personal Identification Number

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PKIX
Public Key Infrastructure X.509

PPKI(1)
Private Public Key Infrastructure (1)

PSE
Personal Secure Environment

PSS
Probabilistic Signature Scheme

RA
Registration Authority

RFC
Request For Comments

RSA
Rivest-Shamir-Adleman

RSASSA
RSA Signature Scheme with Appendix

SHA
Secure Hash Algorithm

SIEM
Security information and event management

SSL
Secure Sockets Layer

TLS

Transport Layer Security

URL
Uniform Resource Locator

UTF-8
Universal Character Set Transformation Format - 8 bits

WWW
World Wide Web

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The PPKI1 makes its CP, CA Certificate(s) publicly available through the INCERT repository accessible at *https://www.incert.lu/download* and additional appropriate communication channels.

The related CRL and ARL are publicly available on the CRL distribution point which can be reached at *http://crl.ppki.incert.lu*.

The online certificate status information can also be accessible via *http://ocsp.ppki.incert.lu*.

These repositories are operated by INCERT itself.

2.2 Publication of Certification Information

INCERT ensures that the following information is published:

- PPKI1 Certificate Policy (*https://repository.incert.lu/ppki_cp.pdf*);
- PPKI1 Certificate Practice Statement (*https://repository.incert.lu/ppki_cps.pdf*);
- PPKI1 Terms and conditions including the PKI Disclosure Statement (*https://repository.incert.lu/ppki_pds.pdf*);
- PPKI1 Root CA Certificate (*https://repository.incert.lu/ppkirca.cer*);
- PPKI1 Qualified CA Certificate (*https://repository.incert.lu/ppkiqca.cer*);
- PPKI1 Root CA ARL (*https://crl.ppki.incert.lu/ppkirca.crl*);
- PPKI1 Qualified CA CRL (*https://crl.ppki.incert.lu/ppkiqca.crl*).

2.3 Time or Frequency of Publication

INCERT must annually review and update the CP for required compliance changes. The updated version of the CP or any new CA certificate will be made publicly available within thirty days of the incorporation of changes.

The CRLs of the issuing CAs are usually published every 1 hour and at least once every 24 hours.

The ARL is published at least once every 6 months and at each new revocation.

2.4 Access Controls on Repositories

Published information objects described in previous sections 2.1 and 2.2 are accessible only in "read-only" right. As long as this information is published in one of these repositories is public information.

INCERT shall implement logical and physical controls to prevent unauthorized write access to repositories.

The publication is hardened and monitored to ensure an adequately control access and to prevent any unauthorized persons from adding, modifying or deleting records of this service.

More information is available in the monitoring management procedure.

In production, a script will be implemented to check the authenticity and integrity of published document (this script is already used for other customer).

3 IDENTIFICATION AND AUTHENTICATION

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

3.1 Naming

Requirements for naming in certificates are as specified in recommendation ETSI EN 319 411-1 V1.1.1 section 6.2.1.

3.1.1 Types of Names

Types of names assigned to the subject, such as:

- X.500 distinguished names;
- RFC-822 names; and
- X.400 names.

Each certificate must have a unique name for the Subscriber in the certificate DN field.

The CN cannot be blank and DN must use UTF-8 printable characters.

A distinguished name which has been used in a certificate by it shall never be re-assigned to another entity.

In all end-entity certificates of identity, the Common Name field contains the full name of the certificate subscriber.

The profile is based on the IETF RFC 5280 recommendations, and the ITU-T X.509 standard. The ETSI EN 319 412-1 and 319 412-2 documents specify the content of the certificates issued to natural persons, and the naming and profile document reflects these recommendations.

3.1.2 Need for Names to be Meaningful

In the case of end entity certificates, the CN contains understood names permitting the determination of the identity of the individual and is provided by the RA as well as the DN.

All certificates naming are described in the “PPKI1 - Naming and profile document”.

3.1.3 Anonymity or Pseudonymity of Subscribers

The PPKI1 Qualified CA may issue end-entity pseudonymous certificates provided that such certificates are not prohibited by applicable policy and name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting various name forms are the X.500 standard, ASN.1 syntax and RFC-822. UTF-8-character set shall be used.

RFC-822 names may be used as Subject’s Alternative Names by indicating the e-mail address of the certificate subscriber.

3.1.5 Uniqueness of Names

The PPKI1 ensures that its CA certificates DN are unique at a given moment. For under each CA and for a specific profile, the PPKI1 ensures that end entity certificates DN are unique and that within a given hierarchy, it cannot be reassigned a subscriber name that has been used by another subscriber.

To avoid duplication of names between different people it may be incorporated the unique national identity card number or the unique social security number identification into the chain of the name that distinguishes the certificate holder.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants may not request certificates with any content that infringes the intellectual property rights of another entity.

3.2 Initial Identity Validation

Applicants for certificates are end entities. The applicant always acts on behalf of the Subscriber.

A certificate shall be issued to a Subject only when the Subject has submitted a Certificate Request and is able to prove to the CA possession of the corresponding private key.

3.2.1 Method to Prove Possession of Private Key

A certificate request must be a self-signed certificate (only accepted as PKCS#10 certificate request) to demonstrate possession of a private key. Signature verification of a PKCS#10 certificate request, which it will be included the public key signed by the associated private key, constitute sufficient proof of possession of the corresponding private key.

This certificate request is sent to the RA service for validation then to the CA service for processing, which makes it possible to detect errors in the generation of the certificate and proves that the subscriber already has the key pair in his/her possession, and can make use of them.

In case of centralized request (the key pair is generated by the CA factory), this requirement is not applicable.

3.2.2 Authentication of Organization Identity

A Subscriber enrollment process must be made by a person authorized to act on behalf of the organization. The enrollment process must include details about the Subscriber as requested by the CAs. The details must be provided in a secure manner.

The RAs must verify the identity of the Subscriber and its right to represent the organization with documents recognized by the Grand-Duchy of Luxembourg. Records of the details used for the Subscriber's identification must be kept for at least seven (7) years.

3.2.3 Authentication of Individual Identity

Identification and authentication requirements for an individual Subscriber or participant (RA, in the case of certificates issued to organizations or devices controlled by an organization, the subscriber, or other participant), includes:

a) An official document required (as eID, ePassport or eRP);
b) In-person appearance before an RA;
c) A visual check of the Subscriber by comparing with the photo on the document provided.

The real procedure will be defined by the customer according to the eIDAS regulation.

3.2.4 Non-Verified Subscriber Information

Information that is not verified (called "non-verified subscriber information") during the initial registration is listed below:

- Subscriber's email.

All other information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key

See section 4.7.

3.3.2 Identification and Authentication for Re-Key after Revocation

The procedures for re-keying after revocation are the same those for the original certificate.

3.4 Identification and Authentication for Revocation Request

Revocation of issuing CA certificates shall only be performed manually by Security and operations team members under dual control.

Revocation requests for end entity certificates are authenticated by the CA and the RA in the same manner of an initial registration to be sure that the Subscriber has effectively requested for the revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This section describes the requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

4.1 Certificate Application

An application for a certificate does not oblige a CA to issue a certificate.

The CA maintains controls to provide reasonable assurance that, for domain validated certificates, Subscriber's certificate requests are accurate, complete and validated.

4.1.1 Who can Submit a Certificate Application

For the Root CA, only Security and operations team manager or the director can decide when a new issuing CA is to be created and to be signed by the Root CA.

For the issuing CAs, certificate applicant can be any physical person.

4.1.2 Enrollment Process and Responsibilities

For CA certificates, following information shall be documented:

- Certificate profile of the new issuing CA including the new CA name (duration of this new CA cannot exceed the rest of duration of the Root CA at the creation date);
- CPS for the new issuing CA; and
- End entity certificate profiles of this new issuing CA.

For end entity certificate application, the enrollment process consisting of:

- Generating or arranging to have generated a key pair;
- Providing a certificate request based on the generated key pair and if the key pair is not generated by the CA, demonstrating to the respective RA that the certificate applicant has possession of the private key corresponding to the public key included in the certificate application;
- Completing the relevant certificate application form with true and correct information; and
- Notifying certificate applicants of the subject responsibilities for usage of the private key and certificates (see Terms and conditions document).

4.2 Certificate Application Processing

This section describes the procedure for processing certificate applications. The issuing CA and RA shall perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application. Finally, this section sets a time limit during which a CA and/or RA must act on and process a certificate application.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in sections 3.2 and 3.3 of this present CP.

For end entity certificates the PPKI1 CA delegates these tasks to respective RAs managed by the customer of this private PKI which have been trusted and for which the general requirements on the security of the TSP apply.

The data collected by the trusted RAs during the certificate application and needed to generate the certificate shall be exchanged securely.

4.2.2 Approval or Rejection of Certificate Applications

The CA or a RA verify that the certificate application is complete, accurate and authorized. If validation fails the certificate application is rejected.

The CA or a RA must notify the subscriber that the request has been rejected or approved. If approved, the CA must create a certificate and provide the subscriber with access to the certificate.

4.2.3 Time to Process Certificate Applications

Certificate application shall be approved or rejected within 3 months after application.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

For the Root CA, the computer running Root CA services is not connected to the network and is located in offline security vault which complies with security standards for cryptographic modules set forth in section 6.2, to ensure proper security of the Root CA key pair.

Procedures are established in the key management policy in order to ensure integrity and non-repudiation of certificate requests and certification of the new issuing CA's public key. Access to the Root CA hardware security module is granted only for authorized personnel from Security and operations team. The Root CA private key must not be used to sign certificates except in the following cases:

- Self-signed certificates to represent the Root CA itself; and
- Certificates for issuing CAs and cross certificates.

For end entity certificate, a certificate is created and issued following approval of a certificate request by authorized persons of following receipt of a RA's request to issue the certificate and using secure means. The issuing CA shall:

- Generate for the subject a certificate based on the information in the certificate application after its approval;
- Check authorization of the respective trusted RA through a secure server; and
- Deliver the certificate, key pair and activation data in case of key pair generated by the CA and only the certificate if a certificate request (in PKCS#10 format) was received.

Moreover, the RA entity provides a Terms and conditions copy sent to the subscriber, as well as the identification minute issued by the RA that intervened in the identification process and notifies the subscriber via email of the conformity of their request.

The CA service proceeds in performing the security integrity verification of the documents received, verifying their consistency and their correspondence with the Certification Policy to which the requested certificate will be submitted. In case of conformity, the certificates are issued.

Once the certificate is issued, the RA informs the subscriber via email, proceeds to activate the necessary computer mechanisms. The subscriber, using the same electronic signature cryptographic device that he used to generate the key pair and request certificate, can download, and install it.

The CA service signs the public keys of the certificates it issues with its private key.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CA through the RA or directly the RA has to notify subjects that their certificates are available and the means for securely obtaining their certificates.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

For instance, acceptance is deemed to occur if the CA or RA does not receive any notice from the subscriber within 7 working days after reception of the certificate describing the reason for rejection and the fields in the certificate that are incorrect or incomplete.

By accepting and using the certificate, the subscriber agrees to comply with the terms and conditions. The RA shall record the signed agreement (terms and conditions) with the subscriber.

4.4.2 Publication of the Certificate by the CA

All CA certificates shall be published as specified in section 2. End entity certificates are not published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The issuing CA may send the certificate to the RA which has done the request and may notify the other RAs.

4.5 Key Pair and Certificate Usage

This section describes the responsibilities relating to the use of keys and certificates.

4.5.1 Subscriber Private Key and Certificate Usage

The Root CA private key is only used for signing:

- Root CA certificate;
- Issuing CA certificates; and
- ARLs;

An issuing CA must only use its private key for use with production implementations and to sign:

- End entity certificates;
- OCSP signer certificate; and
- CRLs.

End entity private keys and certificates shall only be used for the purposes as specified in the certificate. The use of a private key and its certificate are subject to the terms and conditions after the subscriber has accepted the agreement.

The subscriber is responsible for ensuring integrity and confidentiality of its private key and shall be required to use the private key.

4.5.2 Relying Party Public Key and Certificate Usage

Each relying party is obligated to:

- Rely on certificates only for appropriate applications as set forth in the present CP and in consistency with applicable certificate content;
- Successfully perform public key operations as a condition of relying on a certificate;
- Assume responsibility to check the status of a certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see section 4.9); and
- Assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

4.6 Certificate Renewal

This section describes the following elements related to certificate renewal. Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

Certificate renewal is not allowed.

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

This section describes the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

4.7.1 Circumstance for Certificate Re-Key

Circumstances under which certificate re-key can or must take place are following:

- To get a new certificate before the expiration of the previous one;
- To get a new certificate after the previous one is revoked for reasons of key compromise or after a certificate has expired and the usage period of the key pair has also expired;
- To get a new certificate after holder information modification.

4.7.2 Who May Request Certification of a New Public Key

Any subscriber is allowed to request a new public key.

4.7.3 Processing Certificate Re-Keying Requests

In case of getting a new certificate before the expiration of the previous one, subscriber re-key requests may be processed using the same process used for initial certificate issuance except the face to face step which is not anymore mandatory.

In case of getting a new certificate after revocation or expiration, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

Not expired existing evidences can be re-used to validate the identity.
If the terms and conditions have changed, these shall be communicated to the subscriber.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No stipulation.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

This section describes the following elements related to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key. The new certificate shall have a different key, a different serial number and differs in one or more other fields from the old certificate.

4.8.1 Circumstance for Certificate Modification

Certificate modification can take place, such as name change, role change, or reorganization resulting in a change in the DN.

4.8.2 Who May Request Certificate Modification

Any subscriber is allowed to request a certificate modification if this request is relevant.

4.8.3 Processing Certificate Modification Requests

If subscriber information used to generate the certificate changes, then legal evidence of this change has to be provided to the RA.
If the change is validated, the old certificate must be revoked and the subscriber shall process to certificate re-key (see section 4.7).

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate may be suspended and circumstances under which it must be revoked, for instance, in cases of:

- Subscriber employment termination (in case of a company CA);
- Subscriber failure to comply with the terms and conditions or the obligations set out in the related CP;
- Loss of cryptographic token;
- Suspected compromise of the private key;
- Business relationship under which the certificate was issued changes;
- Subscriber's verified data change.

4.9.2 Who can Request Revocation

The revocation of the participant's certificate must only requested by:

- The subscriber to whom the certificate is issued;
- A manager or organization on behalf of a subscriber (if applicable);
- An RA related to the issuing CA;
- The issuing CA;
- In specific case, the Security and operations team may request revocation.

4.9.3 Procedure for Revocation Request

Procedures used for certificate revocation request are defined by the trusted RAs and must include at least a form which may be in an electronic format and provided by the RAs.

A revocation request shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated.

The revocation request shall be transmitted, after RA validation, in a secure way to the CA and then processed.

All revocation of any certificate is definitive and the certificate shall not be reinstated.

The subscriber shall be informed by the RA or the CA of the change of status of the certificate.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted by the requestor as soon as having reason to believe that there is a circumstance for certificate revocation.

4.9.5 Time Within which CA Must Process the Revocation Request

The CA concerned shall process the revocation request within 24 hours after its submission.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. It is the responsibility of the Relying Party to determine how often new revocation data should be obtained, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

A relying party shall check the status of certificates on which they wish to rely by consulting:

- The most recent CRL published by the concerned CA; or
- OCSP service.

4.9.7 CRL Issuance Frequency

The CRLs of any issuing CA are issued every 1 hour.

The ARL is issued every 6 months.

4.9.8 Maximum Latency for CRLs

CRL shall be posted to the repository within a reasonable time after issuing. This is generally done automatically within minutes of generation but shall not exceed the stated time of the next CRL issue.

4.9.9 On-Line Revocation/Status Checking Availability

The PPKI1 can provide on-line service for checking the status of certificates. This service is available 24 hours per day, 7 days per week through an OCSP service at the following URL:

http://ocsp.ppki.incert.lu/ocsp-services/ocsp

In case of system failure preventing to provide the service, INCERT shall make best endeavours to ensure the service level availability defined with the customer:

- 99,0%.

The OCSP signing certificate contains an extension of type *id-pkix-ocsp-nocheck* as defined by the RFC 6960.

4.9.10 On-Line Revocation Checking Requirements

The relying parties using on-line revocation status service, shall check the integrity and authenticity of the status information.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements related to key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Certificates that are issued under this Policy shall not be suspended.

4.9.14 Who can Request Suspension

Certificates that are issued under this Policy shall not be suspended.

4.9.15 Procedure for Suspension Request

Certificates that are issued under this Policy shall not be suspended.

4.9.16 Limits on Suspension Period

Certificates that are issued under this Policy shall not be suspended.

4.10 Certificate Status Services

This section addresses the certificate status checking services available to the relying parties.

4.10.1 Operational Characteristics

Certificate status information is available through CRL (HTTP CDP) and OCSP responder as described in section 4.9.6.

Revocation entries on a CRL or OCSP Response must not be removed until after the expiration date of the revoked Certificate.

4.10.2 Service Availability

The Certificate status service is available on a 24x7 basis except in case of Force Majeure events (see section 9.16.5).

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A Subscriber's subscription service ends if:

- Its certificate expires;
- Its certificate is revoked; or
- The business relationship with INCERT expires or is terminated.

4.12 Key Escrow and Recovery

The CA and end entity private key(s) must not be escrowed.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

5.1 Physical Controls

In this section, the physical controls on the facility housing the entity systems are described.

5.1.1 Site Location and Construction

The location and construction of the facility that will house CA equipment and operations shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

The online CAs shall be hosted in a Tier IV location.

The Root CA(s) shall be kept in a safe in a secure location protected by intrusion sensors and held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing issuing CA certificates.

5.1.2 Physical Access

Physical access to CA rooms or offline CAs shall be:

- Limited to authorized individuals;
- Logged;
- Protected from theft of information or compromising; and
- Located in protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

Specific requirements regarding the keys generation are described in the “Key management policy” document.

5.1.3 Power and Air Conditioning

The locations are equipped with power systems capable of ensuring redundant power supply and redundant air conditioning systems.

5.1.4 Water Exposures

The locations are equipped with flooding detection system.

5.1.5 Fire Prevention and Protection

The locations are equipped with:

- Fire detection alarm system;
- Easily available portable and fixed extinguishing equipment's; and
- Emergency procedures for the full facilities.

5.1.6 Media Storage

The PPKI1 must maintain controls to provide reasonable assurance that media are securely handled to protect them from damage, theft and unauthorized access.

All media are handled securely in accordance with requirements of the information classification scheme and media containing sensitive are securely disposed of when no longer required.

5.1.7 Waste Disposal

The destruction of confidential data shall be ensured by a secure wiping.

5.1.8 Off-Site Backup

Full system backups, sufficient to recover from system failure, shall be made on a monthly basis and stored in the INCERT PKI safe.

5.2 Procedural Controls

In this section, requirements for recognizing trusted roles are described, together with the responsibilities for each role. Examples of trusted roles include system administrators, security officers, and system auditors.

5.2.1 Trusted Roles

Each CA or delegated third party shall document the responsibilities and tasks assigned to trusted roles and implement "separation of duties" for such trusted roles based on the security-related concerns of the functions to be performed.

The PPKI1 trusted roles are described in the document titled "PPKI1 – Security roles and responsibilities".

5.2.2 Number of Persons Required per Task

Two or more persons are required for the following tasks:

- CA key generation;

- Change in the certificate profiles;
- CA signing key activation; and
- CA private key backup.

Where at least dual control is required, at least one of the participants shall be an administrator. All participants must serve in a trusted role as defined in section 5.2.1. Dual control shall not be achieved using personnel that serve in the auditor trusted role.

5.2.3 Identification and Authentication for Each Role

CA software and hardware shall identify and authenticate its users who shall occupy a trusted role.

5.2.4 Roles Requiring Separation of Duties

Individual shall not assume more than one of these trusted roles. No individual shall be assigned more than one identity.

Individual shall not be able to sign subordinate certificates on its own.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The PPKI1 must require that personnel performing duties with respect to the operation of one of its CAs have sufficient training, qualifications, and experience in PKI. PPKI1 personnel must also meet INCERT personnel security requirements.

5.3.2 Background Check Procedures

Background checks must be performed on the PPKI1 operations personnel in accordance with INCERT standard hiring practices.

5.3.3 Training Requirements

INCERT provide comprehensive and appropriately training for the PPKI1 personnel performing duties with respect to the operation of a CA. Topics shall include the operation of the CA software and hardware, operational and security procedures, and the stipulations of this policy.

5.3.4 Retraining Frequency and Requirements

The PPKI1 personnel shall be aware of changes in the CA operation. Any significant change to the CA operation shall have a training (awareness) plan, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The INCERT management shall take appropriate administrative and/or disciplinary actions against personnel who have willingly performed actions that are not authorized in the CP, this CPS, or other published procedures published by the INCERT management.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the PPKI1 shall be subject to the same criteria as INCERT employees and shall be always escorted in the PPKI1 facilities.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role. This documentation includes:

- The relevant CP;
- Relevant parts of this CPS;
- Operating procedures;
- Information security policy; and
- Security handbook.

5.4 Audit Logging Procedures

This section describes event logging and audit systems, implemented for the purpose of maintaining a secure environment.

5.4.1 Types of Events Recorded

For any CA governed by this CP, security auditing capabilities of the underlying CA equipment operating system shall be enabled during installation and operation. At a minimum, the following events shall be recorded:

- CA keys lifecycle management events;
- Keys managed or generated by the CAs lifecycle management events;
- Certificates lifecycle management events;
- PKI application event (configuration change, start-up …);
- Network equipment's activities; and
- Security events.

At a minimum, each audit record shall include the following details:

- The type of event;
- The date and time the event occurred;
- A success or failure indicator; and
- The identity of the entity and/or operator of the CA that caused the event.

5.4.2 Frequency of Processing Log

The audit logs are processed following an alarm or anomalous event and are archived when the audit log storage is 90% full.

5.4.3 Retention Period for Audit Log

The PPKI1 shall retain the described audit logs for seven (7) years after certificate based on these records ceases to be valid.

5.4.4 Protection of Audit Log

Only authorized personnel, assigned to a trusted role, may access to audit logs. Audit logs must be protected against unauthorized viewing (confidentiality), modification (integrity) and deletion (availability).

The protection established may depend on the confidentiality of data in the audit logs.

5.4.5 Audit Log Backup Procedures

Audit logs are backed up regularly on an external media which shall be stored in a safe in different facility. Log files are backed up according internal procedures.

5.4.6 Audit Collection System (Internal vs. External)

The audit collection system is internal to INCERT.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The audit logs are collected by an internal SIEM. Specific rules shall be implemented in order to identify potential attempts to breach the security of the system.

5.5 Records Archival

This section describes general records archival policies.

5.5.1 Types of Records Archived

The PPKI1 shall archive the following:

- Log for all events relating to the life-cycle of keys managed by the CA, certificates and any subject key pairs generated by the CA;
- Documentation describing the procedures and policies to manage the PPKI1;
- PKI and OCSP application configuration.

5.5.2 Retention Period for Archive

The PPKI1 shall retain these records for seven (7) years after any certificate based on these records ceases to be valid.

5.5.3 Protection of Archive

Only authorized personnel, assigned to a trusted role, may access to records archives. Archives must be protected against unauthorized viewing (confidentiality), modification (integrity) and deletion (availability).

The protection established may depend on the confidentiality of records archived.

5.5.4 Archive Backup Procedures

Archive may be backed up.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized trusted role and other authorized person are allowed to access the archive.

5.6 Key Changeover

Automatic key changeover is not supported. However, the CA shall periodically and at a suitable time before its expiration change its private keys preventing downtime in the CA operation.

After key changeover and even the old key is not expired, the CA shall use only the new one to sign certificates.

The CA shall make its old certificate (including the old keys) available to verify signature and sign CRL related to the certificates signed with the old key.

Link certification may be used to certify the new CA with the old key.

5.7 Compromise and Disaster Recovery

This section describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately.

5.7.1 Incident and Compromise Handling Procedures

Information related to business recovery of the CA is provided in BCP procedure.

When there is a compromise of a CA, the PPKI1 must:

- Notify its Subscribers and Relying parties promptly;
- Revoke certificates associates with the compromised key;
- Investigate the compromise;
- Produce an analysis report with actions plan;
- Implement the actions;
- Renew the CA; and
- Notify the Subscribers and Relying parties.

Detailed instructions are specified in:

- This document;
- Incident management procedure; and
- BCP procedure.

INCERT has implemented an incident and problem management policy including a procedure in order to respond quickly to incidents and to limit the impact of security breach or any other incident. Employees are assigned to trusted roles to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the procedure. Critical malfunctions are acted upon on the basis of the same procedure.

The incident and problem management policy also specifies how to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a

significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

In case of security incident, internal procedures are used. In addition, the Supervisory body will be notified within 24 hours after having become aware of it.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

INCERT provides a ticketing tool to its clients and providers in order to report and follow any incident, change or problem.

5.7.2 Computing Resources, Software, and/or Data are corrupted

Local failover capabilities must be implemented to mitigate the loss of computing resources and software or data corruption. When the primary site is inoperable, the BCP must be implemented to ensure the business continuity. Detailed instructions are specified in the BCP procedure.

5.7.3 Entity Private Key Compromise Procedures

The same procedures for the initial creation of a CA are used.

5.7.4 Business Continuity Capabilities after a Disaster

Detailed instructions are specified in the BCP procedure.

5.8 CA or RA Termination

This section describes requirements relating to procedures for termination and termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

In the event that it is necessary for the PPKI1 to terminate a CA service, the PPKI1 shall notify Relying Parties, and other affected entities of the CA termination. Following termination plan should minimize disruption to Relying Parties:

- Notify parties affected by the termination;
- Revoke the certificate issued to Issuing CAs;
- Preserve the CA's archives and records for the time periods required in the related CP;
- Continue the support services;
- Continue the VA services (issuing CRLs…);
- Archive the Root CA's Private Key; and

- Retain the information needed for the transition of actual Root CA's services to the next Root CA.

More instructions are specified in the "Key management policy".

6 TECHNICAL SECURITY CONTROLS

This section defines the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares).

This section also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

6.1 Key Pair Generation and Installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

6.1.1 Key Pair Generation

The key pairs of the Root CAs and Issuing CAs are currently generated in a physically secured environment with a hardware security module by trusted role personnel. Detailed instructions are specified in the "Key management policy".

6.1.2 Private Key Delivery to Subscriber

If the PPKI1 generates the Subscriber's key, the key management policy shall apply and the key's specifications are in accordance with the certificate profile (described in the "naming and profile document".

6.1.3 Public Key Delivery to Certificate Issuer

A certificate Subscriber's public key and identity shall be delivered securely (SSL/TLS session or in a message signed by the RA) to the CA in a certificate signing request (CSR).

6.1.4 CA Public Key Delivery to Relying Parties

The certificates of issuing CAs are distributed to Relying Parties for certificate path validation purposes. The issuing CAs' public keys are published at the PPKI1 repository (see section 2.2).

6.1.5 Key Sizes

The PPKI1 CA's key lengths are defined in the "Naming and profile document" and follow the requirements described in the "Key management policy".

6.1.6 Public Key Parameters Generation and Quality Checking

The issuing CA shall check the public key parameters before issuing the certificate.

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

See the "Naming and profile document".

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Requirements for private key protection and cryptographic modules need to be considered for the issuing CA, repositories, RAs, and subscribers.

6.2.1 Cryptographic Module Standards and Controls

See the "Key management policy".

6.2.2 Private Key (n out of m) Multi-Person Control

See the "Key management policy".

6.2.3 Private Key Escrow

Not applicable.

6.2.4 Private Key Backup

See the "Key management policy".

6.2.5 Private Key Archival

See the "Key management policy".

6.2.6 Private Key Transfer into or from a Cryptographic Module

See the “Key management policy”.

6.2.7 Private Key Storage on Cryptographic Module

See the “Key management policy”.

6.2.8 Method of Activating Private Key

See the “Key management policy”.

6.2.9 Method of Deactivating Private Key

See the “Key management policy”.

6.2.10 Method of Destroying Private Key

See the “Key management policy”.

6.2.11 Cryptographic Module Rating

See the “Key management policy”.

6.3 Other Aspects of Key Pair Management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants.

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival process.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

See the “Key management policy”.

6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and

subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction.

Activation data is used to protect any CA private key, it must be unique and unpredictable and it must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. Activation data may be user selected.

Activation data for cryptographic modules shall be memorized, or if written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

6.5 Computer Security Controls

This section describes computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object re-use, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

6.5.1 Specific Computer Security Technical Requirements

All computer security technical controls implemented for the PPKI1 CAs and Certificate Validation Service are established and documented in accordance to the INCERT ISMS policy.

Local network components shall be kept in a physically and logically secure environment and their configurations shall be periodically checked for compliance with the requirements specified in the INCERT ISMS policy. Multi-factor authentication shall be enforced for all PKI application accounts capable of directly causing certificate issuance.

Certificate Validation Service shall enforce access control on attempts to modify certificate validation status.

All components at the PPKI1 (except offline devices) are subject to constant monitoring.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

This section addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, and configuration management security during product maintenance, software engineering practices, software development methodology, modularity, and layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

6.6.1 System Development Controls

System development controls are provided in accordance with systems development and change management standards of ISMS. Systems development is performed by trusted software supplier(s) in accordance with specifications for secure programming.

The CA software used by the PPKI1 shall be designed and developed under a documented development methodology.

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration.

The PPKI1 security management controls are provided in compliance with the document entitled "Annex 1 to Information security and operational policy".

6.6.3 Life Cycle Security Controls

All Security Controls are audited annually by an external auditor.

6.7 Network Security Controls

This section addresses network security related controls, including firewalls. The PPKI1 shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones. The PPKI1 shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

The PPKI1 shall grant access to secure zones and high security zones to only trusted roles.

The Root CA system should be offline or at least in a high security zone.

Detailed descriptions of implemented network security controls are available as internal documents.

6.8 Time-Stamping

Certificates, CRLs, and Online Certificate Status Protocol (OCSP) responders contain time and date information. Time information does not need to be cryptographic-based.

7 CERTIFICATE, CRL, AND OCSP PROFILES

This section specifies the certificate format and, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used. All digital Certificates issued by the root CAs and the issuing CAs comply with digital Certificate and CRL profiles as described in RFC 5280.

7.1 Certificate Profile

See the “Naming and profile document”.

7.2 CRL Profile

See the “Naming and profile document”.

7.3 OCSP Profile

The OCSP shall be as defined in RFC 6960. The OCSP Responder is operated to provide an interface for a qualified validity check of certificates within the PPKI1. The OCSP responder returns a signed response signifying that the certificate specified in the request is good, revoked, unknown or unauthorized. If it cannot process the request, it returns an error code. Requests for certificate which are not provided by one of the PPKI CA’s will be rejected as “unknown”.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment.

8.1 Frequency or Circumstances of Assessment

There shall be a period of no greater than two years for a full (re-)assessment audit unless otherwise required by the applicable legislation or commercial scheme applying this CP.

8.2 Identity/Qualifications of Assessor

The compliance auditor:

- Shall be external auditor;

- Must demonstrate competence in the field of Public Key Infrastructure (PKI) and information system security;
- Must be thoroughly familiar with the requirements that the ETSI imposes on the issuance and management of certificates; and
- Should perform compliance audits as a primary responsibility.

8.3 Assessor's Relationship to Assessed Entity

The assessor should be impartial and independent of the assessed entity's operational and policy authorities.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that the CA factory comply with all the requirements of this CPS, the associated CP.

The CA factory components shall undergo an audit in accordance with:

- The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation);
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part1: General requirements V1.1.1 (2016-02);
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for trust service providers issuing EU qualified certificates V2.1.1 (2016-02); and
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

8.5 Actions Taken as a Result of Deficiency

If a compliance audit or other assessments of the PPKI1 show deficiencies of the assessed entity:

- The compliance auditor must note the finding as part of the report;
- A determination of correctives actions to be taken shall be made. The determination is made by the INCERT Audit Risk and Compliance committee.

8.6 Communication of Results

The audit compliance report shall be provided to the INCERT Audit Risk and Compliance committee. This committee may make available this report to the RA using the PPKI1.

9 OTHER BUSINESS AND LEGAL MATTERS

This section covers general business and legal matters. The contractual agreement establishing the relationship between INCERT and its customers (PPKI1 users) prevail and provide more detailed information.

9.1 Fees

This section contains any applicable provisions regarding fees charged by CAs, repositories, or RAs. Any detailed fees description is provided in the contractual document establishing the relationship between INCERT and its customers (PPKI1 users).

9.1.1 Certificate Issuance or Renewal Fees

Any CA of the PPKI1 may charge fees for the issuance or renewal of certificates.

9.1.2 Certificate Access Fees

Any CA of the PPKI1 may charge fees for access of certificates.

9.1.3 Revocation or Status Information Access Fees

Any CA of the PPKI1 shall not charge fees for access to revocation or status information.

9.1.4 Fees for Other Services

Any CA of the PPKI1 may charge fees for other services.

9.1.5 Refund Policy

Any CA of the PPKI1 may establish a refund policy.

9.2 Financial Responsibility

This section contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations.

Specific instructions may be provided by the contractual agreement with the customer.

9.2.1 Insurance Coverage

INCERT shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law, to cover liabilities arising from its operations and/or activities.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement.

9.3.1 Scope of Confidential Information

All information used by or transmitted to the PPKI1 shall be classified according the INCERT acceptable use of asset document.

As a minimum the following information shall be treated confidential:

- Audit records;
- Private keys;
- Private parts of the CPS if exist;
- Business continuity plan;
- Audit reports;
- Contractual agreement with INCERT; and
- Security controls.

9.3.2 Information Not Within the Scope of Confidential Information

Information in certificates, CRLs and other status information in the repository are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The PPKI1 and all PKI participants must ensure that confidential information be physically and/or logically protected from unauthorized viewing, modification, or deletion.

9.4 Privacy of Personal Information

This section relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this section addresses the following, to the extent pertinent under applicable law.

Specific instructions may be provided by the contractual agreement with the customer.

9.4.1 Privacy Plan

The PPKI1 gathers and processes personal information in compliance with the European General Data Protection Regulation.

9.4.2 Information Treated as Private

Personal information that is not publicly available through the content of the issued certificate, public certificate repository and CRLs are considered private.

9.4.3 Information not Deemed Private

Personal information that is publicly available through the content of the issued certificate, public certificate repository and CRLs are not considered private.

9.4.4 Responsibility to Protect Private Information

The PPKI1 and its participants shall take appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between PPKI1 system components and its participant.

9.4.5 Notice and Consent to use Private Information

The PPKI1 policy is to not disclose private personal information about its RA's Subscribers, customers, employees, and partners without their prior consent.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Some private information may be disclosed to be used as legal proof during a legal procedure or requisition of an authorized legal or administrative authority.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Only the private key is the sole property of the legitimate holder of the corresponding public key identified in a certificate and it may only be used for the purpose defined in the Terms and conditions agreement.

The PPKI1 retains all intellectual property rights in and to the CP, the certificates and revocation information that it issued.

Specific instructions may be provided by the contractual agreement with the customer.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The PPKI1 is in charge of:

- Validation and publication of this CPS, and respective CP;
- Conformance with the CP, procedures prescribed in its information security policy;
- Compliance with this CPS and respective CP.

9.6.2 RA Representations and Warranties

The RAs are in charge of:

- Authentication of the applicant;
- Verification needed for certificate delivery;
- Authentication of the certificate request;
- Authentication of the revocation request;
- Issuance and validation of the Terms and Conditions document;
- Compliance of its components with documents, regulation and standards described in section 8.4;
- Relation with the subscribers; and
- Communication with the subscribers.

9.6.3 Subscriber Representations and Warranties

Subscribers shall agree:

- The relevant parts of CP and CPS; and
- The Terms and Conditions.

The Terms and Conditions shall contain provisions imposing the following obligations and warranties:

- **Accuracy of Information** – An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the certificate(s) to be supplied by the CA;
- **Protection of Private Key** – An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- **Acceptance of Certificate** – An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- **Use of Certificate** – An obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms and Conditions;
- **Reporting and Revocation** – An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that:
    - Any information in the Certificate is, or becomes, incorrect or inaccurate, or
    - There is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the public key included in the Certificate;
- **Termination of Use of Certificate** – An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;
- **Responsiveness** – An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period; and
- **Acknowledgment and Acceptance** – An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties

Relying Parties using certificates from any CAs governed by the associated CP shall:

- Verify and adhere to by the usage for which the certificate has been issued;
- Verify the revocation status of the certificate; and
- Verify and adhere by obligations defined in the associated CP and in the Relying Party agreement.

9.6.5 Representations and Warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

Instructions may be described in the contractual agreement with the customer.

9.8 Limitations of Liability

INCERT shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under the regulation and standards described in section 8.4.

9.9 Indemnities

Instructions may be described in the contractual agreement with the customer.

9.10 Term and Termination

This section includes the time period in which this CPS or a related CP remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated.

9.10.1 Term

This CPS becomes effective from the date of creation of the Root CA and continues until terminated as provided in section 9.10.2.

9.10.2 Termination

Termination of this CPS will be upon publication of a newer version or a replacement document, or upon termination of CA operations. In any case it will be communicated by the PPKI1, on the repository.

9.10.3 Effect of Termination and Survival

End of validity of the present CP ends all the obligation and liability for the PPKI1.

9.11 Individual Notices and Communications with Participants

Individual notices and communication shall be performed via email except as otherwise set forth in the applicable agreement.

All notices and other communications which may or are required to be given, served or sent pursuant to the CPS shall be in writing and shall be sent, except provided explicitly in the CPS, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognized “overnight” or express courier service, (iii) hand delivery (iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or (v) an advanced electronic signature based on a

Certificate and a (secure) signature creation device ((S)SCD) and be addressed to INCERT using the contact details provided in chapter 1.5.1 from the present document.

9.12 Amendments

INCERT is the responsible authority for reviewing and approving changes to this CP. Written and signed comments on proposed changes must be directed to the Security and operations team manager as described in section 1.5.2. Decisions about proposed changes are at the sole discretion of INCERT.

9.12.1 Procedure for Amendment

INCERT shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be communicated to the PKI participants and subscribers. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

This CPS and any subsequent changes shall be made available to the PKI Participants within one week of approval. INCERT reserves the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the PKI Participants and other parties designated by INCERT shall provide their comments to INCERT in accordance with INCERT rules.

9.12.3 Circumstances Under Which OID Must be Changed

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties, as determined by INCERT, in its sole discretion or if a new version of this CPS is provided.

9.13 Dispute Resolution Provisions

PKI participants' agreements shall contain a conflict resolution clause to the extent permitted by applicable law.

The complaint management procedure details the procedure to follow for any dispute resolution associated with the present CPS.

9.14 Governing Law

The Laws of Grand-Duchy of Luxembourg governs the CP/CPS, according to all relevant European Directive that could apply.

9.15 Compliance with Applicable Law

The CP/CPS is subject to the applicable Laws of Grand-Duchy of Luxembourg.

9.16 Miscellaneous Provisions

This section contains miscellaneous provisions, sometimes called "boilerplate provisions" in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements.

INCERT acting as trust service operator, this CPS, the relevant CP, the Terms and conditions and any other relevant documents are in charge of the CA which is, in a real case, the customer.

9.16.1 Entire Agreement

The PPKI1 shall contractually obligate every RA involved in Certificate issuance to comply with this CP and applicable policies. The PPKI1 will also require parties using its products and services, such as Subscribers and Relying Parties, to accept agreements. No third party may rely on or bring action to enforce any such agreement.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CPS or any of its rights or duties under the associated CP, without the prior written consent of INCERT.

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The PPKI1 is not to be held responsible for any delay or failure in performance of its obligations if such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, an act of God, or other similar causes beyond its reasonable control, and without the fault or negligence of the delayed or non-performing party or of its subcontractors.

9.17 Other Provisions

9.17.1 Organizational

The parts of the PPKI1 concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

Detailed instructions may be described in the “Code of Ethics” document.

9.17.2 Additional testing

The PPKI1 should provide the capability to allow third parties to check and test all the certificates types that the PPKI1 issues.

Any test certificates should clearly indicate that they are for testing purposes by the subject name.

10 REFERENCES

Document A – RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

Document B – RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

Document C – RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013

Document D – eIDAS Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market

Document E – ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part1: General requirements V1.1.1, February 2016

Document F – ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for trust service providers issuing EU qualified certificates V2.1.1, February 2016

Document G – ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons V2.1.1, February 2016

Document H – ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements V2.1.1, February 2016

Document I – ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers V2.1.1, February 2016

Document J – INCERT_R OID management procedure V1.0, February 2017

Document K – INCERT_U PPKI1 Certificate Policy V1.1, **1.3.171.5.2.1.1.1.1**