THALES GLOBAL SERVICES
19-21 Avenue Morane Saulnier
78140 Vélizy-Villacoublay
France
Tel.: +33 (0) 1 40 83 23 00
www.thalesgroup.com

CERTIFICATION POLICY

THALES PKI

THALES GROUP OPEN

Identifiant Entité	Identifiant Document	DTC	Révision
9950-2598	0001-0031865479	541	001

Template: 87202584-DOC-GRP-FR-006

Follow-up of the evolutions

ENREGISTREMENT DES MODIFICATIONS			
Revision	**Date**	**Author**	**Modification**
001	24/01/2018	Erwan LE PALLEC	Document creation for Thales PKIv3
002			
003			

Approval				
	Name	**Role**	**Date**	**Signature**
Written by	Erwan LE PALLEC	RLDS PKI	02/02/2018	-
Reviewed by				
Approved by	Claude BODEL	Direction SSI Groupe	02/02/2018	-
Approved by customer if necessary	-	-	-	-

TABLE OF CONTENTS

1. INTRODUCTION

This Certificate Policy is based on the Internet Engineering Task Force (IETF) RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework”.

1.1 OVERVIEW

Thales owns and operates its own Root Certification Authority (RCA). Thales intends to operate several Certification Authorities (CA) based on this Certification Policy (CP) to facilitate interoperability at a technical level among Thales services, External Entities and/or Partner applications.

All CA managed by this CP are signed by the Root CA (RCA) owned by Thales.

Any use of this CP outside of the scope here above mentioned is entirely at the using party's risk. No Entity shall assert any OID listed in section 1.2 of this CP.

1.1.1 Certificate Policy

All X.509 Subscriber Certificates, i.e. all certificate issued by the Thales trust chain except for RCA and Intermediate CA, issued under this Certificate Policy must contain only one registered Certificate Policy Object Identifiers (OID), each of which is associated with a given assurance level as indicated in section 1.2 of this CP. The same Entity that is described by the OID also publishes the corresponding CP, and Relying Parties may use this CP to establish if a given Certificate satisfies their requirements for identity assurance.

Depending on the type of certificate issued by the “CA”, the “CA” certificate may contain the OID defined in this CP.

1.1.2 Relationship between this CP and the Thales domain CPS

This CP states what assurance can be placed in a Certificate issued under this policy. The associated Certification Practice Statement (CPS) states how the respective certification authorities establish that assurance.

1.1.3 Scope

Thales currently operates two 2-tiers trust chains:

- A current trust chain: this CA hierarchy is issued using 4096 bits RSA key pair and the SHA-256 algorithm;
- A legacy trust chain: this CA hierarchy is issued using 2048 bits RSA key pair and the SHA-1 algorithm.

The usage of the legacy trust chain is limited to specific cases where the current cryptographic standards (RSA 4096 bits key pair and SHA-256 algorithm) are not supported and obsolete cryptographic mechanisms must be used instead.

Both of the trust chains are composed of:

- One (1) non operational off-line root CA (Root CA v3 / Root CA v3 sha1);
- Three (3) operational on-line subordinate CAs:
  - Internal CA v3 / Internal CA v3 sha1: these CAs are dedicated to issue certificates for internal Thales physical subscribers (Thales employees), independently of the certificate usages;
  - External CA v3 / External CA v3 sha1: these CAs are dedicated to issue certificates for external physical subscribers (Thales contractors, partners, interns), independently of the certificate usages;
  - Devices CA v3 / Devices CA v3 sha1: these CAs are dedicated to issue certificates for non physical subscribers (devices, services), independently of the certificate usages.

This CP imposes requirements on:

- The Thales domain PKI; and
- Any CA signed by Thales legacy and current RCA (named RCA in this CP); and
- The Thales PKI shall only issue Certificates to:
  - Other CAs upon approval by the Thales PMA;
  - Trusted roles who operate the PKI, in strict measure with operational necessity;
  - Subscribers requiring certificates inside the Thales domain context (collaboration portals, messaging...).

The scope of this CP, in terms of Subscriber Certificate types is limited to those listed in Section 9.

1.2 DOCUMENT NAME AND IDENTIFICATION

The OID for this CP is the following:

- 1.2.250.1.108.1.3

1.3 PKI PARTICIPANTS

1.3.1 PKI Authorities

1.3.1.1 Policy Management Authority (PMA)

The PMA is the PKI lead authority and is managed by Thales.

The PMA is responsible for:

- Drafting and approval of this CP; and
- Drafting, compliance analysis, and approval of the CPS; and

- Accepting and processing applications from Entities desiring to certify a CA with an external Root CA; and
- Determining the mappings between Certificates issued by Thales domain PKI and the levels of assurance set forth in the CP (which will include objective and subjective evaluation of the respective CP contents and any other facts deemed relevant by the PMA); and
- Manage all the internal certificate request and revocation request in order to sign and revoke RCA and CA within THALES domain, and
- Ensuring continued conformance of the CPSs with applicable requirements as a condition for continued securing of the assurance levels as stipulated in this CP, and
- Ensuring continued conformance of this PKI and other domains' PKI with applicable requirements as a condition for allowing continued interoperability with certification provided by external Root CAs.

1.3.1.2 Root Certificate Authority (RCA)

RCA is owned by Thales.

A Root CA is a CA which is characterized by having itself as the issuer (that is, it is self-signed). Root CAs may not be revoked in the normal manner (they are not put on an Authority Revocation List), and, when used as a Trust Anchor, must be securely transmitted to any Relying Parties which choose to accept it as one by the mechanisms outlined in section 6.1.4.

The RCA operates its services according to this CP and the corresponding CPS. The RCA cannot start operation without prior approval of the PMA.

1.3.1.3 Intermediate Certificate Authority (ICA)

The Thales CA hierarchy is a two tiers hierarchy where signing CAs are directly subordinated to the RCA. Therefore, this is **not applicable** for this CP.

1.3.1.4 Signing Certificate Authority (CA)

CA is owned by entities designated by Thales.

A Signing CA is a CA which primary function is to issue Certificates to Subscribers. A Signing CA does not issue Certificates to other CAs. The CPS references all the Thales Signing CA.

The Signing CA operates its services according to this CP and the corresponding CPS. The Signing CA cannot start operation without prior approval of the PMA.

1.3.1.5 Certificate Status Authorities (CSA)

Thales does not actually implement an online revocation status mechanism (OCSP). Therefore, this is **not applicable** for this CP.

1.3.1.6 Registration Authority (RA)

RA is owned by entities designated by Thales.

The Registration Authority (RA) is the entity that collects and verifies each Subscriber's identity and information that are to be entered into his or her Public Key Certificate. An RA interacts with the CA to enter and approve the Subscriber Certificate request information and with TMA to personalize Subscriber's token.

PMA acts as the RA for the CAs. It performs its function in accordance with the concerned CPS approved by the PMA.

RA can delegate some operation to External Entity or Thales entity to act as Local RA (LRA) for all or few RA's operations to manage Subscriber certificate life cycle. In all cases, LRA perform operation according procedure defined by RA or by LRA and approved by RA. When LRA is a different legal person from Thales, then a contract is established between legal person of the RA and legal person of the LRA.

The RA and LRA operate their services according to this CP and the corresponding CPS. The RA and LRA cannot start operation without prior approval of the PMA.

1.3.2 Token Management Authority (TMA)

TMA is owned by Thales.

TMA is used to personalize Subscriber token and associated activation data.

TMA may be used by RA and LRA in order to manage the Subscriber's certificate stored on token only. When TMA is used to manage a set of certificates for Subscriber, then all life cycle of the certificate shall be managed using the TMA. Certificates contained in a token are linked in their life cycle to the life cycle of the token (for example all certificates in a token are revoked in same time).

The TMA operates its services according to this CP and the corresponding CPS. The TMA cannot start operation without prior approval of the PMA.

1.3.3 Key Escrow Authority (KEA)

The KEA is owned by Thales.

The KEA escrows Subscriber's encryption key pair.

The KEA operates its service according to this CP and the corresponding CPS. The KEA cannot start operation without prior approval of the PMA.

1.3.4 Key Recovery Authority (KRA)

The KRA is owned by Thales.

The KRA generates Subscriber's encryption key pair and proceed to the recovery of Subscriber's encryption key pair.

RA and Local Registration Authorities (LRA), if any, implement KRA role and procedures to support Subscriber recovery requests.

The KRA operates its service according to this CP and the corresponding CPS. The KRA cannot start operation without prior approval of the PMA.

1.3.5 Operational Authority (OA)

OA is owned by entity designated by Thales.

The Operational Authority (OA) is the entity that hosts and manages all the software, hardware and HSM used to support PKI services and PKI component of the present CP. The OA is the entity which sets up and realizes all operations for the PKI services. The CPS gives details on how each service is provided to each PKI component.

OA operates its services according to this CP and the corresponding CPS and its own security policy. OA cannot start operation without prior approval of the PMA.

1.3.6 Publication Service (PS)

PS is owned by Thales.

The Publication Service (PS) repository (refer to section **Erreur ! Source du renvoi introuvable.** below) which provides the following PKI services:

- Publication services (refer to section **Erreur ! Source du renvoi introuvable.** below).
- Log trail generation.

1.3.7 Subscribers

A Subscriber is the entity whose identity appears as the subject in a Certificate, who asserts that it uses its key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and who does not itself issue Certificates.

Subscribers are the following:

- Physical person: includes Thales employees, subcontractor personnel, suppliers, partners;
- Device: Device or service that uses a key pair and certificate for Thales or Thales's External Entity needs. When the Subscriber is a machine or a service, its key pairs and certificates are managed by a Technical Contact (TC).

1.3.8 Relying Parties

A Relying Party is the entity that relies on the validity of the binding between the Subscriber and a credential (in the context of a PKI, a Certificate and associated Public Key). The Relying Party is responsible for deciding how to check the validity of the Certificate by checking the appropriate Certificate status information (ARL and CRL). The Relying Party can use the Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the Certificate. A Relying Party may use information in the

Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.9 Other Participants

1.3.9.1 External Entity (Organization)

Not applicable. Thales does not provide any certificate or trust service to external entity.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Thales issues certificate for the following usages:

- Authentication:
  - Server/Service authentication (HTTPS, LDAPS, etc.);
  - Physical persons (employees, contractors, partners);
- Encryption: Encryption certificates are limited to physical persons (employees, contractors, partners) and are used to secure communication (email), file and disk encryption;
- Signing:
  - Code Signing (ActiveX, Java applet etc.);
  - Time stamping;
  - Physical persons (employees, contractor, partners) for digital signing, email signing.

The certificate signed by CA governed by this CP can only be used in the context of Thales.

1.4.2 Prohibited Certificate Uses

All the other usages are forbidden.

1.5 Policy Administration

1.5.1 Organization administering the document

The PMA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the PMA. Current contact details for the chair may be requested at: certificatemanagement@thalesgroup.com.

1.5.3 Person Determining Certificate Practice Statement Suitability for the Policy

The term CPS is defined in the [RFC 3647] as: "A statement of the practices, which a Certification Authority employs in issuing Certificates." It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of Certificate life-cycle management. It shall be more detailed than the corresponding Certificate Policy defined above.

A CPS may be approved as sufficient for fulfilling the obligations under this CP when such a CPS has been reviewed by an auditor or compliance analyst competent in the operations of a PKI, and when said person determines that the CPS is in fact in compliance with all aspects of this CP. The auditor or compliance analyst shall be from a firm which is independent from the entity being audited. Additionally, the auditor or compliance analyst may not be the author of the subject CPS.

The PMA shall approve the CPS, and shall furthermore make the determination whether a compliance analyst meets the requirements outlined herein.

1.5.4 CPS Approval Procedures

The PMA Charter shall outline the specific procedures necessary to approve the CPS.

1.5.5 Waivers

There is no waiver to this CP.

1.6 DEFINITIONS AND ACRONYMS

Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code…) that is used to perform cryptographic operations using a Private Key.
Assurance Level	A representation of how well a Relying Party can be certain of the identity binding between the Public Key and the individual whose subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the End-Entity whose subject name is cited in the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system which was used to produce the Certificate and (if appropriate) deliver the Private Key to the End-Entity performs its task.
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: • The identity of the issuing Certification Authority; • The identity of the certified End-Entity; • A Public Key that corresponds to a Private Key under the control of the certified End-Entity; • The Operational Period; • A serial number. The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or

	elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorized Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. Within this document, the term CP, when used without qualifier, refers to the Thales domain CP, as defined in section 1.
Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Certificate Request	A message sent from an applicant to a CA in order to apply for a digital Certificate. The Certificate request contains information identifying the applicant and the Public Key chosen by the applicant. The corresponding Private Key is not included in the request, but is used to digitally sign the entire request. If the request is successful, the CA will send back a Certificate that has been digitally signed with the CA's Private Key.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When an End-Entity chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Status Authority (CSA)	A CSA is an authority that provides status of Certificates or certification paths.
Common Criteria	Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine:

	• Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. • Whether the message has been altered since the transformation was made.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End-Entity within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Token	A hardware device that can hold Private Keys, digital Certificates, or other electronic information that can be used for authentication or authorization. Smartcards and Trusted Platform Module hardware chip are examples of hardware tokens.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the RCA and Signing CA keys.
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Issuing CA	In the context of a particular Certificate, the issuing Certification Authority is the Certification Authority that signed and issued the Certificate.
Key Generation	The process of creating a Private Key and Public Key pair.
Key Pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Local Registration	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is

Authority (LRA)	delegated certain tasks on behalf of a RA or CA).
Memorandum of Agreement	As used in the context of this CP, between Thales domain and an Entity PKI Domains legal Representation allowing interoperation between the respective Entity PCA and the Thales domain Bridge CA.
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.
PIN	Personal Identification Number. See activation data for definition.
PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Policy	This Certificate Policy.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.

Public/Private Key Pair	See Key Pair.
Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Relying Party (RP)	A person or Entity who has received information that includes a Certificate and a digital signature verifiable with reference to a public key listed in the Certificate, and is in a position to rely on them.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Software-based Certificate	A digital Certificate (and associated Private Keys) that are created and stored in software – either on a local workstation or on a server.
Sponsoring Organization	An organization with which an Authorized Subscriber is affiliated (e.g., as an employee, user of a service, business partner, External Entity etc.).
Subscriber Agreement	An agreement, entered into by a Subscriber that provides for the respective liabilities of the Entity PKI and of the Subscriber. Such agreement is a prerequisite in order to be able to use the Private Key associated to the Certificate.
Token	A hardware security device containing an End-Entity's Private Key(s) and Certificate. (Refer to "Hardware Token").
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not “valid” until it is both issued by a CA and has been accepted by the Subscriber.

2. PUBLICATION AND PKI REPOSITORY RESPONSIBILITIES

2.1 PKI REPOSITORIES

Operational Authority uses several methods for posting the artifacts (CRL, CA certificates, CP) that are required by this CP to an appropriate Repository. However, these mechanisms include as a minimum:

- Hypertext Transport Protocol (HTTP); and
- Availability of the information as required by the Certificate information posting and retrieval stipulations of this CP; and
- Access control mechanisms when needed to protect repository information as described in later sections.

The PKI Repositories containing Certificates and Certificate status information are deployed so as to provide 24 hours per day/365 day per year availability. This requirement does not apply to any PKI component other that the Repositories containing CA Certificates information.

2.2 PUBLICATION OF CERTIFICATE INFORMATION

2.2.1 Publication of CA Information

This CP is published electronically on the Thales web site at the following URL: http://crl.thalesgroup.com/certification_policy/.

The PS publishes any additional information concerning the CA which is necessary to support its use and operation.

The PS publishes any additional information concerning the PKI that is necessary to support its use and operation.

The PS publishes all CRLs and CA Certificates:

- Legacy CA certificates are available at the following URL: http://crl.thalesgroup.com/sha1;
- Legacy CRL are available at the following URL: http://crl.thalesgroup.com/sha1;
- Current CA certificates are available at the following URL: http://crl.thalesgroup.com;
- Current CRL are available at the following URL: http://crl.thalesgroup.com.

2.3 TIME OR FREQUENCY OF PUBLICATION

This CP defines the following frequencies of publication depending on the considered artefact:

- A new version of this CP is published within the next 48 hours following the CP validation by the PMA;
- Certificate Authority certificates are published within the next 48 hours following the Certificate Authority issuance;
- Authority Revocation List (ARL) are published within the next 24 hours following issuance;
- CRL (Certificate Revocation List) are published within the next 30 minutes following issuance.

2.4 ACCESS CONTROLS ON PKI REPOSITORIES

The OA is responsible for the security policy set granting access to the published information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

CAs shall ensure that all Certificates issued have a clearly distinguishable and non-null Distinguished Name (DN) in the Subject and Issuers fields and in accordance with RFC 5280. Certificates may include additional names via the subject alternative name (subjectAltName extension), provided it is marked noncritical, and is in accordance with the profiles in section 9.

3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CP are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates must identify the person or object to which they are assigned to in a meaningful way.

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscriber certificates must not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable Certificate profile. The authority responsible for Entity CA name space control is the RA or the LRA.

3.1.5 Uniqueness of Names

Name uniqueness is not enforced within Thales as long as certificates issued with the same name identify the same subscriber.

3.1.6 Recognition, Authentication and Role of Trademarks

Not applicable.

3.1.7 Name Claim Dispute Resolution Procedure

The PMA shall resolve any name claims or collisions that are brought to its attention, in a manner that ensures interoperability.

Entity RA or LRAs offering services to any organization outside of itself have a dispute resolution procedure to ensure prompt resolution of any claims of this type.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 RCA and CA

RCA and CA key pairs are generated, stored, activated, used and destroyed by the OA in a manner that the PMA is ensured that RCA and CA owns the private key corresponding to the public key contained in its RCA, and CA certificate.

3.2.1.2 Physical Subscriber

Physical subscribers' key pairs are generated (refer to section 6.1 below) and stored on board in tokens by the RA and transmitted (refer to section 0 below) to the Subscriber by the RA and LRA in a manner that guarantees that the Subscriber only owns private keys corresponding to the public keys contained in certificates.

Subscriber activation data (PIN) is securely delivered (refer to section 6.4 below) to the physical subscriber by the RA or LRA in a manner that guarantees that the physical person is the sole to have the control of its private key pair stored in the subscriber's token.

3.2.1.3 Other Type of Subscribers

Proof of the TC's possession of the private key is obtained through procedures to generate the private key (refer to section 6.1 below) that corresponds to the public key to be certified, and through the public key transmission method (refer to section 0 below).

3.2.2 Authentication of Organization Identity

Thales does not issue certificate for third party organization. Therefor this section is **not applicable**.

3.2.2.1 Organization Affiliation

Not applicable.

3.2.2.2 RCA and CA

Not applicable.

3.2.3 Authentication of Individual Identity

3.2.3.1 RCA and CA

Evidence of the individual identity of a person who; has a trusted role (refer to section 5.2 below), is authorized representatives or Witness is checked by the PMA and OA against a physical person during face to face meetings (refer to section **Erreur ! Source du renvoi introuvable.** below) or equivalent method, with that provides the same level of security assurance, authorized by PMA.

Evidence of the individual is verified by the PMA or the OA using the following rules:

- Verification of one (1) National Government-issued ID document that contains a picture of the individual.

- The identification process has to be done by a trusted operator in charge of security operation (refer to section **Erreur ! Source du renvoi introuvable.** below).

The unique identification numbers of the ID document presented by each individual part of the process is duly recorded.

3.2.3.2 Common to all assurance Levels for subscriber

A RA and LRA shall ensure that the applicant's identity information is verified and checked in accordance with the applicable CP and CPS. The RA or an LRA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the LRA or the RA shall record the process that was followed for issuance of each Certificate. Process information shall depend upon the Certificate level of assurance and shall be addressed in the applicable CPS.

LRAs and RAs are responsible for ensuring that they are in compliance with all applicable laws when collecting personally identifiable information. If a jurisdiction prohibits the collection, distribution or storage of any of the information specified in this section, an alternate, equivalent proofing mechanism may be used that insures the identity of the applicant to an equivalent level, subject to approval of the PMA.

The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identity verification.

3.2.3.3 Non physical Subscribers

This section applies to non physical subscribers, i.e. devices and services.

For this type of Certificates, the following information must be recorded:

- The full name, including surname and given name(s) of the applicant (Technical Contact or TC), and maiden name, if applicable; and
- The full name and legal status of the TC's Employer; and
- An email address for the applicant; and
- The date and time of the verification;
- Equipment identification or service name (e.g., DNS name) sufficient to unique identify the Subject; and
- Equipment Public Keys, if the private key is generated by the TC; and
- Equipment authorizations and attributes (if any are to be included in the Certificate).

TC is authenticated using means and procedures adapted to the role the individual is assigned to (refer to section **Erreur ! Source du renvoi introuvable.** below).

3.2.3.4 Physical Subscribers

The following information must be recorded:

- The full name, including surname and given name(s) of the Subscriber, and maiden name, if applicable; and
- The date and time of the verification.

In addition to the above, the applicant shall accordingly to the type of Subscriber:

- Present one (1) National Government-issued photo ID or two non-National Government IDs, one of which shall be a recent photo ID (e.g., Driver License) for Subscriber outside from Thales. If Subscriber is inside Thales, therefore internal badge and authentication procedure based on Human Resource (or IT like enterprise database) are sufficient; and/or
- Internal processes of External Entity approved by PMA. In this case, it is the External Entity's LRA authenticates the Subscriber according the procedure defined by the External Entity.

In all cases, LRA and RA verify ID and other information used to support the Subscriber registration process.

CPS gives details procedure to be respected according to the type of Subscriber.

Identity shall be established by in-person proofing before the RA or LRA; information provided shall be verified to ensure legitimacy.

3.2.4 Non-verified Subscriber Information

Information that has not been verified shall not be included in Certificates.

3.2.5 Validation of Authority

3.2.5.1 RCA and CA

The PMA appoints and authorizes the OA to generate RCA and CA certificates, under its control.

3.2.5.2 Subscriber

The authentication and identification of an authority of a Subscriber is done by the RA or LRA using and verifying information contained in the application.

3.2.6 Criteria for Interoperation

This CP covers Thales domain. Certificates delivered by PKI components are managed according to the rules and requirements stated by the PMA.

The RCA certificate is a self-signed certificate and is never signed by another CA (never certified by an external CA or never cross-certified with a CA).

CA cannot be:

- Cross-certified; and

- Signed by other external CAs.

Certificates delivered by PKI components of CA contained in RCA trusted domain are managed according to the rules and requirements stated by Thales only.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

3.3.1.1 RCA and CA

Same procedures as described in section 3.2 above apply.

3.3.1.2 Subscriber

Certificate re-key consists in renewing the key pair and assigning a new certificate in accordance with the same procedure as defined in section 3.2.
The previous key can be used for a new certificate only for devices as specified in the CPS.

3.3.2 Identification and Authentication for Re-key after Revocation

3.3.2.1 RCA and CA

Same procedures as described in section 3.2 above apply.

3.3.2.2 Subscriber

Certificate re-key after revocation consists in renewing the key pair and assigning a new certificate in accordance with the same procedure as defined in section 3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

3.4.1.1 RCA and CA

Same procedures as described in section 3.2 above apply.

3.4.1.2 Subscriber

Revocation requests shall be authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's associated Private Key, regardless of whether or not the Private Key has been compromised.

If the Private Key is not available, alternate authentication methods may be available. For Subscribers, the authentication can be done in face to face meeting with RA or LRA or by approved methods described in the appropriate CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Application

4.1.1.1 RCA and CA

The authorized representative of the RCA and CA shall submit the RCA and CA certificate request as directed by the PMA.

4.1.1.2 Subscriber

A Subscriber or Technical Contact may submit a certificate application to the RA or LRA.

A hierarchical manager of the Physical person (Professional, employee of entity) may submit a certificate request on behalf of a Subscriber to the RA or LRA.

A LRA may submit a certificate application on behalf of a Subscriber to the RA.

A RA may submit a certificate application on behalf of a Subscriber to the CA.

A TC may submit a certificate application to the RA or LRA.

A hierarchical manager of the TC may submit a certificate request on behalf of a TC to the RA or LRA.

4.1.2 Registration Process and Responsibilities

4.1.2.1 RCA and CA

RCA and CA certificates must be authorized by the PMA prior to issuance. The issuance process will require documenting the following information in the application request:

- Identity to set in the RCA and CA certificate (refer to section 3.1.1 above).
- Legal Entity which owns RCA and CA identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- CSR associated with the generated key pair (refer to section 6.1). The CSR shall be included in the application only for CA.
- Identity of the RCA to be used to sign the CA certificate.
- Validity period of the CA certificate.
- Cryptographic information of the RCA and CA certificates.
- RCA and CA Certificate content.
- Authorized representative information:

- The full name, including surname and given name(s) of the representative.
- The full name and legal status of the authorized representative's Employer.
- Professional phone number and email of the authorized representative.
- A place of business physical address or other suitable method of contact for the authorized representative.

The RCA and CA application shall be signed by the authorized representative. If the signature is electronic signature, then the PMA shall first authorize means to be used for electronic signature and validation of the electronic signature of the application.
The RCA and CA application has to be submitted in a due delay in order to be sure to have a new RCA and CA certificate and operational RCA's and CA's key pair before the expiration of the current RCA's private key (refer to section **Erreur ! Source du renvoi introuvable.** and **Erreur ! Source du renvoi introuvable.** below). The date of submission has also to take into account the time required for approval (refer to section **Erreur ! Source du renvoi introuvable.** below).

Associated to the CA certificate request, the authorized representative shall join its copy of a National Government-issued ID containing her/his picture. The PMA stores a copy of the authorized representative's ID along with the CA certificate request.

4.1.2.2 Physical Subscriber

There is no application form associated to the request of certificate for physical subscriber.

4.1.2.3 Other Type of Subscriber

The application form is signed by the Technical Contact and/or the authorized person (refer to section **Erreur ! Source du renvoi introuvable.**).
CPS gives the detailed procedure used for such application form.

4.1.3 Certificate Application Processing

4.1.3.1 RCA and CA

Requests are submitted by an authorized representative at the discretion of the PMA prior to issuance. It is the responsibility of the PMA to authenticate the authorized representative as described in section **Erreur ! Source du renvoi introuvable.** above, and to verify that the information in RCA and CA Certificate request is accurate for the RCA and CA.

4.1.3.2 Subscriber

It is the responsibility of the LRA, if it is the LRA that authenticates the Subscriber and TC, to verify that the information in Certificate request is accurate for a Subscriber.

It is the responsibility of the RA, if it is the RA that authenticates the Subscriber and TC, to verify that the information in Certificate request is accurate for a Subscriber.

4.1.4 Performing Identification and Authentication Functions

4.1.4.1 CA Certificates

RCA and CA certificate requests shall be submitted to the PMA by the authorized representative.

The PMA shall be responsible for approving or rejecting the RCA and CA certificate request.

Once a completed RCA, and/or CA certificate request has been submitted to the PMA, the PMA studies it. PMA cannot take decision based on an incomplete request. All required information listed in section 4.1.2 above shall be given to the PMA. The PMA shall evaluate the completeness of the submitted request.

In the case where the RCA and/or CA certificate request is complete and compliant with this CP statement, the PMA approves the RCA and/or CA certificate creation.

In the case where the RCA and/or CA certificate request is rejected, the PMA will ask to re-submit a new RCA and/or CA certificate request.

4.1.4.2 Subscriber Certificates

It is the responsibility of the RA and LRA to authenticate and verify that the information in the Certificate request is accurate for a Physical person (refer to section 3.2.2 and 3.2.5 above).

It is the responsibility of the RA and LRA to authenticate and verify that the information in the Certificate request is accurate for a Technical Contact (refer to section 3.2.2 and 3.2.5 above).

The Physical person face to face verification will be performed during the token delivery as explain in 4.3.

4.1.5 Approval or Rejection of Certificate Applications

4.1.5.1 RCA and CA

PMA may approve or reject a RCA and CA application.

4.1.5.2 Subscriber Certificate

LRA or RA may approve or reject a Subscriber Certificate application.

4.1.6 Time to Process Certificate Applications

4.1.6.1 RCA and CA

No stipulation.

4.1.6.2 Subscriber

The time to process the identification and authentication process of a Subscriber certificate application is defined by each RA and set in the Subscriber and TC agreement.

4.2 CERTIFICATE ISSUANCE

4.2.1 CA Actions during Certificate Issuance

4.2.1.1 RCA

The PMA transmits the RCA certificate request to the OA. The OA authenticates the certificate request before issuance. OA authenticates all key ceremony attendees (refer to section 3.2 above) using a list provided by an authorized representative (for witness) and the list of OA of the PKI.

The RCA certificate is generated during a key ceremony using a RCA key pair (refer to section 6.1.1 below). During the key ceremony, the RCA private key is backed-up (refer to section 6.2.4 below). At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9 below) and destroyed inside the HSM (refer to section 6.2.9 below) and only exist on backup format.

4.2.1.2 CA

The PMA shall transmit the CA certificate request to the OA. The OA shall authenticate the request prior to the generation of the CA certificate. Transmission of the certificate request and CSR shall be performed in a manner which ensures the integrity of the information. The OA authenticates all key ceremony attendees (refer to section 3.2 above) using a list provided by an authorized representative (for witness) and the list of OA of the PKI.

The following actions must occur during a CA certificate generation, which shall be witnessed at least by a PMA:

- Issuance of CA keys (refer to section 6.1.1 below).
- Backup of CA private key (refer to section 6.2.4 below).
- Generation of CA CSR (The CSR shall include the CA's public key, refer to section 6.1.1 below).
- RCA private key is activated to sign the CA certificate (refer to section 6.2.6, 6.2.7 and 6.2.8 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9 below. The RCA key is destroyed inside the HSM (refer to section 6.2.9 below) and only exist on backup format (refer to section 6.2.4 below).

4.2.1.3 Physical Subscriber

The tokens are personalized (refer to section 6.1.1 below) by the RA or LRA (using TMA). For encryption key pair, RA or LRA (using TMA) requests the KRA to generate encryption key pair (refer to section 6.1.1 below).

RA or LRA transmits public key to be certified to the CA contained in the certificate request (refer to section 6.1.3 below).

CA receives the certificate request from the RA.

CA authenticates the RA.

CA generates the certificate.

LRA or RA (using TMA) personalizes the token (refer to section 6.1.1 below) and delivers the token and activation data to the physical person (refer to section 6.1.2 and 6.4 below) during a face to face meeting (refer to section 3.2.3 above).

4.2.1.4 Non physical Subscriber

RA or LRA transmits the certificate request to the CA (refer to section 6.1.3 below).

CA receives the certificate request from the RA or LRA.

CA authenticates the RA or LRA.

CA generates the certificate.

The RA or LRA sends the certificate to the TC using the email of the TC.

4.2.2 Notification to Subscriber of Certificate Issuance

4.2.2.1 RCA and CA

Not applicable.

4.2.2.2 Physical Subscriber

The physical subscriber is not notified of the certificate issuance as the issuance is performed during a face to face with the RA or LRA.

4.2.2.3 Non physical Subscriber

Upon certificate issuance, the certificate is automatically sent by email to the Technical Contact associated with the certificate request.

4.3 CERTIFICATE ACCEPTANCE

4.3.1 Conduct Constituting Certificate Acceptance

4.3.1.1 RCA and CA

The PMA accepts the RCA and CA certificate when the PMA's representative that witnesses the RCA and CA signs the RCA and CA certificate issuance attestation.

Once the RCA and CA certificate has been accepted, the RCA and CA may start signing certificates and CRLs.

4.3.1.2 Subscriber

Regardless of the type of subscriber, the certificate is considered as accepted upon its first usage.

4.3.2 Publication of the Certificate by the CA

RCA and CA certificates are published by the PS (refer to section **Erreur ! Source du renvoi introuvable.** above).

4.3.3 Notification of Certificate Issuance by the CA to Other Entities

Notification of Certificate issuance is provided to other entity by publishing RCA and CA certificates (refer to section **Erreur ! Source du renvoi introuvable.** above).

4.4 KEY PAIR AND CERTIFICATE USAGE

4.4.1 Subscriber Private Key and Certificate Usage

Key pair and certificate usage are set forth in section **Erreur ! Source du renvoi introuvable.** above.

Usage of a key pair and the associated certificate is also indicated in the certificate itself, via extensions related to key pair usage (refer to section **Erreur ! Source du renvoi introuvable.** below).

4.4.2 Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained by the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of Subscriber certificates.

Relying parties have to be aware of the security rules to be deployed in the External Entity electronic transaction for the usage of a Subscriber certificate. A Subscriber certificate is used to identify, for example, the Subscriber as a physical person who sometimes belongs to an entity. Relying party has to check additional information (key usage, Policy OID ...) in order to accept and use the right Subscriber certificate in the electronic transaction. The relying party has to use all the required information in the certificate (DN as described in section 3.1.1 above, extensions ...) in order to be sure to accept the right Subscriber.

A Subscriber's certificate cannot be used without preliminary check from Relying party like for example trusted path validation, additional information only known from Subscriber and Relying party (in order to register the Subscriber's certificate) and External Entity information about Subscriber enrolment and use of signed document verifiable using Subscriber certificate.

4.5 CERTIFICATE RENEWAL

Renewing a Certificate (as detailed in [RFC 3647]) means creating a new Certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. Thales does not authorize certificate renewal and enforces certificate re-key (refer to section 4.7 below).

4.5.1 Circumstance for Certificate Renewal

4.5.1.1 RCA and CA

Not applicable.

4.5.1.2 Subscriber

Not applicable.

4.6 CERTIFICATE RE-KEY

The longer and the more often a key is used, the more susceptible it is to be lost or compromised. Therefore, it is important that a Subscriber periodically obtains new keys and reestablishes its identity. Re-keying a Certificate means that a new Certificate is created that has the same characteristics and level as the old one, except that the new Certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

4.6.1 Circumstance for Certificate Re-key

RCA and CA certificate re-key shall be processed when a key pair reaches the end of its life (refer to section **Erreur ! Source du renvoi introuvable.** below), the end of operational use, or when the private key is compromised or suspected of being compromised. A new key pair shall be generated in all cases.

A CA may issue a new Certificate to the Subject when the Subject has generated a new key pair and is entitled to a Certificate. The CA must only re-key when:

- The old private key of the same type corresponding to the public key in a Certificate issued to a Subscriber has reached the end of the lifetime period described in section 6.6;
- The subscriber certificate was revoked and a new one must be issued.

Same procedures as the ones applied for initial generation apply for a new RCA and CA certificate and associated key pair generation (refer to sections 4.1, 4.2, 4.3 and 4.4 above).

4.7 CERTIFICATE MODIFICATION

Updating a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that it differs in one or more other fields, from the old Certificate. For example, an Entity CA may choose to update a Certificate of a Subscriber whose characteristics have changed. The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, if an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or the trusted agent in order for an updated Certificate having the new name to be issued.

This practice is not allowed for RCA's, CAs' and Subscribers' certificates. In case a new certificate is created, a new key pair must be created.

4.8 CERTIFICATE REVOCATION AND SUSPENSION

4.8.1 Circumstance for Revocation of a Certificate

4.8.1.1 RCA

A RCA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The private key is suspected of being compromised.
- The private key is compromised.
- The RCA can be shown to have violated the stipulations of the present CP.
- End of RCA services.
- Privilege attributes asserted in the RCA certificate are reduced.
- Change in the key length size or algorithm recommendation coming from PMA or international standard institutes.

4.8.1.2 CA

A certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate the binding are:

- The RCA is revoked.
- The CA private key is suspected of being compromised or is compromised.
- The CA can be shown to have violated the stipulations of the present CP.
- End of the CA services.
- Privilege attributes asserted in the CA's certificate are reduced.
- Change in the key length size or algorithm recommendation coming from international standard institute.
- PMA obtains evidence that the CA Certificate was misused.
- PMA determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- The RCA or CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Subscriber or CA Certificate.
- The Issuing CA’s right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA’s Certificate Policy and/or Certification Practice Statement.

4.8.1.3 Subscriber

4.8.1.3.1 Physical subscriber

A certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Circumstances for physical subscriber that invalidate the binding are:

- The CA is revoked.
- Change in the key length size recommendation coming from national agencies or international standard institute.
- DN information filled incorrectly.
- The physical person failed to comply with the necessary obligations and security rules in the CP and CPS.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- Physical person stops to have the technical role for which she/he has had a certificate.
- Any other reasons indicated by PMA.

4.8.1.3.2 Non physical subscriber

A certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Circumstances for non physical subscriber (device, service) that invalidate the binding are:

- The CA is revoked.
- Change in the key length size recommendation coming from national agencies or international standard institute.
- DN information filled incorrectly.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The TC has used a wrong DN in his initial certificate request.
- The TC failed to comply with the necessary obligations and security rules in the CP and CPS.
- The server/service information included in the certificate is no longer consistent with the server/service's identity or the intended usage in the certificate (for example, modification of the FQDN or server name), before the certificate's scheduled expiration.
- The end of the service mentioned in the certificate.
- Any other reasons indicated by the PMA.

4.8.2 Who Can Request Revocation of a Certificate

4.8.2.1 RCA and CA

Only the PMA has the authority to request RCA and CA certificate revocation.

4.8.2.2 Subscriber

4.8.2.2.1 Physical subscriber

The physical subscriber can submit a revocation request in the following cases:

- The CA is revoked.
- DN information filled incorrectly.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The physical person has used a wrong DN in his initial certificate request.
- The cessation of the activity of the entity that the physical person belongs to.
- Physical person stops to have the technical role for which she/he has had a certificate.

The PMA can submit a certificate revocation request in the following cases:

- The CA is revoked.
- Change in the key length size recommendation coming from national agencies or international standard institute.
- DN information filled incorrectly.
- The physical person failed to comply with the necessary obligations and security rules in the CP and CPS.
- The private key corresponding to the certificate has been lost or compromised or suspected to be.
- The physical person has used a wrong DN in his initial certificate request.
- The physical person stops to have the technical role for which she/he has had a certificate.
- Any other cases indicated by PMA.

The RA or LRA can submit a certificate revocation request in the following cases:

- The CA is revoked.
- DN information filled incorrectly.
- The physical person failed to comply with the necessary obligations and security rules in the CP and CPS.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The physical person has used a wrong DN in his initial certificate request.
- The physical person stops to have the technical role for which she/he has had a certificate.

4.8.2.2.2 Non physical subscriber

The Technical Contact can submit a revocation request in the following cases:

- DN information filled incorrectly.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The TC has used a wrong DN in his initial certificate request.

- The server information included in the certificate is no longer consistent with the server's identity or the intended usage in the certificate (for example, modification of the FQDN or server name), before the certificate's scheduled expiration.
- The end of the service mentioned in the certificate.
- Subscriber stops to have the technical role for which she/he has had a certificate.
- Any other cases indicated by PMA.

The PMA can submit a certificate revocation request in the following cases:

- The CA is revoked.
- Change in the key length size recommendation coming from national agencies or international standard institute.
- DN information filled incorrectly.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The TC has used a wrong DN in his initial certificate request.
- The TC failed to comply with the necessary obligations and security rules in the CP and CPS;
- The server information included in the certificate is no longer consistent with the server's identity or the intended usage in the certificate (for example, modification of the FQDN or server name), before the certificate's scheduled expiration.
- The end of the service mentioned in the certificate.
- Subscriber stops to have the technical role for which she/he has had a certificate.

The RA or LRA can submit a certificate revocation request in the following cases:

- The Sub-CA is revoked.
- DN information filled incorrectly.
- The private key corresponding to the certificate has been lost or compromised or is suspected to be.
- The TC has used a wrong DN in his initial certificate request.
- The TC failed to comply with the necessary obligations and security rules in the CP and CPS.
- The server information included in the certificate is no longer consistent with the server's identity or the intended usage in the certificate (for example, modification of the FQDN or server name), before the certificate's scheduled expiration.
- The end of the service mentioned in the certificate.
- Subscriber stops to have the technical role for which she/he has had a certificate.

4.8.3 Procedure for Revocation Request

Revocation requests must be authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's associated Private Key, regardless of whether or not the private key has been compromised. If the Private Key is not available anymore, specific identification measures may be used, as described in section 1.4.

A request to revoke a Certificate must identify the Certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

4.8.3.1 RCA

Revocation of the RCA certificate requires revocation of all subordinated CA certificates (refer to section 4.9.3.2 below) it has issued.

The revocation of a RCA certificate requires the authorization of two (2) distinct individuals acting as permanent members of the PMA.

PMA can also decide in this particular case to destroy the RCA private key backup.

4.8.3.2 CA

Revocation of the CA certificate requires also revocation of all Subscriber certificates the CA has issued. The revocation of a CA certificate requires the authorization of two (2) distinct individuals acting as permanent members of the PMA.

CA revocation request is transmitted to the OA by the PMA. The OA authenticates the CA revocation request during a face to face meeting. OA authenticates all key ceremony attendee (refer to section 3.2 above) using list provided by authorized representative (for witness) and the list of OA of PKI trusted role.

The operation is video-recorded and performed according to a key ceremony script.

RCA key pair, according which has to be used for the revocation operation, is undertaken and witnessed in a physically secure environment (refer to section **Erreur ! Source du renvoi i ntrouvable.** below) by personnel in trusted roles (refer to section **Erreur ! Source du renvoi introuvable.** below) under at least dual supervision.

RCA key pair is carried out within a hardware security module (refer to section 6.2 and below). Witnesses are persons other than the operational personnel. RCA private key is activated to sign CRL (refer to section 6.2.6, 6.2.7 and 6.2.8 below).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9 below), RCA key is destroyed inside the HSM (refer to section 6.2.9.1 below) and only exist on backup format (refer to section 6.2.4 below).

The current RCA issued CRL (also called ARL) is replaced by the new one in the PS.

The PMA also requests to destroy the CA private key backup and CA key in HSM hosted by Thales's OA after all Subscriber certificate issued by CA has been revoked.

4.8.3.3 Subscriber certificate

Revocation requests are authenticated by the RA or LRA.

The revocation request is stored in the RA's logs.

The RA authenticates the revocation request it receives (refer to section 4.4 above).

The RA transmits the revocation request to the CA.

The CA authenticates the RA and makes sure the request was issued by an RA authorized by the CA.

The CA revokes the certificate by including the certificate's serial number in the next CRL to be issued by the CA.

4.8.4 Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

For Subscribers, revocation request processing time shall be within 24 hours.

4.8.5 Timeframe within which CA Must Process the Revocation Request

The CA shall process a revocation request as soon as possible after receiving the revocation request, not to exceed 48 hours.

4.8.6 Revocation Checking Requirements for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

The PMA shall provide Subscribers, Relying Parties, External Entity, partner and other third parties with clear instructions for reporting suspected RCA and CA Private Key Compromise, RCA, and CA Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

4.8.7 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of Certificate status information for off-line or remote (laptop) operation. PKI participants shall coordinate with the PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

The RCA that issue routine CRLs less frequently that the requirement for Emergency CRL issuance (i.e., CRL issuance for loss or compromise of key or for compromise of CA) shall meet the requirements specified above for issuing Emergency CRLs. CAs shall also be required to notify the PMA upon Emergency CRL issuance.

RCA issues CRL every thirteen months.

CA issues CRL at least every 24 hours.

CRL publication service availability is 24 out of 24 hours and 7 out of 7 days.

PS ensures that superseded CRLs are removed from the repository upon publication of the latest CRL.

4.8.8 Maximum Latency for CRLs

The maximum delay between the time a Subscriber Certificate revocation request is received by a CA and the time that this revocation information is available to Relying Parties shall be no greater than 4 hours.

Revocation entries on a CRL shall not be removed until after the expiration date of the revoked CA Certificate.

Thales maintain CRL, for RCA and CA, publication capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.8.9 Online Revocation Checking Availability

Not applicable.

4.8.10 Online Revocation Checking Requirements

Not applicable.

4.8.11 Other Forms of Revocation Advertisements Available

Thales does not support any other form of revocation advertisements. This section is not applicable.

4.8.12 Special Requirements Related to Key Compromise

Entities that are authorized to submit revocation requests are required to do so as quickly as possible after being informed of the compromise of the private key.

For RCA and CA Certificates, clear notification of revocation due to compromise of private key is published at a minimum on the PS website and possibly by other means (other institutional websites, newspapers …).

The general terms and conditions of use applicable to the Subscribers' certificates clearly state than in the event of the compromise of the private key or knowledge of the compromise of the private key of the CA that issued its certificate, the subscriber must immediately and permanently stop using his/her private key and the associated certificate.

Additional stipulations are defined beyond section 5.7 and 5.8.

4.8.13 Circumstances for Suspension

Not applicable.

4.8.14 Who can Request Suspension

Not applicable.

4.8.15 Procedure for Suspension Request

Not applicable.

4.8.16 Limits on Suspension Period

Not applicable.

4.9 CERTIFICATE STATUS SERVICES

4.9.1 Operational Characteristics

CRL and ARL are only available through HTTP at the following URLs:

- http://crl.thalesgroup.com/sha1 for legacy CAs;
- http://crl.thalesgroup.com for current CAs;

This certificate status service is hosted internally, available internally to Thales but also externally (accessible from the Internet) to third parties.

ARL (RCA's CRL) is published every 12 months;

CRL are published every 4 hours.

Thales does not implement any other certificate status service (OCSP, LDAP).

4.9.2 Service Availability

The HTTP ARL and CRL publication service is available 24 hours per days, 7 days a week.

4.9.3 Optional Features

No optional feature.

4.10 END OF SUBSCRIPTION

Certificates that have expired prior to or upon end of subscription are not required to be revoked. Unexpired CA Certificates shall always be immediately revoked at the end of subscription.

4.10.1 Key Escrow and Recovery

Under no circumstances shall a RCA and CA key be escrowed by a third-party.

4.10.1.1 Which key pair can be escrowed

Under no circumstances signature and authentication keys can be escrowed.

Only encryption keys for physical subscriber are escrowed by PKI.

KRA generates the Subscriber's key pair for encryption certificate and escrows it. The Subscriber's key pair is ciphered by the KEA.

Encryption key pairs are generated by KRA (refer to section **Erreur ! Source du renvoi introuvable.** b elow) and automatically escrowed by KEA.

4.10.1.2 Who Can Submit a Recovery Application

When recovering a certificate is necessary, a recovery request must be addressed to the PMA. In all cases, without distinction of Subscriber, only the PMA is allowed to request the recovery of encryption key to the KRA for the following reasons:

- Legal request;
- Business continuity;
- Thales' security.

4.10.1.3 Recovery Process and Responsibilities

The recovery process addressed to the PMA is based on a digitally signed email that contains at a minimum the following information:

- The full name, including surname and given name(s) of the Subscriber, and maiden name, if applicable for which the encryption certificate must be recovered; and
- Email address of the subscriber for which the encryption certificate must be recovered; and
- A description of the reason why the encryption certificate must be recovered; and
- The date and time of the request.

The PMA registers the recovery request. Encryption certificate can only be recovered as software certificate. Encryption certificate are never recovered on token.

4.10.1.4 Performing Identification and Authentication

It is the responsibility of the PMA to authenticate and verify that the information in the recovery request is accurate.

The identification and authentication are performed through the email digital signature.

4.10.1.5 Approval or Rejection of Recovery Applications

The PMA verifies that:

- The email digital signature is valid, i.e., the requester is identified and authenticated;
- The request is complete and complies with the recovery request reasons detailed section 4.11.1.2;

Based on the verification performed above, the PMA:

- Approve the recovery request and and transmits it to the KRA;
- Reject the request and notify the requester by email of the rejection.

4.10.1.6 KEA and KRA Actions during key pair recovery

PMA transmits key recovery request to the KRA.

KRA receives recovery request from the PMA.

KRA authenticates the PMA.

KRA recovers key pair.

KRA transmits the encryption certificate along with the associated private key as a PKCS#12 along with a password to the PMA.

4.10.1.7 KEA and KRA Availability

KEA and KRA are available 24 hours a day, 7 days a week.

4.10.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location & Construction

The location and construction of the facility housing RCA, CA, RA, KRA, KEA, PS and TMA (means for software and HSM used for RCA, CA, RA, KRA, KEA, PS and TMA) equipment are 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, provide robust protection against unauthorized access to the RCA, RA, KRA, KEA, PS and TMA equipment and records.

5.1.2 Physical Access

5.1.2.1 RCA

The location and construction of the facility of the OA housing RCA equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) are consistent with facilities used to house high value and sensitive information. RCA is operated in a dedicated physical area separated from other PKI component physical area.

The OA has implemented policies and procedures to ensure that the physical environment, in which the RCA equipment is installed, maintains a high level of security that guarantees that:

- It is isolated from outside networks.
- It is separated into a series of progressively secure physical perimeters.
- The entrances and exits from the secure physical areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.
- Sensitive data (HSM, key pair backup, activation data …) are stored in dedicated safe located in dedicated physical area under control of trusted role only.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include:

- Perimeter alarms, closed circuit television, reinforced walls and motion detectors.
- Strong authentication to go in and out in the RCA and safe physical secured area.

OA uses human to continually monitor the OA facility housing equipment on a 7x24x365 basis. The OA facility is never left unattended.

5.1.2.2 CA, KEA, KRA, RA and PS

The location and construction of the facility of the OA housing CA, KEA, KRA, RA and PS equipment and data (log, archive, HSM, server, network security component …) are consistent with facilities used to house high value and sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors, provide robust protection against unauthorized access to equipment and records.

OA are located in country approved by PMA.

The OA implements policies and procedures to ensure that the physical environments, in which CA, KEA, KRA, RA and PS equipment are installed, maintains a high level of security that guarantees that:

- It is separated into a series of progressively secure physical perimeter.
- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.
- Strong authentication to go in and out in the CA, KEA, KRA, RA and PS physical secured area.
- CA, KEA, KRA, RA and PS equipment and data (server, HSM, log, archive …) are stored in cabinet in area under control of trusted role only.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include:

- Perimeter alarms, closed circuit television, reinforced walls and motion detectors.
- Two-factor authentication using Biometrics and badge.
- All the networking and systems components are installed in cabinets in secure area.

OA uses human to continually monitor the OA facility housing equipment on a 7x24x365 basis. The OA facility is never left unattended.

5.1.3 Power and Air Conditioning

OA have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories are provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Water Exposures

The OA ensures that systems are protected in a way that minimizes impact from water exposure consequences.

5.1.5 Fire Prevention & Protection

The OA ensures that systems are protected with fire detection and suppression systems.

5.1.6 Media Storage

RCA, CA, KEA, KRA, RA and PS media are stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit archive, or backup information are duplicated and the duplicates are stored in a location separated from the OA location.

5.1.7 Waste Disposal

Sensitive waste material are disposed-off in a secure fashion. All media used for the storage of sensitive information such as keys, activation data or files are destroyed before released for disposal.

5.1.8 Off-Site backup

Full back-ups of PKI component, sufficient to recover from system failure, are made after PKI deployment and after each new key pair generation. Back-up copies of essential business information (key pair and CRL) and software are taken regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of the OA business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery OA). The back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the PKI service.

PMA shall ensure that OA's roles are defined in order to operate the following set of trusted functions in support of the PKI services (deployed by Thales only) with an appropriate separation of duties:

- Security operation: Owns overall responsibility for managing the implementation of policy practices and CP and defines all the PKI roles and appoints physical person to trusted role.
- PKI system operation: Cleared to install, configure, back-up, recover and maintain PKI systems (off-line and on-line).
- Key management operation: Manages all HSM of the PKI (on-line) and performs key ceremonies (off-line and on-line).
- Audit operation: Authorized to view archives and audit logs produced during the usage and management of the PKI systems (on-line).
- HSM activation: Cleared to hold activation data which are necessary for hardware security module operation (off-line and on-line).
- Key pair protection: Cleared to hold activation data that are necessary for CA private key management (role different from the HSM activation role).
- On-line PKI Software administration: manage technical roles of the PKI software and configuration of the PKI software.
- On-line PKI software operation: uses the PKI software functionality in order to manage Subscriber's certificate life cycle.

5.2.2 Number of Persons Required per Task

Three or more persons are required to perform the following tasks:

RCA and CA Signing key generation; or

RCA and CA Signing key activation; or

RCA and CA Signing key backup.

Multiparty control must not be achieved using personnel that serve in the Auditor Role.

All roles are granted to multiple persons in order to support continuity of operations.

5.2.3 Identification and Authentication for Each Role

An individual must identify and authenticate herself/himself before being permitted to perform any actions set forth above for that role or identity.

All Trusted Roles who operate a PKI component are allowed access only when authenticated using a method of strong authentication. Physical person in trusted role uses a certificate for PKI software component issued like as a physical Subscriber. Machine of PKI component are secured with a certificate issued like Device Subscriber.

5.2.4 Roles Requiring Separation of Duties

The number of persons who provide PKI services is detailed in the CPS. The number of persons is defined to guarantee trust for all services (key generation, certificate generation, revocation, certificate request …), so that no malicious activity may be conducted by a single person acting on behalf of the PKI. All participants must serve in a trusted role as defined in section **Erreur ! Source du renvoi introuvable.** above.

RCA and CA keys are under dual control at minimum.

The following tasks must be completed by two persons authorized for PKI system operations:

- key generation
- key activation
- key backup
- CA certificate revocation.

It is forbidden to own more than one privilege (role) for the following operations at the same time:

- An individual owning a role in PKI system operation must not be involved in any other operation.
- An individual owning a role in security operation must not be involved in any other operation except HSM activation and Key pair protection (only if dual control is respected).
- An individual owning a role in key management operation must not be involved in any other operation except HSM activation and Key pair operation (only if dual control is respected).
- An individual owning a role in audit (only for internal and External Entity audit) operation must not be involved in any other operation except security operation. This rule doesn't apply to any kind of external auditor which can't have any role in the PKI.
- An individual owning a role in an off-line PKI Software administration must not be involved in on-line PKI software operations.
- An individual owning a role in HSM activation may be involved in key pair protection if and only if she/he cannot control key pair alone.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

A group of individuals responsible and accountable for the operation of each PKI component is identified. The trusted roles of these individuals must be identified.

All persons filling trusted roles must be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation. Personnel appointed to trusted roles shall:

- Have successfully completed an appropriate training program; and
- Have demonstrated the ability to perform their duties; and
- Be trustworthy; and
- Have no other duties that would interfere or conflict with their duties for the trusted role; and
- Have not been previously relieved of duties for reasons of negligence or non-performance of duties; and
- Have not been denied a security clearance, or had a security clearance revoked for cause; and
- Have not been convicted of a serious criminal offense; and
- Be appointed by an approving authority.

5.3.2 Background Check Procedures

All persons filling trusted roles shall have completed a background investigation as allowed by applicable national law or regulation.

Adjudication of the background investigation shall be performed in accordance with the requirements of the appropriate national adjudication authority.

The results of these checks shall not be released except as required in sections 8.3 and 8.4.

Background check procedures are described in the CPS.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of PKI shall receive comprehensive training.

Training shall be conducted in the following areas:

- PKI component security principles and mechanisms; and
- All PKI software versions in use on the PKI system; and
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations 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 responsible PMA shall ensure appropriate administrative and disciplinary actions are taken against personnel who violate this policy.

5.3.7 Independent Contractor Requirements

Sub-Contractor personnel employed to perform functions pertaining to PKI operations shall meet applicable requirements set forth in this CP.

5.3.8 Documentation Supplied to Personnel

The PKI component shall make available to its personnel the Certificate Policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the PKI component. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. All security audit logs, both electronic and non-

electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section are maintained.

5.4.1 Types of Events Recorded

All security auditing capabilities of the PKI operating system and the PKI services required by this CP are enabled. As a result, most of the events identified in the table are automatically recorded. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event; and
- The date and time the event occurred; and
- Success or failure where appropriate; and
- The identity of the entity and/or operator that caused the event; and
- A message from any source requesting an action by a PKI component is an auditable event.
- The message must include message date and time, source, destination and contents.

The CPS gives details on what is logged. Logging should address, at minimum, the following topics:

- Physical facility access.
- Trusted roles management.
- Logical access.
- Backup management.
- Log management.
- Certificate creation.
- Certificate revocation.
- Key creation, using or destruction.
- Key recovery operation.
- Activation data management.
- Roles management.
- IT and network management.
- PKI documentation management.
- Security management.

LRA has to log the following operation and data:

- Certificate application form.
- Revocation application form.

- Other forms used in the LRA management (roles management…).

5.4.2 Frequency of Processing Audit Logs

PKI operation audit logs shall be reviewed on an annual basis by the member of the OA responsible for audits, who conducts a reasonable search for any evidence of malicious activity, and following each important operation.

A statistically significant sample of security audit data generated by their PKI business entity since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. OA review log on day to day basis for IT and physical security.

The OA shall explain all significant events in log audit report. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Records related to PKI operation are held on the OA site for at least one year before being archived.

5.4.4 Protection of Audit Logs

Event logs are protected in such a way that only authorized users can access them.

Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Event logs are protected in such a way so as to remain readable for the duration of their storage period.

5.4.5 Audit logs are not modified

Audit logs and audit summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Audit log backups are protected with the same level of trust defined for the original logs.

5.4.6 Audit Log Backup Procedures

Audit logs and audit summaries are backed up at least once every 30 days. A copy of the audit log is sent off-site every 30 days in accordance with a process to be described in the CPS.

5.4.7 Audit Collection System (internal vs. external)

Audit processes are invoked at system start up, and end only at system shutdown. The audit collection system maintains the integrity and availability of all data collected and protects the integrity of the data. If a problem appears during the process of the audit collection system, the PMA determines whether it has to suspend operations until the problem is solved and inform the impacted component.

5.4.8 Notification to Event-Causing Subject

When an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.9 Vulnerability Assessments

Auditor and PKI system operators explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

5.4.10 Real time monitoring and notification

The PKI system integrated an automatic notification system covering every aspects of the certificates lifecycle.

OA monitors the PKI system in real time.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

PKI components archive records are sufficiently detailed to establish the proper operation of the component or the validity of any Certificate (including those revoked or expired) and key pair managed by PKI component.

Archived Data:

- Certification Practice Statement;
- Contractual obligations;
- System and equipment configuration;
- Modifications and updates to system or configuration;
- Certificate requests;
- Revocation requests;
- Recovery request;
- Subscriber identity authentication data;
- All Certificates issued or published;
- All CRLs and ARLs issued and/or published;
- All Audit Logs;
- Other data or applications to verify archive contents;
- Documentation required by compliance auditors.

5.5.2 Retention Period for Archive

The retention period for archive data depends on the legal and business requirements and is set forth in the respective CPS. However, the archive data is kept for a minimum retention period of ten (10) years except for the subscriber enrollment details that are kept only during the lifetime of the subscriber's certificate.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

Applications required to process the archive data shall also be maintained for the minimum retention period specified above.

The archive of the revocation data can be omitted when archived logs contains the information needed to track these events.

5.5.3 Protection of Archive

No unauthorized user are permitted to write, modify, or delete the archive. The contents of the archive are not to be released except as determined by the PMA or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media are stored in a safe, secure storage facility separate from the PKI component with physical and procedural security controls equivalent or better than those required for the component.

5.5.4 Archive Backup Procedures

The CPS describes how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for Time-Stamping of Records

PKI archive records have a trusted time as they are created as defined in section 6.8 below.

5.5.6 Archive Collection System (internal or external)

The archive collection system is compliant with security requirements defined in section 5.4.6.

5.5.7 Procedures to Obtain & Verify Archive Information

Procedures detailing how to create, verify, package, and transmit archive information is detailed in the applicable CPS.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a RCA and CA's private key, that key may be changed; from that time on, only the new key must be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key must be retained and protected.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If an OA detects a potential hacking attempt or other form of compromising, it shall perform an investigation in order to determine the nature and the degree of damage. If the PKI component key is suspected of compromise, the procedures outlined in section 5.7.3 must be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the PKI component needs to be rebuilt, only some Certificates need to be revoked, and/or the PKI component key needs to be declared compromised.

The above measures will allow member Entities to protect their interests as Relying Parties.

An Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the respective CPS.

The OA must have a documented incident handling procedure that is approved by the head of the organization responsible for operating the PKI. If the PKI component is compromised, all Certificates issued to the Subscriber must be revoked, if applicable. The damage caused by the compromised PKI component must be assessed and all Subscriber Certificates that may have been compromised must be revoked, and Subscribers shall be notified of such revocation. The PKI component shall be re-established.

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

If a PKI component equipment is damaged or rendered inoperative, but the CA keys are not destroyed; the operation shall be reestablished as quickly as possible, giving priority to the ability to generate Certificate status information, i.e. CRL.

If a RCA and/or CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs and/or Subscriber that have been issued Certificates shall be securely notified immediately.

The RCA and/or CA shall reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If revocation capability cannot be established in a reasonable time-frame, the RCA and/or CA shall determine whether to request revocation of its Certificate(s). If the CA is a Root CA, the CA shall determine whether to notify all subscribers that use the CA as a trust anchor to delete the trust anchor.

5.7.3 Private Key Compromise Procedures

If a RCA and/or CA signing keys are compromised, lost, or suspected to be compromised:

- A RCA and/or CA key pair shall be generated by the RCA and/or CA in accordance with procedures set forth in the applicable CPS; and
- New RCA and/or CA Certificates shall be requested in accordance with the initial registration process set elsewhere in this CP; and
- If the RCA and/or CA can obtain accurate information on the Certificates it has issued and that are still valid (i.e., not expired or revoked), the RCA and/or CA may re-issue (i.e., renew) those Certificates with the notAfter date in the Certificate as in original Certificates; and
- If the CA is the Root CA, it shall provide the Subscribers the new trust anchor using secure means.

The PMA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

If a TMA or KEA key is compromised, all Certificates issued with the TMA or KEA shall be revoked, if applicable. The TMA or KEA will generate a new key pair and request new Certificate(s), if applicable.

If a trusted role keys are compromised, lost, or suspected to be compromised:

- The trusted role certificate shall be immediately revoked; and
- A new trusted role key pair shall be generated in accordance with procedures set forth in the applicable CPS; and
- New trusted role certificate shall be requested in accordance with the initial registration process set elsewhere in this CP; and
- All Certificate registration or recovery requests approved by the trusted role since the date of the suspected compromise shall be reviewed to determine which one are legitimate; and
- For those Certificates or recovery requests or approval than cannot be ascertained as legitimate, the resultant Certificates shall be revoked and their subjects (i.e., subscribers) shall be notified of revocation.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a PKI component installation is physically damaged and all copies of the PKI component Key are destroyed as a result, the CA shall request that its Certificates be revoked. The CA shall follow the steps outlined in section 5.7.3 above.

5.8 PKI COMPONENT TERMINATION

5.8.1 RCA

In the event of the termination of the RCA service provided by a RCA, the PMA provides notice prior to the termination, and:

- Revoke all CA certificates under the RCA.
- Destroys the RCA private key.
- Communicate last revocation status information (CRL signed by RCA) to the relying party indicating clearly that it is the latest revocation information.
- CA stops delivering certificates according to and referring to this CP. But CA can deliver certificate using its own CA certificate signed by itself or by another CA in order to validate certificate and CRL.
- In case of compromising RCA, PMA and OA both use secure means to notify External Entity to delete all trust anchors representing RCA with the compromised(s) key pair(s).
- PMA alerts and notifies relying party and External Entity providers to delete all trust anchors.
- Archives all audit logs and other records prior to termination of the PKI.
- Archived records are transferred to an appropriate authority.

The PMA may take appropriate measures and reasonable effort to transfer RCA records to an entity appointed by PMA.

5.8.2 CA

In the event of the termination of the CA service, the PMA provides notice prior to the termination, and:

- Inform External Entity.
- Destroys the CA private key.
- Publishes the most recent revocation status information (CRL signed by the CA) to all Relying parties (if any).
- The CA signed by the RCA stops delivering certificates in accordance with its CP.
- In the case of a compromised CA, the PMA and OA both use secure means to notify Subscribers and relying parties that they must delete all trust certificates representing the CA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to the PMA.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the PMA

5.8.3 Other PKI components

All other PKI components must archive all audit logs and other records prior to termination.

All other PKI components must destroy all their private keys upon termination.

All PKI components archive records must be transferred to an appropriate authority such as the PMA responsible for the entity.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 RCA

After the PMA agrees to the generation of the RCA, a key pair and RCA certificate are generated for the RCA.

The operation of the RCA key pair and RCA certificate generation is video-recorded and performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

RCA key pair generation is undertaken and witnessed in a physically secure environment (refer to section **Erreur ! Source du renvoi introuvable.**.1 and 5.1.2 above) by personnel in trusted roles (refer to section **Erreur ! Source du renvoi introuvable.** above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. RCA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than operational personnel who perform the key ceremony. As trusted role, witness can only have “HSM activation” and “Key pair protection”. RCA activation and initialization is under the control of RCA activation data holders. During the key ceremony, the RCA key pair is backed up (refer to section 6.2. below).

The key pair and certificate generation process creates a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure is detailed enough to show that appropriate role separation was used. An independent third party shall validate the process.

6.1.1.2 CA

After the PMA agrees to the generation of the CA, a key pair and CSR are generated for the CA.

The operation of the CA key pair and CSR generation is performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

CA key pair generation is undertaken and witnessed in a physically secure environment (refer to section **Erreur ! Source du renvoi introuvable.**.1 and 5.1.2 above) by personnel in trusted roles (refer to section **Erreur ! Source du renvoi introuvable.** above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. CA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than the operational personnel who perform the key ceremony. As trusted role, witness can only have “HSM activation” and “Key pair protection”. CA activation and initialization is under the control of CA activation data holders. During the key ceremony, the CA key pair is backed up (refer to section 6.2. below).

The key pair and CSR generation process creates a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure is detailed enough to show that appropriate role separation was used.

6.1.1.3 Subscriber

6.1.1.3.1 Physical subscriber

Token certificate and key pair is personalized by the RA or LRA using TMA.

Software certificate and key pair are personalized by the RA or LRA.

RA or LRA generates private keys for the certificate for a physical person. The generation is performed directly on the token of the physical person, to avoid compromising the private key and associated activation data. The private key is protected with the associated activation data.

KRA generates the encryption key pair of the physical person. The generation is performed using a HSM, to avoid compromising of the private key along with the associated activation data. The private key is protected with the associated activation data. After key pair generation, the KEA escrows the key pair.

6.1.1.3.2 Non physical subscriber

The TC generates the non physical subscriber (devices and services) key pairs to ensure to be the sole to have the control of the private key. In this case the TC is responsible of the protection and confidentiality of the private key.

6.1.2 Private Key Delivery to Subscriber

6.1.2.1.1 Physical subscriber

KRA transmits securely the encryption key pair to the TMA, protected by the activation data also generated by KRA. TMA uses the activation data to put the encryption key pair in the token. Signature and authentication keys being generated in the token, they are already inside the token (refer to section 6.1.1 above).

The private key is delivered securely to the physical person. Private key is delivered stored in the token protected by the activation data of the physical person (refer to section 6.4 below) and the following requirements are met:

- TMA who import the private key on the token does not retain any copy of the key after integrating the key; and
- The private key is protected from activation, compromise, or modification during the delivery process.

The delivery process ensures that the correct tokens and activation data are provided to the correct physical subscriber. Accountability for the location and state of the module is maintained until the physical person accepts possession of it.

The RA and LRA shall maintain a record of the delivery of the token to the physical subscriber.

6.1.2.1.2 Non physical subscriber

This section is only be applicable when the CA issued the key pair.

CA transmits securely the key pair to RA or LRA protected by an activation data also generated by CA or provided by TC.

The private key is delivered securely to the TC, protected in activation generated by the CA or provided by the TC and the following requirements are met:

- The RA and LRA who transmits a private key for a non physical subscriber does not retain any copy of the key after delivery of the private key to TC; and
- The private key is protected from activation, compromise, or modification during the delivery process.

The delivery process is accomplished in a way that ensures that the correct key pair and activation data are provided to the correct TC.

The RA and LRA maintain a record of the delivery of the token to the TC.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 RCA and CA

For RCA, the delivery of RCA public key is done during the key ceremony.

For CA, public keys is delivered securely to the relevant Root CA for certificate issuance during key ceremonies or during the registration process (refer to section 4.1 and 4.2 above). The delivery mechanism binds CA checked identities to the public keys to be certified using PKCS#10 format.

6.1.3.2 Subscriber

When the Subscriber, TC or RA or LRA generates Key Pairs, the Public Key is delivered securely to the CA for Certificate issuance through a PKCS#10. The delivery mechanism binds the subscriber's verified identity to the Public Key.

6.1.4 CA Public Key Delivery to Relying Parties

The Public Key of a trust anchor shall be provided to the Subscribers acting as Relying Parties in a secure manner so that the trust anchor is not vulnerable to modification or substitution. Acceptable methods for delivery of trust anchor include but are not limited to:

- The CA loading a trust anchor onto tokens delivered to Subscribers via secure mechanisms; or
- Secure distribution of a trust anchor through secure out-of-band mechanisms; or
- Comparison of Certificate hash (fingerprint) against trust anchor hash made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the Certificate are not acceptable as an authentication mechanism); or
- Loading trust anchor from web sites secured with a currently valid Certificate of equal or greater Assurance Level than the Certificate being downloaded and the trust anchor is not in the certification chain for the Web site Certificate.

6.1.5 Key Sizes

Legacy Certificate Authorities (RCA and CAs) use 2048 bits RSA key and sign certificates and CRL using the SHA-1 algorithm (sha1withrsa).

Current Certificate Authorities (RCA and CAs) use 4096 bits RSA key and sign certificates and CRL using the SHA-256 algorithm (sha256withrsa).

Certificates issued by the Thales legacy trust chain may use 1024 bits RSA key but 2048 bits RSA key are preferred whenever possible.

Certificate issued by the current trust chain must use at minimum 2048 bits RSA key, not exceeding the size of the issuing CA key.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters are generated and checked in accordance with the standard that defines the crypto-algorithm for the parameters that are to be used.

RCA CA keys are generated in accordance with the cryptography tools of the hardware security modules (refer to section 6.2.1 below). Random numbers for keys RCA and CA are generated in FIPS 140-2 Level 3 or Common Criteria EAL 4+ validated hardware cryptographic modules (refer to section 6.2 below).

Subscriber, when it uses a token, has its key generated in accordance with the cryptography tools of the hardware security modules (refer to section 6.2.1 below).

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

The use of a specific key is determined by the keyUsage extension in the X.509 Certificate. The Certificate Profiles in section 9 specify the allowable values for this extension for different types of Certificates defined under this CP, and all CAs issuing Certificates in accordance with this CP must adhere to those values.

Public keys that are bound into Certificates shall be certified for use in signing or encrypting, but not both. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management Certificates and require setting both digitalSignature and keyEncipherment bits to be set.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Relevant standards for cryptographic modules are FIPS PUB 140-2 and Common Criteria. The PMA may determine that other, comparable, validation, certification, or verification standards are sufficient. Such standards, once approved will be published by the PMA. Cryptographic modules shall be validated to the FIPS 140-2 level 3 or Common Criteria EAL4+ identified in this section, or validated, certified, or verified to the aforementioned equivalent standards.

Additionally, the PMA reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the CAs.

6.2.2 Private Key Multi-Person Control

6.2.2.1 RCA and CA

RCA and CA implement technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive RCA and CA cryptographic operations.

6.2.2.2 Subscriber

6.2.2.2.1 Physical subscriber

Physical subscriber certificate is activated with an activation data.

6.2.2.2.2 Non physical subscriber

Non physical subscriber (devices, services) certificate is activated with password and mechanism provided by the equipment and configured by the system administrator of the device, service.

6.2.3 Private Key Escrow

6.2.3.1 RCA and CA

Under no circumstances shall the private keys be escrowed by a third party.

6.2.3.2 Subscriber

Only encryption keys are escrowed by the KEA.

Under no circumstances shall other type of private key (authentication, signing) be escrowed by a third party or PKI component.

The Subscriber's private keys used solely for decryption must be escrowed prior to the generation of the corresponding Certificates.

6.2.4 Private Key Backup

6.2.4.1 RCA and CA

The private keys shall be backed up under the same multi-person control as the operational signature key. A single backup copy of the signature key shall be stored at or near the RCA and CA location. A second backup copy shall be kept at the backup location (5.1.8). Procedures for private signature key backup are be included in the appropriate CPS and meet the multiparty control requirement of Section 5.2.2.

6.2.4.2 Subscriber

6.2.4.2.1 Physical subscriber

Subscriber key pair is not backed up by the Subscriber or by any PKI component.

Only the encryption key is escrowed by the KEA for recovery purpose.

6.2.4.2.2 Non physical subscriber

Technical Contact may make a back-up copy of their private key so as to be able to deploy it on several devices or services in the event of an incident or for reasons relating to the performance of protected websites.

The Technical Contact is responsible for defining and ensuring compliance with the resources and procedures that will enable a key pair to be securely generated, protected and used (refer to 6.1.1 above).

6.2.5 Private Key Archival

6.2.5.1 RCA and CA

Private keys must never be archived.

6.2.5.2 Subscriber

Subscriber's private key must not be archived.

Only encryption key (for physical subscriber) are escrowed for recovery purpose.

6.2.6 Private Key Transfer into or from a Cryptographic Module

6.2.6.1 RCA and CA

In case of private key transfer, then the key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 above with one of the following methods:

- Direct token-to-token copy;
- Trusted path under N out of M multi-person control (refer to section 6.2.2 above);
- Wrapping mechanism with the wrapping asymmetric key generated on the destination HSM.

Keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, private keys are encrypted. An encrypted private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.2 Subscriber

6.2.6.2.1 Physical subscriber

Physical person's private key must not be transferred from or into the token.

Only Physical person's private key for encryption certificate is securely transferred in the token using TMA.

6.2.6.2.2 Non physical subscriber

Non physical subscriber use software key. Therefore, this section is not applicable.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 RCA and CA

The HSM stores private keys in any form as long as the keys are not usable without authentication mechanisms that are compliant with the ones mentioned in the security policy attached to the HSM approved use and are not exportable out of the HSM.

6.2.7.2 Subscriber

6.2.7.2.1 Physical subscriber

The token stores Private Keys in any form as long as the keys are not usable without authentication mechanism that is in compliance with the evaluation criteria of the token and not exportable out of the token.

6.2.7.2.2 Non physical subscriber

Non physical subscriber use software key. Therefore, this section is not applicable.

6.2.8 Method of Activating Private Key

6.2.8.1 RCA and CA

For RCA, activation of the RCA's HSM, to sign and/or revoke CA certificates, requires several trusted roles with activation data to activate the RCA private key. Each trusted role is authenticated before activating a RCA private key.

Several trusted roles with activation data are required to realize the initial activation of the HSM that contains the CA key pair corresponding to a CA Certificate. Once the HSM containing the CA key and the CA key is operational, only the authorized services of the PKI system can use the CA key pair within the HSM, by using mutual authenticated interface of the PKI systems.

6.2.8.2 Subscriber

6.2.8.2.1 Physical subscriber

The physical person must be authenticated to the token before the activation of any private key(s). The authentication requires her/his activation data.

6.2.8.2.2 Non physical subscriber

The TC is responsible for defining the resources and procedures that will enable a key pair to be securely generated, protected and used (refer to 6.1.1 above).

6.2.9 Methods of Deactivating Private Key

6.2.9.1 RCA

An activated RCA HSM is never left unattended or otherwise available to unauthorized access. After use, the HSMs are deactivated. The HSMs are removed from RCA component and stored in secure locations (refer to section 5.1 above) to avoid their use without authorization and strongly authenticated roles. After deactivation, the use of the HSM based RCA key pair requires the presence of the trusted roles with the activation data in order to reactivate said RCA key pair (refer to section **Erreur ! Source du renvoi introuvable.** above).

6.2.9.2 CA

HSM that has been activated is never left unattended or otherwise available to unauthorized access.

After use, HSM are deactivated. After deactivation, the use of the HSM based CA key pair requires the presence of the trusted roles with the activation data in order to reactivate said CA key pair (refer to section 6.2.8 above).

6.2.9.3 Subscriber

6.2.9.3.1 Physical subscriber

Physical person's private key is deactivated once the session of the token is expired or closed. Then, the activation data is required to reactivate the private key.

6.2.9.3.2 Non physical subscriber

Non physical subscriber use software key. Therefore, this section is not applicable.

6.2.10 Method of Destroying Private Key

6.2.10.1 RCA and CA

Destroying private key inside an HSM requires destroying the key(s) inside the HSM using the 'zeroization' function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the private key back-ups have to be destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of HSM are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section **Erreur ! Source du renvoi introuvable.** above) by personnel in trusted roles (refer to section 5.2 above) under at least dual control.

6.2.10.2 Subscriber

6.2.10.2.1 Physical subscriber

When the private key must be destroyed, the physical subscriber must bring back the token to the RA, LRA or TMA.

Then, the RA or LRA or TMA destroys the Physical person's private keys in the token by using function of the token. If the token is completely blocked, then RA, LRA or TMA physically destroys the token.

6.2.10.2.2 Technical Contact

The TC is responsible for defining the resources and procedures that will enable a key pair to be securely destroyed (refer to section 6.1.1 above).

6.2.11 Cryptographic Module Rating

See sections 6.1.1 and 6.2.1.

6.3 OTHER ASPECTS OF KEY MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods/Key Usage Periods

6.3.2.1 RCA

The maximum operational period for a legacy RCA certificate is 10 years' maximum.

The maximum operational period for a legacy RCA private key is the end validity period of the valid legacy RCA certificate.

The maximum operational period for a current RCA certificate is 25 years' maximum.

The maximum operational period for a current RCA private key is the end validity period of the valid current RCA certificate.

6.3.2.2 CA

The maximum operational period for a legacy CA certificate is 10 years' maximum.

The maximum operational period for a legacy CA private key is the end validity period of the valid legacy CA certificate.

The maximum operational period for a current CA certificate is 10 years' maximum.

The maximum operational period for a current CA private key is the end validity period of the valid current CA certificate.

6.3.2.3 Subscriber

Subscriber private key can be used as long as the associated certificate is valid (neither expired nor revoked).

The maximum operational period for a subscriber certificate issued by a legacy CA is 1 year maximum.

The maximum operational period for a subscriber certificate issued by a current CA is 3 years' maximum.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

6.4.1.1 RCA and CA

Activation data used to protect HSM containing private keys are generated during the initial PKI key ceremony. The activation data used to unlock private keys, in conjunction with any other access control have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Some of the most critical activation data are backed-up (CPS gives exact details).

The PMA appointed individuals receive their activation data during the key ceremony through a face to face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.2 Subscriber

6.4.1.2.1 Physical subscriber

For physical person, the generation of activation data used to activate private keys is made during the personalization of the token by the RA.

For a token, the following activation data are created:

- Activation data: this activation is defined by the RA or LRA. This code is used to activate private keys (PIN).
- Unlock data: this activation data is defined by the TMA. This code is used to unblock the token (SOPIN or PUK).

RA or LRA has to transmit securely during a face to face, protected in integrity and confidentiality, the activation code to the physical person.

The unlock code (SOPIN or PUK) is stored encrypted by TMA, the activation code is not stored anywhere.

Physical subscriber has to change her/his activation code before using the associated private key.

6.4.1.2.2 Non physical subscriber

Technical Contact chooses the value for activation data and ensure it is of a strength that is commensurate with the assurance level of the private key being protected.

6.4.2 Activation Data Protection

6.4.2.1 RCA and CA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The PMA requires that activation data holder store activation data in a safe for which access is controlled by both the holder and other employees in trusted roles. When they are not used, activation data are always stored in a safe (refer to section 5.1 above).

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.2 Subscriber

6.4.2.2.1 Physical subscriber

Physical person is responsible to ensure the protection of its activation data (activation code / PIN).

TMA are responsible to ensure the protection of the unlock code (SOPIN / PUK).

6.4.2.2.2 Non physical subscriber

TC is responsible to ensure the protection of its activation data.

6.4.3 Other Aspects of Activation Data

6.4.3.1 RCA and CA

Activation data are changed in case the hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending an HSM to the manufacturer for maintenance, all sensitive information contained in the HSM shall be destroyed (refer to section **Erreur ! Source du renvoi introuvable.** above).

6.4.3.2 Subscriber

6.4.3.2.1 Physical subscriber

When token is blocked due to false activation code enter in token, the physical subscriber can request TMA, RA or LRA to unlock it's token.

The LRA, RA or TMA identifies and authenticates the subscriber. If the subscriber is successfully authenticated, then TMA unlock the token and request the subscriber to change its activation data (PIN).

6.4.3.2.2 Non physical subscriber

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. PKI components implement the following functionalities:

- Require authenticated logins for trusted roles.
- Provide discretionary access control.
- Require use of authentication for session communication.
- Require user identification.
- Provide domain isolation for processes involving roles using PKI services.
- Remove unwanted services and ports from the PKI components.

When the PKI equipment is hosted on platforms certified for computer security assurance requirements, the system (hardware, software and operating system), when possible, operates in said certified configuration. At minimum, such platforms use the same version of the computer operating system as the one which received the evaluation rating. OA computer systems are configured with minimum required accounts, network services, and no remote login.

PKI components (RCA) that is used for RCA key ceremony operation are not connected to any communication network. Key ceremony workstations for RCA are dedicated to key ceremony operations only.

6.5.2 Computer Security Rating

No stipulations

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The system development controls for the PKI are as follows:

- Use software that has been designed and developed under a formal, documented development methodology according to Common Criteria evaluation.
- Hardware and software procured are purchased in such a way so as to reduce the likelihood that any particular component was tampered with.
- Hardware and software are developed in a controlled environment, and the development process is defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware is shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software is dedicated to performing the PKI activities. There is no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation.
- Proper care is taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations are obtained from sources authorized by local policy.

Hardware and software updates are purchased or developed in the same manner as original equipment, and installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the PKI system as well as any modifications and upgrades is documented and controlled. A procedure is used for installation and ongoing maintenance of the PKI system. The PKI software is verified as being that supplied from the vendor, with no modifications, and be the version intended for use. There is a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance for the system.

The following rules apply:

- Implement an IT administration system under the control of the OA that monitors, detects, and reports any security-related configuration change PKI systems (for online system).
- Require trusted role personnel to follow up on alerts of possible critical security events.

- Conduct a human review of application and system logs and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (refer to section **Erreur ! Source du renvoi introuvable.** above).

6.6.3 Life Cycle Security Controls

For the software and hardware that are evaluated, the PMA and External Entity monitor the maintenance scheme requirements to ensure the same level of trust.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 NETWORK SECURITY CONTROLS

6.7.1 RCA

Key ceremony operations for RCA are performed in off-line environment. The key ceremony workstation is never connected to any communication network.

6.7.2 Online PKI component

The PKI system implements appropriate security measures to ensure it is guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls and filtering routers. Unused network ports and services are turned off. Any network software present is necessary to the functioning of the PKI system.

The following rules apply:

- Any boundary control devices used to protect the network on which PKI equipment is hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
- Segment PKI equipment into networks or zones based on their functional, logical, and physical (including location) relationship. Only authorized flow, used for administration and PKI services, between PKI equipment are authorized.
- Maintain and protect PKI components in at least dedicated zone and make a separation between interfaces accessible from Internet to interfaces accessible by internal needs.
- Implement and configure an administration network (a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, anti-virus when it is applicable and IT administration) that protects systems and communications between PKI systems and communications with non-PKI systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.
- Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the PKI component has identified as necessary to its operations.
- Configure PKI components by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the PKI component's operations and allowing only those that are approved by the PKI component.
- Review regularly configurations of the PKI system to determine whether any changes have violated the PKI component security policies.
- Grant administration access to PKI components only to persons acting in trusted roles and require their accountability for the PKI component's security.

- Implement strong authentication for each component of the PKI system that supports multi-factor authentication.
- Change authentication keys and passwords for any privileged account or service account on a PKI System whenever a person's authorization to administratively access that account on the PKI System is changed or revoked.

Apply recommended security patches, viewed by the software editor and entity like CERT as mandatory to avoid a concrete and high risk attack on the PKI system, with to PKI systems within six months of the security patch's availability, unless the PKI establishes that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

6.8 TIME STAMPING

For trusted time on audit records, all PKI components are regularly synchronized with reliable time service Network Time Protocol (NTP) Service. Time derived from the time service are used for establishing the time of:

- Initial validity time of a Certificate; and
- Revocation of a Certificate; and
- Recovery operation; and
- Posting of CRL updates.

Asserted times is accurate to within three minutes. Electronic or manual procedures may be used to maintain system time.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

The RCA and CAs issue X.509 v3 Certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Any CAs asserting critical private extensions shall be interoperable in their intended community of use.

RCA, CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 details the Certificate profiles.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

7.1.3.1 Legacy Certificate Authorities

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
Certificates under this CP shall use the following OID for identifying the subject public key information: rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.3.2 Current Certificate Authorities

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
Certificates under this CP shall use the following OID for identifying the subject public key information: rSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The Subject and Issuer fields of the Certificate are populated with a Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by [RFC5280], and section 4.1.2.

When multiple values exist for an attribute in a DN, the DN shall be encoded so that each attribute value is encoded in a separate relative distinguished name.

7.1.5 Certificate Policy Object Identifier

Subscriber Certificates issued under this CP must assert only one of the Certificate policy OIDs listed in section 1.2 of this CP.

7.1.6 Policy Qualifiers Syntax and Semantics

Certificates issued under the Thales domain CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers.

7.1.7 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical Certificate policy extension must conform to X.509 certification path processing rules.

7.2 CRL PROFILE

7.2.1 Version Numbers

CAs must issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL and CRL Entry Extensions

Critical private extensions must be interoperable in their intended community of use.

CPS contains the CRL formats.

7.3 OCSP PROFILE

7.3.1 Version Number

Not applicable.

7.3.2 OCSP Extensions

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS

All PKI component and a sample of RA/LRA shall be subject to a periodic compliance audit according frequency defined by PMA.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of the applicable CP. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor shall be a firm, which is independent from Thales. The PMA shall determine whether a compliance auditor meets this requirement.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that a component operates in accordance with the applicable CP, the component CPS.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The PMA may determine that a PKI component is not complying with its obligations set forth in this CP. When such a determination is made, the PMA may suspend operation of the PKI component or may direct that other corrective actions be taken which allow interoperation to continue.

When the compliance auditor finds a discrepancy between how the PKI component and/or service is designed or is being operated or maintained, and the requirements of this CP, the Entity CP or the applicable CPS, the following actions shall be performed:

- The compliance auditor shall note the discrepancy; and
- The compliance auditor shall notify the Entity of the discrepancy; and
- The Entity shall notify the PMA promptly.

The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to halt temporarily operation of the CA or only the PKI component, to revoke a Certificate issued by the CA, or take other actions it deems appropriate. The PMA shall develop procedures for making and implementing such determinations.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, shall be provided to the PMA. The report shall identify the versions of the CP and CPS used in the assessment.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance and Renewal Fees

Not applicable.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Thales maintains reasonable levels of insurance coverage as required by applicable laws.

9.2.2 Other Assets

Thales maintains sufficient financial resources to maintain operations and fulfill their respective obligations under this CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Subscribers acknowledge that any information made public in a Certificate is deemed not private. In that respect, Certificates, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or confidential.

Personal and corporate information, which does not appear in Certificates and in public directories, held by a PKI component is considered confidential and shall not be disclosed by the PKI component. Unless required by law or court order, any disclosure of such information requires Subscriber's written prior consent.

The treatment of confidential business information provided to external PKIs in the context of submitting an application for certification will be in accordance with the terms of the agreements entered into between the applicable entity and Thales.

Each PKI component shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the PMA treats its own most confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

For the purposes of the PKI related services, the Thales and External Entity may collect, store, or process personally identifiable information. Any such use or disclosure shall be in accordance with applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

Entity PKI components shall develop a Privacy Policy, according to European Law, and stipulate in their CP or a document referenced in their CP how they protect any personally identifiable information they collect.

Subscribers must be given access and the ability to correct or modify their personal or organization information upon appropriate request to the RA. Such information must be provided only after taking proper steps to authenticate the identity of the requesting party.

When personal or organization information for Subscriber's certificate has to be modified, then if the certificate is generated, the certificate has to be revoked. Subscriber can't request modification or suppression of personal data for issued certificate because PKI shall keep it at a proof of identity and registration operation for the issued certificate. Personal data are not stored more than duration defined in section 5.5.

9.5 INTELLECTUAL PROPERTY RIGHTS

9.5.1 Property Rights in Certificates and Revocation Information

Thales shall retain all intellectual property rights in and to the Certificates and revocation information that they issue.

Thales shall grant permission to reproduce and distribute Certificates, and/or use Revocation or Certificate status information (minimum are ARL and CRL) on a non-exclusive, royalty-free basis, provided they are reproduced in full and that use of said Certificates is subject to a memorandum of agreement or equivalent contractual mechanism between the Thales PKI and their Subscribers and Relying Parties.

9.5.2 Property Rights in the CPS

Thales asserts that it owns and/or has licensed all Intellectual Property rights to this CP and related CPS. Furthermore, Thales reserves all Intellectual property rights in this CP to be granted to any Licensor at its discretion in conjunction with any agreement or equivalent contractual mechanism expressing such a license.

9.5.3 Property Rights in Names

The Certificates may contain copyrighted material, trademarks and other proprietary information, and no commercial exploitation or unauthorized use of the material or information in or via the Certificates is permitted, except as may be provided in this CP or in any applicable agreement. In the event of any permitted use or copying of trademarks and/or copyrighted material, no deletions or changes in proprietary notices shall be made without written authorization from the owner.

9.5.4 Property Rights in Keys

Key pairs corresponding to Certificates of PKI components and Subscribers are the property of Thales. For PKI components and Subscriber in contract with Thales and Subscribers' entity for Subscriber in contract with external entity that are the respective subjects of these Certificates, subject to the rights of Subscribers regardless of the physical medium within which they are stored and protected. Such persons retain all Intellectual Property Rights in and to these Key Pairs. Notwithstanding the foregoing, the Thales's RCA and CA Public Keys and self-signed Certificates are the property of Thales.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

9.6.1.1 Policy Management Authority

PMA defines the present CP and the corresponding CPS. PMA establishes that PKI component complies with the present CP. The processes and procedures and audit framework used to determine compliance are documented within the CPS.

PMA ensures that all requirements on Entity PKI component, as detailed in the present CP and in the corresponding CPS, are implemented as applicable to deliver and manage CA and Subscriber certificate.

PMA has the responsibility for compliance with the procedures prescribed in this CP, even when PKI component functionality is undertaken by sub-contractors (OA …). RCA provides all its certification services consistent with its certification practice statement.

9.6.1.2 Root Certification Authority (RCA)

Common obligations for RCA components are:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their private key and certificate, with associated tools specified in CPS, for the purpose they have been generated as defined in the CP.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Allow the auditor team to control and check the compliance with the present CP and with the components CP/CPS and communicate requested information to them, in accordance with the intentions of the PMA.
- Document their internal procedures to complete the global CPS.
- Use every means (technical and human) necessary to achieve the realization of the CP/CPS it has to implement and for which they are responsible.
- Alert PMA in case of incident due to RCA.

9.6.1.3 Certification Authority (CA)

The CA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their cryptographic key and certificate, with associated tools specified in CPS, for what purpose they have been generated as defined in the present CP.
- Respect and operate the section(s) of the present CP and CPS and its CP and its CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Allow the auditor team to control and check the compliance with the present CP and with its CP/CPS and communicate the requested information to them, in accordance with the intentions of the PMA.
- Document their internal procedures to complete their global CPS.
- Use every means (technical and human) necessary to achieve the realization of the present CP and its CP/CPS it has to implement and for which they are responsible.
- Respect the agreement established between External Entity and Thales.
- Transmit the right public key to be certified by RCA.
- Establishes contract with CA and RA entity when they are different legal entity from it with clear identification of PKI services run by the entity and all RA's obligations and warranties according PKI services managed.
- Only issue and manage type of Subscriber Certificate with level of trust approved by PMA.
- Alert PMA in case of incident due to CA or PKI component used by CA to manage Subscriber Certificate.

9.6.1.4 Registration Authority

The RA has the responsibility to:

- Authenticates and identify Subscriber and LRA.
- Submit accurate and complete information to the CA.
- Nominates and identifies LRA.
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the OA’s security policy.
- Alert PMA when there is a security incident about the CA services that the OA performed; and
- Deliver token to the LRA.
- Deliver the activation code to the Subscriber and LRA.
- Respect the CP and corresponding CPS.

9.6.1.5 LRA

The LRA has the responsibility to:

- Authenticate and identify Subscriber.
- Submit accurate and complete information to the RA.
- Deliver token the the Subscriber.
- Alert and notify RA for revocation request.
- Protect identity smart card and associated activation data.
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS.
- Alert PMA when there is a security incident about the CA or RA services that the OA performed.
- Respect the CP and corresponding CPS.

9.6.1.6 TMA

The TMA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their secret data and private key.
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the OA's security policy.
- Alert PMA when there is a security incident about the PKI services that the OA performed.
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component).
- Generate Subscriber's key pair in the token and associated activation data in a secure way and personalize the token with it and inject securely encryption key pair in the token of the Subscriber.
- Store securely activation data and unlock data and authentication data of Subscriber.
- Provided unlock capability for Subscriber token.
- Deliver Subscriber's public key to the CA.
- Deliver Subscriber's key pair and associated activation data securely to the LRA or RA.

9.6.1.7 Operational Authority

The OA has the responsibility to:

- Respect its security policy.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the OA's security policy.
- Alert PMA when there is a security incident about the CA services that the OA performed; and
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component).
- Protect identity smart card and associated activation data.
- Document their internal procedures to complete global CPS and its security policy.
- Respect total or part of agreements that binds it to the PMA.

9.6.2 KRA

The KRA has the responsibility to:

- Respect its security policy.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the OA's security policy.
- Alert PMA when there is a security incident about the PKI services that the OA performed;
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component).
- Protect identity token and associated activation data.
- Generate Subscriber's key pair and associated activation data in a secure way.
- Deliver Subscriber's key pair and associated activation data securely to the RA.
- Deliver External Entity's key pair and associated activation data securely to the RA.
- Provide recovery services for encryption key pair for authorized request.
- Protect and respect procedure defined by PMA to interact with PKI to manage recovery request.

9.6.3 KEA

The KEA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the OA's security policy.
- Alert PMA when there is a security incident about the PKI services that the OA performed.
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component).
- Escrow external encryption key pair and activation data.
- Deliver Subscriber's encryption key pair and associated activation data securely to the KRA and RA.

9.6.4 Physical subscriber

The physical subscriber has the responsibility to:

- Accurately represent themselves in all communications with the RA and LRA.
- Protect their private keys at all times and prevent them from unauthorised access in accordance with this policy, as stipulated in their Subscriber agreement.
- Promptly notify the appropriate RA or LRA upon suspicion of loss or compromise or suspicion of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CP.
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates, as set forth in this CP and the Subscriber agreement.
- Use Certificates provided by the CA only for authorized and legal purposes in accordance with the Entity CP.
- Cease to use such issued Certificates if they become invalid and remove them from any applications they have been installed on.

9.6.5 Non physical subscriber

The Technical Contact has the responsibility to:

- Accurately represent themselves in all communications with the RA.
- Transmit right public key associated with the private key to the RA.
- Protect their Private Keys at all times and prevent them from unauthorized access in accordance with this policy, as stipulated in their Subscriber agreement.
- Promptly notify the appropriate RA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with this CP.
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Keys and Certificates, as set forth in this CP and the Subscriber agreement.
- Use Certificates provided by the CA only for authorized and legal purposes in accordance with the CP.
- Cease to use such issued Certificates if they become invalid and remove them from any applications they have been installed on.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 Relying Party

Any relying party has the responsibility to validate a digital certificate using:

- Only accept the use of the Certificate for the purposes indicated in the Certificate keyUsage extensions.
- Verify the validity of the Certificate, using the procedures described in [RFC5280], prior to any reliance on said Certificate.
- Check the OID contained in each certificate of the trusted certification path in order to be sure to accept the right kind of certificate.
- Establish trust in the RCA and CA who issued the Certificate by the methods outlined elsewhere in this CP, and using the path validation algorithm outlined in [RFC5280].
- Preserve the original signed data, the applications necessary to read and process that data and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify said signature.
- Check alert provided by Application Software Suppliers, External Entity and Thales (using PS information as stated in section 2 above).
- Cease to use such issued Certificates (Subscriber, RCA and CA) if they become invalid and remove them from any applications they have been installed on.

9.7 DISCLAIMERS OF WARRANTIES

Thales guarantees through the PKI services:

- Identification and authentication of CA, with the CA Certificate generated by the RCA.
- Management of corresponding certificates and certificate status information regarding the present CP.
- Level of trust of Subscriber Certificate managed by CA signed by RCA.
- Identification and authentication of Subscriber, with Subscriber certificate generated by the applicable CA.
- Management of corresponding certificates and certificate status information regarding the present CP.
- CA certificate content according information transmitted by External Entity.

Thales provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the PKI or for the legal validity, acceptance or any other type of recognition of its own certificates otherwise mentioned above. No more guarantees can be pinpointed by the External Entity, Subscriber and Relying Party in their contractual relationship (if there is any).

9.8 LIMITATIONS OF LIABILITIES

Thales makes no claims with regard to the suitability or authenticity of certificates issued under this CP. Relying parties may only use these RCA, CA and Subscriber certificates at their own risk. Thales assumes no liability what so ever in relation with the use of certificate or associated public/private key pairs for any use other than those described in the present CP/CPS.

9.9 INDEMNITIES

Thales makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these RCA, CA and Subscriber certificates at their own risk. Thales has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP. Contract between Thales and External Entity describe the rule to be applied.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP and any amendments thereto, become effective upon ratification by the PMA and publication.

There is no specified term or limitation thereon to this CP.

9.10.2 Termination

While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by a resolution of the PMA. For purposes of clarity, termination of any PKI component contract shall not operate as a termination of this CP unless this CP is explicitly terminated by a separate resolution of the PMA (refer to section 5.8).

9.10.3 Effect of Termination and Survival

Upon termination of this CP, CA certified by Thales domain are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates (refer to section 5.8).

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All parties mentioned herein will use the methods specified in the respective agreements between the parties to communicate and/or deliver any relevant notices.

The PMA provides all participants with new version of CP via the PS, as soon as it is validated by the PMA.

Notices and Communication to Relying Parties or other parties for whom an explicit agreement does not exist shall be by commercially reasonable methods, taking into account the criticality and subject matter of the communication.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The PMA shall review the CP and CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the PMA.

If the PMA wishes to recommend amendments or corrections to the CP or CPS, such modifications shall be circulated to appropriate parties identified by the PMA (including, without limitation, CAs).

Notwithstanding the foregoing, if PMA believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of PKI component, they shall be entitled to make such amendments effective immediately upon publication in the Repository. PMA shall use commercially reasonable efforts to immediately notify PKIs component of such changes.

9.12.2 Notification Mechanism and Period

Errors and anticipated changes to the CP and CPS resulting from reviews shall be published publicly online. The location of the most up to date copy of the CP shall be described in the CPS, and clearly communicated on the Thales web site.

In addition, changes are communicated by the PMA to every External Entity and PKI component via a designated point of contact, including a description of the change.

This CP and any subsequent changes shall be made publicly available within seven days of approval.

9.12.3 Circumstances under Which OID Must be changed

Certificate Policy OIDs shall be changed if the PMA determines that a change in the CP materially affects the level of assurance provided.

9.13 DISPUTE RESOLUTION PROVISIONS

Provisions for resolving disputes between Thales and its External Entity or PKI component shall be set forth in the applicable agreements between the parties.

9.13.1 Disputes among Thales domain

Provisions for resolving disputes between Thales and its External Entity or PKI component shall be set forth in the applicable agreements between the parties.

9.13.2 Alternate Dispute Resolution Provisions

In case of any dispute or disagreement between two or more participants arising out of or related to this CP, the Disputing Parties will use their best efforts to settle the dispute or disagreement through mediation or good faith negotiations following notice from one disputing party to the other. If the dispute is not successfully resolved by negotiation between the entities or the parties within sixty (60) days following the date of such notice, it shall be settled by final and binding arbitration before a single arbitrator knowledgeable in the information technology industry in accordance with the then existing Rules of Conciliation and Arbitration of the Paris Chamber of Commerce. The place of arbitration shall be defined in the relevant agreement between contracting parties.

This provision does not limit the right of a party to obtain other recourse and relief under any applicable law for disputes or disagreements that do not arise out of or which are not related to this CP.

9.14 GOVERNING LAW

French law governs this CP and CPS.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. French law governs this CP and CPS.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

This CP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this CP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this CP which by their nature extend beyond the term of the performance of the services such as without limitation those concerning confidential information and intellectual property rights shall survive such term until fulfilled and shall apply to any party's successors and assigns.

9.16.2 Assignment

Except as otherwise provided under the applicable agreements, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party, except that Thales may assign and delegate this CP to any party of its choosing.

9.16.3 Severability

If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CP are for convenience only and cannot be used in interpreting this CP.

9.16.5 Force Majeure

Thales shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

THALES HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO THALES DOMAIN.

9.17 OTHER PROVISIONS

No stipulation.

10. CERTIFICATE PROFILES

Certificates profiles are referenced in CPS.

End of Document