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

CERTIFICATE PRACTICE STATEMENT

THALES PKI

THALES GROUP OPEN

Identifiant Entité	Identifiant Document	DTC	Révision
9950-2598	0001-0031865608	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 Practice statement is consistent with the Internet Engineering Task Force (IETF) RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework” and Thales CP.

1.1 OVERVIEW

Refer to CP.

1.1.1 Certificate Policy

Refer to CP.

1.1.2 Relationship between this CP and the Thales domain Bridge CPS and Thales domain Root CPS

Refer to CP.

1.1.3 Scope

Refer to CP.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CPS is not specifically registered and does not have a specific OID.

1.3 PKI PARTICIPANTS

1.3.1 PKI Authorities

1.3.1.1 Policy Management Authority (PMA)

GPSSI is the PMA.

1.3.1.2 Root CA

Refer to [PKI Architecture].

1.3.1.3 Intermediate CA (ICA)

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.1.4 Signing CA

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.1.5 Certificate Status Authorities

Refer to CP.

1.3.1.6 Registration Authority (RA)

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.2 Token Management Authority (TMA)

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.3 Key Escrow Authority (KEA)

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.4 Key Recovery Authority (KRA)

Refer to [PKI Architecture] and [PKI role and Subscriber procedure].

1.3.5 Operational Authority (OA)

OA is located in Thales physical location.

1.3.6 Publication Service (PS)

Refer to [PKI Architecture].

1.3.7 Subscribers

Refer to [PKI role and Subscriber procedure].

1.3.8 Relying Parties

Refer to CP.

1.3.9 Other Participants

1.3.9.1 External Entity (Organization)

Refer to CP.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

Refer to CP.

1.4.2 Prohibited Certificate Uses

Refer to CP.

1.5 Policy Administration

1.5.1 Organization administering the document

Refer to CP.

1.5.2 Contact Person

Refer to CP.

1.5.3 Person Determining Certificate Practice Statement Suitability for the Policy

Refer to CP.

1.5.4 CPS Approval Procedures

Refer to CP.

1.5.5 Waivers

Refer to CP.

1.6 Definitions and Acronyms

Refer to CP.

2. PUBLICATION AND PKI REPOSITORY RESPONSIBILITIES

2.1 PKI REPOSITORIES

Refer to [PKI Architecture].

2.2 PUBLICATION OF CERTIFICATE INFORMATION

2.2.1 Publication of CA Information

Refer to CP.

2.3 TIME OR FREQUENCY OF PUBLICATION

Refer to CP.

2.4 ACCESS CONTROLS ON PKI REPOSITORIES

Refer to [PKI Architecture] and [Security Policy].

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

Refer to [CA naming] and [Subscriber naming].

3.1.2 Need for Names to be Meaningful

Refer to [CA naming] and [Subscriber naming].

3.1.3 Anonymity or Pseudonymity of Subscribers

Refer to [CA naming] and [Subscriber naming].

3.1.4 Rules for Interpreting Various Name Forms

Refer to [CA naming] and [Subscriber naming].

3.1.5 Uniqueness of Names

Refer to [CA naming] and [Subscriber naming].

3.1.6 Recognition, Authentication and Role of Trademarks

Refer to CP.

3.1.7 Name Claim Dispute Resolution Procedure

Refer to [PKI role and Subscriber procedure].

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 RCA, ICA and CA

Refer to [Key ceremony] and [PKI Architecture].

3.2.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

3.2.1.3 Machine

Refer to [PKI role and Subscriber procedure].

3.2.2 Authentication of Organization Identity

3.2.2.1 Organization Affiliation

3.2.2.2 RCA, ICA and CA

PMA authorizes legal entity names to be set in the RCA, ICA and CA certificate.

For delegated CA signed by ICA, CA's legal entity name authentication is realized by trusted role (refer to [PKI role and Subscriber procedure]) delegated by PMA to create CA certificate with legal entity name.

3.2.3 Authentication of Individual Identity

3.2.3.1 RCA, ICA and CA

PMA authorizes person to be activation data holder for RCA to be set in the RCA, ICA and CA certificate.

During RCA key ceremony person are authenticated by security officer using official ID government card (refer to [Key ceremony]).

For delegated CA refer [PKI role and Subscriber procedure].

3.2.3.2 Common to all assurance Levels for subscriber

Refer to [PKI role and Subscriber procedure].

3.2.3.3 Machine

Refer to [PKI role and Subscriber procedure].

3.2.3.4 Physical person

Refer to [PKI role and Subscriber procedure].

3.2.4 Non-verified Subscriber Information

Refer to [PKI role and Subscriber procedure].

3.2.5 Validation of Authority

3.2.5.1 RCA, ICA and CA

The PMA appoints and authorizes the OA to generate RCA, ICA and CA certificates, under its control.
For delegated CA refer [PKI role and Subscriber procedure].

3.2.5.2 Subscriber

Refer to [PKI role and Subscriber procedure].

3.2.6 Criteria for Interoperation

Refer to CP.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

3.3.1.1 RCA, ICA and CA

Same procedures as described in section 3.2 above apply.

For delegated CA refer [PKI role and Subscriber procedure].

3.3.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

3.3.2 Identification and Authentication for Re-key after Revocation

3.3.2.1 RCA, ICA and CA

Same procedures as described in section 3.2 above apply.

For delegated CA refer [PKI role and Subscriber procedure].

3.3.2.2 Subscriber

Refer to [PKI role and Subscriber procedure].

3.4 Identification and Authentication for Revocation Requests

3.4.1.1 RCA, ICA and CA

Same procedures as described in section 3.2 above apply.

For delegated CA refer [PKI role and Subscriber procedure].

3.4.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Application

4.1.1.1 RCA, ICA and CA

PMA authorizes the creation of the initial RCA, ICA and CA certificate signing a [CA naming] prepared by OPENTRUST. OPENTRUST gives the [CA naming] to the Administrative contact.

For online delegated CA signed by ICA, trusted role (refer to [PKI role and Subscriber procedure]) is delegated by PMA to create CA.

4.1.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.1.2 Registration Process and Responsibilities

4.1.2.1 RCA, ICA and CA

Prior to the RCA, CA and ICA certificate initial creation, the administrative contact transmits the [CA naming] signed to the Master of Key Ceremony of OpenTrust and PMA.

For delegated CA signed by ICA, CA creation is realized by trusted role (refer to [PKI role and Subscriber procedure]) is delegated by PMA to create CA.

4.1.2.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1.1 RCA, ICA and CA

PMA authorizes the creation of the initial RCA, CA and ICA certificate signing a [CA signing].

For delegated CA refer to [PKI role and Subscriber procedure].

4.2.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.2.2 Performing Identification and Authentication Functions

4.2.2.1 CA Certificates

PMA authorizes the creation of the initial RCA, CA and ICA certificate signing a [CA signing] prepared by OPENTRUST.

For delegated CA signed by ICA, trusted role is delegated by PMA to create CA (refer to [PKI role and Subscriber procedure]).

4.2.2.2 Subscriber Certificates

Refer to [PKI role and Subscriber procedure].

4.2.3 Approval or Rejection of Certificate Applications

4.2.3.1 RCA, ICA and CA

PMA may approve or reject a RCA, ICA and CA application.

Delegated trusted role approve or reject the CA creation (refer to [PKI role and Subscriber procedure]).

4.2.3.2 Subscriber Certificate

Refer to [PKI role and Subscriber procedure].

4.2.4 Time to Process Certificate Applications

4.2.4.1 RCA, ICA and CA

No stipulation.

4.2.4.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

4.3.1.1 RCA

Refer to [Key ceremony].

4.3.1.2 ICA and CA

For CA and ICA refer to [Key ceremony].

For delegated CA refer to [PKI role and Subscriber procedure].

4.3.1.3 Physical person

Refer to [PKI role and Subscriber procedure].

4.3.1.4 Device

Refer to [PKI role and Subscriber procedure].

4.3.2 Notification to Subscriber of Certificate Issuance

4.3.2.1 RCA, ICA and CA

Not applicable.

4.3.2.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 RCA, ICA and CA

For RCA refer to [Key ceremony].

For delegated CA refer to [PKI role and Subscriber procedure].

4.4.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.4.2 Publication of the Certificate by the CA

RCA, CA and ICA certificate to be published are communicated by witness to the PS.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 2.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Refer to CP.

4.5.2 Relying Party Public Key and Certificate Usage

Refer to CP.

4.6 CERTIFICATE RENEWAL

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, but a new, extended validity period and a new serial number.

4.6.1 Circumstance for Certificate Renewal

4.6.1.1 RCA, ICA and CA

For RCA refer to [Key ceremony].

For delegated CA refer to [PKI role and Subscriber procedure].

4.6.1.2 Subscriber

Refer to [PKI role and Subscriber procedure].

4.7 CERTIFICATE RE-KEY

Refer to CP.

4.7.1 Circumstance for Certificate Re-key

For RCA refer to [Key ceremony].

For delegated CA refer to [PKI role and Subscriber procedure].

Refer to [PKI role and Subscriber procedure].

4.8 CERTIFICATE MODIFICATION

For RCA refer to [Key ceremony].

For delegated CA refer to [PKI role and Subscriber procedure].

Refer to [PKI role and Subscriber procedure].

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstance for Revocation of a Certificate

4.9.1.1 RCA

Refer to CP.

4.9.1.2 ICA

Refer to CP.

4.9.1.3 CA

Refer to CP.

4.9.1.4 Subscriber

4.9.1.4.1 Physical person

Refer to CP.

4.9.1.4.2 Machine

Refer to CP.

4.9.2 Who Can Request Revocation of a Certificate

4.9.2.1 RCA, ICA and CA

Refer to CP.

4.9.2.2 Subscriber

4.9.2.2.1 Physical person

Refer to CP.

4.9.2.2.2 Machine

Refer to CP.

4.9.3 Procedure for Revocation Request

Refer to CP.

4.9.3.1 RCA

Revocation of the RCA certificate requires revocation of all ICA certificate (refer to section 4.9.3.2 below) and CA certificates (refer to section 4.9.3.3 below) it has issued.

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

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

A signed naming document shall be established by PMA and transmitted to master of key ceremony to perform the key ceremony.

Security Officer is in charge of contacting activation data holder and organizes the key ceremony.

4.9.3.2 ICA and CA signed by RCA

Authorized person transmit revocation request to the PMA.

Once the PMA receives the request, it shall approve or reject this request. In case the request is approved, to member in PMA representative shall elaborate, sign a revocation request form.

The revocation request form shall contain the following information:

- Serial number of the CA and/or ICA to revoke;
- DN of the CA and/or ICA to revoke;
- DN of the issuer CA and/or ICA certificate;
- Name of the first PMA representative;
- Name of the second PMA representative;
- PMA representative company name;
- Phone number where to contact the PMA representative that signed the form within six hours for call back procedure;
- Name of the Activation data holder that will attend the key ceremony;
- Name of the PMA witness that will attend the key ceremony.

The PMA representative also has to call security officer to inform that a revocation request form was send.

Once the revocation request is received by security officer, Security officer verifies the PMA representative that signed the request has been already identified and that all information are provided. Then security officer call back the PMA representative to check that the PMA representative is the person that signed the request and that the received form is correct.

All the following operation are done in a key ceremony room in the key ceremony location (Refer to § 5.1.1). Before all the Operation on the key ceremony platform, the Key Manager has to prepare the CRL ceremony script.

To proceed to a revocation, the Key manager has to generate a new ARL with the key ceremony platform. The ARL contained the following information:

- All the CA and/or ICA certificate if it is a RCA revocation. It means all the certificate serial number of CA and/or ICA certificate has to be set in the ARL. The Key manager has to set all the CA and/or ICA certificate serial number in the ARL.
- The CA and/or ICA certificate if it is a CA and/or ICA to revoke. It means the selected certificate serial number of the CA and/or ICA certificate to be revoked has to be set in the ARL. The Key Manager has to set this CA certificate serial number in the ARL.

For the ARL generation, the Key manager prepares the key ceremony platform with the dedicated HSM and all the trusted roles with activation data has to be present for the ceremony (refer to § 6.2.6.1). Key manager restore the current valid RCA's private key in the dedicated key ceremony HSM of the key ceremony platform (refer to § 6.2.6). Key Manager generates all the ARL according the script.

PMA and Security Officer verify that the ARL generated is compliant with [CA naming] and/or revocation request. The key ceremony platform generates an attestation form for the generation of the ARL certificate. Key Manager and PMA representative signed this attestation form if the result of the verification is correct.

Key manager transmits the ARL to the PS for publication in the PS. Security Officer and trusted role of PS ensure that superseded ARL is removed from the repository of PS upon posting of the latest ARL.

At the end of the ceremony, the Key Manager deactivates the RCA key in the key ceremony HMS and takes off the HSM from the key ceremony platform and store it according rules defines in § 5.1.6.

Security Officer and all trusted roles can only leave the ceremony when they had supervised and controlled that all the operation has done correctly according this CPS.

4.9.3.3 CA

For delegated CA refer to [PKI role and Subscriber procedure].

4.9.3.4 Subscriber certificate

Refer to [PKI role and Subscriber procedure].

4.9.4 Revocation Request Grace Period

Refer to CP.

4.9.5 Timeframe within which CA Must Process the Revocation Request

Refer to CP.

4.9.6 Revocation Checking Requirements for Relying Parties

Refer to CP.

4.9.7 CRL Issuance Frequency

Refer to CP.

4.9.8 Maximum Latency for CRLs

Refer to CP.

4.9.9 Online Revocation Checking Availability

Refer to CP.

4.9.10 Online Revocation Checking Requirements

Refer to CP.

4.9.11 Other Forms of Revocation Advertisements Available

Refer to CP.

4.9.12 Special Requirements Related To Key Compromise

Refer to CP.

4.9.13 Circumstances for Suspension

Refer to CP.

4.9.14 Who can Request Suspension

Refer to CP.

4.9.15 Procedure for Suspension Request

Refer to CP.

4.9.16 Limits on Suspension Period

Refer to CP.

4.10 Certificate Status Services

Refer to CP.

4.10.1 Operational Characteristics

Refer to CP.

4.10.2 Service Availability

Refer to CP.

4.10.3 Optional Features

Refer to CP.

4.11 End Of Subscription

Refer to CP.

4.11.1 Key Escrow and Recovery

Refer to CP.

4.11.1.1 Which key pair can be escrowed

Refer to [PKI role and Subscriber procedure].

4.11.1.2 Who Can Submit a Recovery Application

Refer to [PKI role and Subscriber procedure].

4.11.1.3 Recovery Process and Responsibilities

Refer to [PKI role and Subscriber procedure].

4.11.1.4 Performing Identification and Authentication

Refer to [PKI role and Subscriber procedure].

4.11.1.5 Approval or Rejection of Recovery Applications

Refer to [PKI role and Subscriber procedure].

4.11.1.6 KEA and KRA Actions during key pair recovered

Refer to [PKI role and Subscriber procedure].

4.11.1.7 KEA and KRA Availability

Refer to [PKI role and Subscriber procedure].

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

Refer to CP.

5. FACILITY MANAGEMENT & OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location & Construction

RCA and PKI component are hosted in Thales data center protected according [Security Policy].

5.1.2 Physical Access

5.1.2.1 RCA

RCA is stored in safe and protected according [Security Policy].

5.1.2.2 ICA, CA, KEA, KRA, RA and PS

PKI components are hosted and secured according [Security Policy].

5.1.3 Power and Air Conditioning

Refer to [Security Policy].

5.1.4 Water Exposures

Refer to [Security Policy].

5.1.5 Fire Prevention & Protection

Refer to [Security Policy].

5.1.6 Media Storage

Refer to [Security Policy].

5.1.7 Waste Disposal

Refer to [Security Policy].

5.1.8 Off-Site backup

Refer to [Security Policy].

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

RCA roles are the followings:

- Holder of activation data used for RCA HSM.
- Master of key ceremony who operates the RCA private key during key ceremony.
- Witness of key ceremony.

Refer to [PKI role and Subscriber procedure] for PKI components.

5.2.2 Number of Persons Required per Task

Task	People that are technically required
RCA key generation RCA ARL Generation RCA signing key activation RCA private key backup RCA and CA (signed by CA) certificate	Several activation data holder with Thales activation data refer to [Key ceremony] for initial key activation and set of activation data required
ICA and CA key generation CA CRL Generation CA and ICA signing key activation CA and ICA private key backup during key ceremony CA and ICA private key backup in online HSM	CA trusted role only refer to [PKI role and Subscriber procedure].

5.2.3 Identification and Authentication for Each Role

Identification and authentication of all person involved during key ceremony is done according to [Security Policy] and [Key ceremony].

The identification and authentication of the person who have privileges on HSMs is assimilated to the possession of physical items (smart cards). These items are required to set up functionality on HSMs. Only cleared person can enter the key ceremony room to activate the HSM that contained the RCA private key.

For PKI component refer to [PKI role and Subscriber procedure] and [PKI Architecture].

5.2.4 Roles Requiring Separation of Duties

Refer to [Key ceremony] and to [PKI role and Subscriber procedure]

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Refer to [Security Policy].

5.3.2 Background Check Procedures

Refer to [Security Policy].

5.3.3 Training Requirements

Refer to [Security Policy].

5.3.4 Retraining Frequency and Requirements

Refer to [Security Policy].

5.3.5 Job Rotation Frequency and Sequence

Refer to [Security Policy].

5.3.6 Sanctions for Unauthorized Actions

Refer to [Security Policy].

5.3.7 Independent Contractor Requirements

Refer to [Security Policy].

5.3.8 Documentation Supplied To Personnel

Refer to [Security Policy] and [Training].

5.4 AUDIT LOGGING PROCEDURES

Refer to CP.

5.4.1 Types of Events Recorded

Thales records all given information related to RCA operation, i.e information related to RCA life cycle management.

Thales records every access to areas where RCA life cycle management operations proceed. Records are made either logically (for employees allowed to enter the areas), either manually (for person not allowed to enter the areas).

All operation regarding the RCA certificate life cycle management is video-recorded.

Each audit record includes the following:

- Type of event;
- Date and time of event;
- Result of event : success or failure (where appropriate);
- Identity of the entity and/or operator that caused the event.

Following data are recorded.

Auditable Event	Root CA level	Storage location
SECURITY AUDIT		
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	Secure area[1]
Any attempt to delete or modify the Audit logs	X	Secure area
Obtaining a third-party time-stamp	N/A	-
IDENTITY-PROOFING		
Successful and unsuccessful attempts to assume a role	X	Safe[2]
The value of *maximum number of authentication attempts* is changed	X	Safe
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	Safe
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	Safe
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	Secure area
LOCAL DATA ENTRY		
All security-relevant data that is entered in the system	X	Safe
REMOTE DATA ENTRY		
All security-relevant messages that are received by the system	N/A	-
DATA EXPORT AND OUTPUT		
All successful and unsuccessful requests for confidential and security-relevant information	X	Safe
KEY GENERATION		
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	X	Safe
PRIVATE KEY LOAD AND STORAGE		

[1] Secure area: location were access control applies,

[2] Safe: safe is located in a secure area, not all people accessing the secure area are cleared to access the safe.

Auditable Event	Root CA level	Storage location
The loading of Component private keys	X	Safe
All access to Certificate subject Private Keys retained within the CA for key recovery purposes	N/A	-
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE		
All changes to the trusted Component Public Keys, including additions and deletions	X	Safe
SECRET KEY STORAGE		
The manual entry of secret keys used for authentication	X	Safe
PRIVATE AND SECRET KEY EXPORT		
The export of private and secret keys (keys used for a single session or message are excluded)	X	Safe
CERTIFICATE REGISTRATION		
All Certificate requests	X	Safe
CERTIFICATE REVOCATION		
All Certificate revocation requests	X	Safe
CERTIFICATE STATUS CHANGE APPROVAL		
The approval or rejection of a Certificate status change request	X	Safe
CA CONFIGURATION		
Any security-relevant changes to the configuration of the Component	X	Safe
ACCOUNT ADMINISTRATION		
Roles and users are added or deleted	X	Secure area
The access control privileges of a user account or a role are modified	X	Secure area
CERTIFICATE PROFILE MANAGEMENT		
All changes to the Certificate profile	X	Safe
CERTIFICATE STATUS AUTHORITY MANAGEMENT		
All changes to the CSA profile (e.g. OCSP profile)	N/A	-
REVOCATION PROFILE MANAGEMENT		
All changes to the revocation profile	X	Safe

Auditable Event	Root CA level	Storage location
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT		
All changes to the Certificate revocation list profile	X	Safe
MISCELLANEOUS		
Appointment of an individual to a Trusted Role	X	Secure area
Designation of personnel for multiparty control	X	Secure area
Installation of the Operating System	X	Secure area
Installation of the PKI Application	X	Secure area
Installation of hardware cryptographic modules	X	Secure area
Removal of hardware cryptographic modules	X	Secure area
Destruction of cryptographic modules	X	Safe
System Start-up	X	Safe
Logon attempts to PKI Application	X	Safe
Receipt of hardware / software	X	Secure area
Attempts to set passwords	X	Safe
Attempts to modify passwords	X	Safe
Back up of the internal CA database	X	Safe
Restoration from back up of the internal CA database	X	Safe
File manipulation (e.g., creation, renaming, moving)	X	Secure area
Posting of any material to a PKI Repository	N/A	-
Access to the internal CA database	N/A	-
All Certificate compromise notification requests	X	Safe
Loading tokens with Certificates	N/A	-
Shipment of Tokens	X	Safe
Zeroizing Tokens	X	Safe
Re-key of the Component	X	Safe
CONFIGURATION CHANGES		
Hardware	X	Secure area
Software	X	Secure area

Auditable Event	Root CA level	Storage location
Operating System	X	Secure area
Patches	X	Secure area
Security Profiles	X	Secure area
PHYSICAL ACCESS / SITE SECURITY		
Personnel Access to room housing Component	X	Secure area
Access to the Component	X	Safe
Known or suspected violations of physical security	X	Secure area
ANOMALIES		
Software error conditions	X	Secure area
Software check integrity failures	N/A	-
Receipt of improper messages	N/A	-
Misrouted messages	N/A	-
Network attacks (suspected or confirmed)	N/A	-
Equipment failure	X	Safe
Electrical power outages	N/A	-
Uninterruptible Power Supply (UPS) failure	N/A	-
Obvious and significant network service or access failures	N/A	-
Violations of Certificate Policy	X	Secure area
Violations of Certification Practice Statement	X	Secure area
Resetting Operating System clock	X	Safe

For a key ceremony the logs include, but are not limited to, the following events:

- Physical access to the key ceremony room: Log by access system control. Security Officer register (id badge, name, first name and date) in log book the distribution of badge that allow access to the trust center;
- Signed [CA naming]: PMA's administrative contact retains this document and OpenTrust;
- [Key ceremony]: PMA's administrative contact retains this document and OpenTrust;
- DVD of the key ceremony;
- List, established by Security Officer, of all the attendees to the key ceremony retains by OpenTrust with copy of identity card.

OpenTrust and/or Thales have the [Key ceremony] used to generate RCA and or ICA and CA.

For PKI components, records are described in the below table:

Auditable Event	CA	CMS	RA	Storage location
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X	X	Server, computer and PKI database
Any attempt to delete or modify the Audit logs	X	X	X	Server, computer and PKI database
Obtaining a third-party time-stamp	N/A	N/A	N/A	N/A
IDENTITY-PROOFING				
Successful and unsuccessful attempts to assume a role	X	X	X	Server, computer and PKI database
The value of *maximum number of authentication attempts* is changed	N/A	N/A	N/A	Only authentication by certificate and there is no limit for the online revocation authentication
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login	X	X	X	Server and computer
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X	X	Server and computer
An Administrator changes the type of authenticator, e.g., from a password to a biometric	X	X	X	Server and computer
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system	X	X	X	Server, PKI database, computer and CA trusted role

Auditable Event	CA	CMS	RA	Storage location
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system	X	X	X	Server, computer and PKI database
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information	X	X	X	Server, computer and PKI database (authentication code is the sole confidential data)
KEY GENERATION				
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	N/A	X	N/A	Server and CMS database
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	X	X	X	Server (Front End SSL key) and PKI database (software key RA and CMS), HSM (CA) and USB key for CA backup.
All access to Certificate subject Private Keys retained within the CA for key recovery purposes	X	X	X	Server, computer and PKI database
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted Component Public Keys, including additions and deletions	X	X	X	Server, computer and PKI database
SECRET KEY STORAGE				

Auditable Event	CA	CMS	RA	Storage location
The manual entry of secret keys used for authentication	N/A	N/A	N/A	Only authentication by certificate and secret code for online revocation and unlock function (Subscriber only)
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	N/A	X	N/A	Only authentication by certificate and secret code for online revocation (Subscriber only)
CERTIFICATE REGISTRATION				
All Certificate requests	X	X	X	Server and PKI database
CERTIFICATE REVOCATION				
All Certificate revocation requests	X	X	X	Server and PKI database
CERTIFICATE STATUS CHANGE APPROVAL				
The approval or rejection of a Certificate status change request	X	X	X	Server and PKI database
CA CONFIGURATION				
Any security-relevant changes to the configuration of the Component	X	X	X	Server, computer and PKI database
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	Server, computer and PKI database
The access control privileges of a user account or a role are modified	X	X	X	Server, computer and PKI database
CERTIFICATE PROFILE MANAGEMENT				
All changes to the Certificate profile	X	N/A	X	Server and PKI database
CERTIFICATE STATUS AUTHORITY MANAGEMENT				

Auditable Event	CA	CMS	RA	Storage location
All changes to the CSA profile (e.g. OCSP profile)	N/A	N/A	N/A	There is no OCSP services
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile	X	X	X	Server and PKI database
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				
All changes to the Certificate revocation list profile	X	X	X	Server and PKI database
MISCELLANEOUS				
Appointment of an individual to a Trusted Role	X	X	X	Server, computer and PKI database and nomination form
Designation of personnel for multiparty control	X	X	X	Server and PKI database and nomination form
Installation of the Operating System	X	X	X	Server, computer and PKI database and Manuel log of the System Administrator
Installation of the PKI Application	X	X	X	Server, computer and PKI database and Manuel log of the System Administrator
Installation of hardware cryptographic modules	X	N/A	N/A	Server, computer and PKI database, Manuel log of the System Administrator and Key manager manual log
Removal of hardware cryptographic modules	X	N/A	N/A	Server and PKI database, Manuel log of the System Administrator and Key manager manual log
Destruction of cryptographic modules	X	N/A	N/A	Server and PKI database, Manuel log of the System Administrator and Key manager manual log

Auditable Event	CA	CMS	RA	Storage location
System Start-up	X	X	X	Server, computer and Manuel log of the System Administrator
Logon attempts to PKI Application	X	X	X	Server, computer and PKI database
Receipt of hardware / software	X	X	X	Server, computer and PKI database and Manuel log of the System Administrator and Key manager manual log
Attempts to set passwords	X	X	X	Server, computer and PKI database (authentication code for online revocation)
Attempts to modify passwords	X	X	X	Server, computer and PKI database
Back up of the internal CA database	X	X	X	Server, central log server and Manuel log of the System Administrator (for offline media storage) and Key manager manual log (for offline media storage)
Restoration from back up of the internal CA database	X	X	X	Server and and Manuel log of the System Administrator (for offline media storage) and Key manager manual log (for offline media storage)
File manipulation (e.g., creation, renaming, moving)	X	X	X	Server and computer
Posting of any material to a PKI Repository	X	X	X	Server, computer and PKI database
Access to the internal CA database	X	X	X	Server and PKI database
All Certificate compromise notification requests	X	X	X	Server and PKI database and Manuel log Key manager

Auditable Event	CA	CMS	RA	Storage location
Loading tokens with Certificates	X	X	X	Server and PKI database
Shipment of Tokens	X	N/A	N/A	Manuel log CA trusted role
Zeroizing Tokens	X	X	N/A	Manuel log CA trusted role and CMS
Re-key of the Component	X	X	X	Server and PKI database
CONFIGURATION CHANGES				
Hardware	X	X	X	Manuel log of the System Administrator
Software	X	X	X	Server, computer and Manuel log of the System Administrator
Operating System	X	X	X	Server, computer and Manuel log of the System Administrator
Patches	X	X	X	Server, computer and Manuel log of the System Administrator
Security Profiles	X	X	X	Server, computer and Manuel log of the System Administrator
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to room housing Component	X	X	X	Manuel log and physical access control log
Access to the Component	X	X	X	physical access control log
Known or suspected violations of physical security	X	X	X	physical access control log
ANOMALIES				
Software error conditions	X	X	X	Server and computer
Software check integrity failures	X	N/A	X	Integrity software
Receipt of improper	X	X	X	Server and computer

Auditable Event	CA	CMS	RA	Storage location
messages				
Misrouted messages	X	X	X	Server
Network attacks (suspected or confirmed)	X	X	X	Server and computer
Equipment failure	X	X	X	Log from System Administrator
Electrical power outages	X	X	X	Server, computer and log from System Administrator
Uninterruptible Power Supply (UPS) failure	X	X	X	Server, computer and log from System Administrator
Obvious and significant network service or access failures	X	X	X	Server, computer and log from System Administrator
Violations of Certificate Policy	X	X	X	Server, computer and log from System Administrator and OA Administrator
Violations of Certification Practice Statement	X	X	X	Server, computer and log from System Administrator and OA Administrator
Resetting Operating System clock	X	X	X	Server, computer and manual log for System Administrator (but it is forbidden to do it by default, only NTP synchronize servers)

All the log and data stored on the server and PKI database are backup on a dedicated server and/or on offline media storage as described after in chapter 5.4.2 to 5.4.6.

The location storage are the following:

- Manual log of the System Administrator: server;
- Physical access control log: physical access control server.

5.4.2 Frequency of Processing Audit Logs

Refer to [Security Policy] and [PKI Architecture].

For RCA audit log, they are only review during audit.

5.4.3 Retention Period for Audit Logs

Refer to [Security Policy].

5.4.4 Protection of Audit Logs

Refer to [Security Policy] and [PKI Architecture].

5.4.5 Audit logs are not modified.

Refer to [Security Policy] and [PKI Architecture].

5.4.6 Audit Log Backup Procedures

Refer to [Security Policy] and [PKI Architecture].

5.4.7 Audit Collection System (internal vs. external)

For RCA, audit log are produced only for and during key ceremony. They are collected by witness during key ceremony and by security officer for authentication and access to activation data of HSM.

Refer to [Security Policy] and [PKI Architecture].

5.4.8 Notification to Event-Causing Subject

Refer to [Security Policy] and [PKI Architecture].

5.4.9 Vulnerability Assessments

Refer to [Security Policy] and [PKI Architecture].

5.4.10 Real time monitoring and notification

Refer to [Security Policy] and [PKI Architecture].

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

Refer to CP.

5.5.2 Retention Period for Archive

Refer to [Security Policy].

5.5.3 Protection of Archive

Refer to [Security Policy].

5.5.4 Archive Backup Procedures

Refer to [Security Policy].

5.5.5 Requirements for Time-Stamping of Records

Refer to [Security Policy].

5.5.6 Archive Collection System (internal or external)

Refer to [Security Policy].

5.5.7 Procedures to Obtain & Verify Archive Information

Refer to [Security Policy].

5.6 KEY CHANGEOVER

Refer to CP.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Refer to [Security Policy].

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

Refer to [Security Policy].

5.7.3 Private Key Compromise Procedures

Refer to [Security Policy].

5.7.4 Business Continuity Capabilities after a Disaster

Refer to [Security Policy].

5.8 PKI COMPONENT TERMINATION

5.8.1 RCA

Refer to [Security Policy].

5.8.2 ICA and CA

Refer to [Security Policy].

5.8.3 Others PKI components

Refer to [Security Policy].

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 RCA

Refer to [Key ceremony].

6.1.1.2 ICA and CA

Refer to [PKI role and Subscriber procedure]

6.1.1.3 Subscriber

6.1.1.3.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.1.1.3.2 Machine

Refer to [PKI role and Subscriber procedure].

6.1.2 Private Key Delivery to Subscriber

6.1.2.1.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.1.2.1.2 Machine

Refer to [PKI role and Subscriber procedure].

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 RCA, ICA and CA

Refer to CP.

6.1.3.2 Subscriber

Refer to [PKI role and Subscriber procedure].

6.1.4 CA Public Key Delivery to Relying Parties

Refer to CP.

6.1.5 Key Sizes

Refer to [CA naming] and [Subscriber naming].

6.1.6 Public Key Parameters Generation and Quality Checking

Refer to [Key ceremony] and [PKI role and Subscriber procedure].

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

Refer to [CA naming] and [Subscriber naming].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Refer to [Key ceremony] and [PKI role and Subscriber procedure].

6.2.2 Private Key Multi-Person Control

6.2.2.1 RCA, ICA and CA

RCA private key is protected using multi-person control (refer to [Key ceremony]) performing duties associated with their trusted roles. Trusted person attending and participating to a private key activation are strongly authenticated.

A key contained in a HSM can only be exported in a back file form (see section 6.2.6).

RCA private key only exist in backup (Cf. § 6.2.4) form when it is not used for a key ceremony.

RCA private key is physically stored in a storage location that requires at a minimum participation of three trusted employee in trusted roles to access it, according to [Security Policy].

Distribution of activation data is made to Thales trusted employee in the shareholder trusted role pool (refer to [Key ceremony]).

To use a backup file of RCA key it is necessary to initialize a HSM, on an off-line dedicated computer for key ceremony, with Thales cryptographic trusted domain, created during a key ceremony (refer to [Key ceremony]), in order to use the RCA key in the HSM.

Therefore to use the RCA private keys inside a HSM, it is necessary to have activation data created during key ceremony in order to initialize the HSM (see section 6.2.8).

After the initialization of the HSM, the RCA key has to be inserted in the HSM to be used (Cf. § 6.2.6).

A key contained in a HSM can only be exported in a backup file format (Cf. § 6.2.6). The key has to be destroyed in the HSM (see section 6.2.10) after the end of an operation with RCA key, therefore the RCA key is always under multiple controls.

ICA and CA private key is activated in HSM using multi-person control (refer to [Key ceremony]) performing duties associated with their trusted roles. Trusted person attending and participating to a private key activation are strongly authenticated. Once, ICA and CA key are in the HSM, they are used by OpenTrust CA software only.

ICA and CA private key backup is physically stored in a storage location (safe) that requires at a minimum participation of one trusted employee in trusted roles to access it, according to [Security Policy].

Distribution of activation data is made to Thales trusted employee in the activation data holder trusted role.

To use a backup file of ICA and CA key it is necessary to initialize a HSM, with cryptographic trusted domain, created during a key ceremony (refer to [PKI role and Subscriber procedure]), in order to use the CA and ICA key in the HSM.

Therefore to use the ICA and CA private keys inside a HSM, it is necessary to have activation data created during key ceremony in order to initialize the HSM (see section 6.2.8).

After the initialization of the HSM, the ICA and CA key has to be inserted in the HSM to be used (Cf. § 6.2.6).

When the HSM is personalized with this trusted domain, and is on-line, the keys can only be imported or exported from the HSM (refer to § 6.2.6) and are stored in an encrypted file stored in the OpenTrust CA software server.

6.2.2.2 Subscriber

6.2.2.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.2.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.2.3 Private Key Escrow

6.2.3.1 RCA, ICA and CA

Refer to CP.

6.2.3.2 Subscriber

Refer to [PKI role and Subscriber procedure].

6.2.4 Private Key Backup

6.2.4.1 RCA, ICA and CA

RCA private keys are backed-up under multi-person control for disaster recovery purposes only. RCA private key back-ups are generated during key ceremony, back-ups are rapidly transferred to Thales offsite secure storage location to maintain and provide RCA disaster recovery capability. Back-ups of private keys are stored applying security measures at least equivalent to these applied to primary private key, [Security Policy] document conditions apply.

RCA privates keys are back-up on several files contained in several media stored in safe (refer to [Key ceremony] and [Security Policy]). The key are ciphered, and to use the keys it is necessary to insert it in a HSM (refer to § 6.2.6).

ICA and CA private keys are backed-up under multi-person control for disaster recovery purposes only. CA private key back-ups are generated during key ceremony, back-ups are rapidly transferred to Thales offsite secure storage location to maintain and provide ICA and CA disaster recovery capability. Back-ups of private keys are stored applying security measures at least equivalent to these applied to primary private key, [Security Policy] document conditions apply.

ICA and CA privates keys are back-up on several files contained in several media stored in safe (refer to [Key ceremony] and [Security Policy]). The key are ciphered, and to use the keys it is necessary to insert it in a HSM (refer to § 6.2.6).

6.2.4.2 Subscriber

6.2.4.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.4.2.2 Machine

Refer to [PKI role and Subscriber procedure].

6.2.5 Private Key Archival

6.2.5.1 RCA, ICA and CA

Refer to CP.

6.2.5.2 Subscriber

Refer to [PKI role and Subscriber procedure].

6.2.6 Private Key Transfer into or from a Cryptographic Module

6.2.6.1 RCA, ICA and CA

RCA private keys are generated in HSMs during key ceremony. RCA key can only be export from the HSM in encrypted form (Cf. § 6.2.4). This operation can only be done during key ceremony. At the end of a key ceremony, the RCA key is destroyed in the HSM. The operation to restore keys in an encrypted format in a HSM requires the use of activation data in order to initialize the HSM (Cf. § 6.2.8). All these operations can be done only during key ceremony under video recording, following a technical key ceremony script and in the presence of PMA witness. Transfer into or from a HSM is realized by the key manager only in the key ceremony room (cf. § 6.1).

ICA and CA private keys are generated in HSMs during key ceremony. ICA and CA key can only be export from the HSM in encrypted form (Cf. § 6.2.4). This operation can only be done during key ceremony.

The operation to restore keys in an encrypted format in a HSM is performed by HSM functionality.

6.2.6.2 Subscriber

6.2.6.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.6.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 RCA, ICA and CA

Refer to [Key ceremony] and [PKI role and Subscriber procedure].

6.2.7.2 Subscriber

6.2.7.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.7.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.2.8 Method of Activating Private Key

6.2.8.1 RCA, ICA and CA

Activation proceeds on PMA authority request only to sign a certificate, revoke a certificate or generate an ARL. Activation requires all necessary activation data and RCA private key backup files to be retrieved from storage location (Cf. § 6.2.4 an § 6.2.6). Access to storage location requires at least one security officer and one Safe access officer. Activation can only be done in the key ceremony room.

To activate the key contained in a HSM, multiple activation data and RCA private key backup are required (refer to [Key ceremony] for initial key activation and set of activation data required).

Activation is proceeded on PMA authority request only to authorized CA trusted role to create ICA and CA private in on-line HSM (§ 6.2.4 an § 6.2.6) in order to sign subscriber and CA certificate and revoke subscriber and CA certificate. When an ICA and CA private key is in the HSM in the data center, the CA software only activates technically the ICA and CA private key in order to sign the CA and Subscriber certificate and revoke the CA and Subscriber certificate on request made by CA trusted role. CA software is only used by authorized trusted roles (refer to [PKI role and Subscriber procedure]) that is authorized to send CA and Subscriber certificate request and CA and Subscriber revocation request.

6.2.8.2 Subscriber

6.2.8.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.8.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.2.9 Methods of Deactivating Private Key

6.2.9.1 RCA

RCA private key is deactivated at the end of each key ceremony. The HSM used for key ceremony purposes is switched off, the RCA keys it contains are erased using the HSM internal functionalities (Cf. § 6.2.10).

6.2.9.2 ICA and CA

ICA and CA private key are stored in on-line HSM and server used by CA software to be continuously activated. In case the usage of an ICA and CA key stored in the HSM and in the CA software server is not any more required, the corresponding CA and ICA key private key will be destroyed (Cf. § 6.2.10). In case the HSM has to be remove, for termination reason, from the PKI platform, then all the key inside the HSM and in the server are destroyed (Cf. § 6.2.10).

6.2.9.3 Subscriber

6.2.9.3.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.9.3.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.2.10 Method of Destroying Private Key

6.2.10.1 RCA, ICA and CA

A normal operation of destruction of RCA key inside a HSM is made during key ceremony by the Key manager. This operation uses the functionality of the HSM.

If the RCA private key has to be destroyed because of the end of RCA certificate lifetime, then the destruction operation of RCA private key is made on PMA request.

Destruction is made during a dedicated key ceremony and requires that all back-up copies of RCA keys (Cf. § 6.2.4) are erased. This operation is made by the Key manager under the control of PMA witness and security Officer. This operation is video recorded and done in the key ceremony room.

If the RCA private key and the RCA trusted domain have to be destroyed, then the destruction operation of RCA private key and RCA trusted domain is made on PMA request. This operation is made by the Key manager under the control of PMA witness and security Officer. This operation requires the presence of the activation data holder that have the activation data card (Cf. § 6.2.2).

In this case, the operation consists in:

- Physical destruction of the smart card of the RCA activation data domain;
- Destruction of all the backup files of the RCA private key.

This operation is video recorded and done in the key ceremony room.

If the CA or ICA private key has to be destroyed because of the end of CA or ICA certificate lifetime, then the destruction operation of CA or ICA private key is made on PMA request. Deletion of private keys of a CA or ICA is realized by the CA trusted role (refer to [PKI role and Subscriber procedure]) using HSM interface.

The CA or ICA key are selected in the HSM using CA certificate associated to the private key to be destroyed. After deletion of the key(s) on the HSM, a new backup files has to be created and backed up (refer to section 6.2.4). Destruction is made during a dedicated key ceremony and requires that all back-up copies of CA or ICA keys (Cf. § 6.2.4) are erased. This operation is made by the CA trusted role (refer to [PKI role and Subscriber procedure]).

6.2.10.2 Subscriber

6.2.10.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.2.10.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

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.

6.3.2 Certificate Operational Periods/Key Usage Periods

6.3.2.1 RCA

Refer to CP.

6.3.2.2 ICA

Refer to CP.

6.3.2.3 CA

Refer to CP.

6.3.2.4 Subscriber

Refer to CP.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 RCA, ICA and CA

Thales trusted cryptographic domain had been created during the initial key ceremony of the ACR. Activation data are kept during all RCA operation, including new key pair generation. Activation data are stored on smart cards. Activation data are provided to their activation data holders during a face to face meeting at the end of the initial key ceremony. Installation of activation data requires their activation holders to participate and bring their smart cards. Refer to [Key ceremony].

ACR activation data are stored in safe in according to [Security Policy].

ACS trusted cryptographic domain had been created during the initial key ceremony of the AC and ICA. Activation data are stored on smart cards. Activation data are provided to their activation data holders during a face to face meeting at the end of the initial key ceremony. Installation of activation data requires their activation holders to participate and bring their smart cards.

For ICA and CA, refer to [PKI Architecture] and [PKI role and Subscriber procedure].

6.4.1.2 Subscriber

6.4.1.2.1 Physical person

Refer to [PKI role and Subscriber procedure].

6.4.1.2.2 Machine

Refer to [PKI role and Subscriber procedure].

6.4.2 Activation Data Protection

6.4.2.1 RCA, ICA 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 and/or External Entity, according the owner of the CA, 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 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 person

Refer to [PKI role and Subscriber procedure].

6.4.2.2.2 Technical Contact

Refer to [PKI role and Subscriber procedure].

6.4.3 Other Aspects of Activation Data

6.4.3.1 RCA, ICA and CA

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending 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

Refer to [PKI role and Subscriber procedure].

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Refer to [PKI Architecture] and [Security Policy].

6.5.2 Computer Security Rating

Refer to [PKI Architecture] and [Security Policy].

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

Refer to [PKI Architecture] and [Security Policy].

6.6.2 Security Management Controls

Refer to [PKI Architecture] and [Security Policy].

6.6.3 Life Cycle Security Controls

Refer to [PKI Architecture] and [Security Policy].

6.7 Network Security Controls

6.7.1 RCA

Refer to [PKI Architecture] and [Security Policy].

6.7.2 Online PKI component

Refer to [PKI Architecture] and [Security Policy].

6.8 Time Stamping

Refer to [PKI Architecture] and [Security Policy].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

Refer to [CA naming] and [Subscriber naming].

7.1.2 Certificate Extensions

Refer to [CA naming] and [Subscriber naming].

7.1.3 Algorithm Object Identifiers

Refer to [CA naming] and [Subscriber naming].

7.1.4 Name Forms

Refer to [CA naming] and [Subscriber naming].

7.1.5 Certificate Policy Object Identifier

Refer to [CA naming] and [Subscriber naming].

7.1.6 Policy Qualifiers Syntax and Semantics

Refer to [CA naming] and [Subscriber naming].

7.1.7 Processing Semantics for the Critical Certificate Policy Extension

Refer to [CA naming] and [Subscriber naming].

7.2 CRL PROFILE

7.2.1 Version Numbers

Refer to [CA naming] and [Subscriber naming].

7.2.2 CRL and CRL Entry Extensions

Refer to [CA naming] and [Subscriber naming].

7.3 OCSP PROFILE

7.3.1 Version Number

Refer to CP.

7.3.2 OCSP Extensions

Refer to CP.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENT

Refer to CP.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS

Refer to [Security Policy] and [KC audit report].

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

Refer to [Security Policy] and [KC audit report].

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Refer to [Security Policy] and [KC audit report].

8.4 TOPICS COVERED BY ASSESSMENT

Refer to [Security Policy] and [KC audit report].

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Refer to [Security Policy] and [KC audit report].

8.6 COMMUNICATION OF RESULTS

Refer to [Security Policy] and [KC audit report].

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance and Renewal Fees

Refer to CP.

9.1.2 Certificate Access Fees

Refer to CP.

9.1.3 Revocation or Status Information Access Fees

Refer to CP.

9.1.4 Fees for Other Services

Refer to CP.

9.1.5 Refund Policy

Refer to CP.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

Refer to CP.

9.2.2 Other Assets

Refer to CP.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to CP.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Refer to [Security Policy].

9.4 PRIVACY OF PERSONAL INFORMATION

Refer to [Security Policy].

9.5 INTELLECTUAL PROPERTY RIGHTS

Refer to [Security Policy].

9.5.1 Property Rights in the CPS

Refer to [Security Policy].

9.5.2 Property Rights in Names

Refer to CP.

9.5.3 Property Rights in Keys

Refer to CP.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

9.6.1.1 Policy Management Authority

Refer to CP.

9.6.1.2 Root Certification Authority (RCA)

Refer to CP.

9.6.1.3 Intermediate Certification Authority (ICA)

Refer to CP.

9.6.1.4 Certification Authority (CA)

Refer to CP.

9.6.1.5 Registration Authority

Refer to CP.

9.6.1.6 TMA

Refer to CP.

9.6.1.7 Operational Authority

Refer to [Security Policy].

9.6.1.8 LRA

Refer to CP.

9.6.2 KRA

Refer to CP.

9.6.3 KEA

Refer to CP.

9.6.4 Subscriber: physical person

Refer to CP.

9.6.5 Subscriber: machine

Refer to CP.

9.6.6 Representations and Warranties of Other Participants

9.6.6.1 External Entity

Refer to CP.

9.6.6.2 Relying Party

Refer to CP.

9.7 DISCLAIMERS OF WARRANTIES

Refer to CP.

9.8 LIMITATIONS OF LIABILITIES

Refer to CP.

9.9 INDEMNITIES

Refer to CP.

9.10 TERM AND TERMINATION

9.10.1 Term

Refer to CP.

9.10.2 Termination

Refer to CP.

9.10.3 Effect of Termination and Survival

Refer to CP.

9.11 Individual Notices and Communications with Participants

Refer to CP.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to CP.

9.12.2 Notification Mechanism and Period

Refer to CP.

9.12.3 Circumstances under Which OID Must be changed

Refer to CP.

9.13 Dispute Resolution Provisions

Refer to CP.

9.13.1 Disputes among Thales domain

Refer to CP.

9.13.2 Alternate Dispute Resolution Provisions

Refer to CP.

9.14 Governing Law

Refer to CP.

9.15 Compliance with Applicable Law

Refer to CP.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Refer to CP.

9.16.2 Assignment

Refer to CP.

9.16.3 Severability

Refer to CP.

9.16.4 Waiver of Rights

Refer to CP.

9.16.5 Force Majeure

Refer to CP.

9.17 Other Provisions

Refer to CP.

10. CERTIFICATE PROFILES

Refer to [CA naming] and [Subscriber naming].

11. REFERENCED DOCUMENTS

Reference	Document
[CA naming]	OpenTrust_DMS_Thales_Naming_Document_v1.12S_Signed
[Subscriber naming]	TBD
[KC audit report]	A1300003638 OpenTrust Thales - Key Ceremony Findings Report – DRAFT
[Key ceremony]	- OpenTrust_DMS_Thales_KC_Preparation_Guide_v1.30 - Script_KC_THALES_V3 1.0
[PKI role and Subscriber procedure]	New PKI Roles and Processes - v 1.3
[PKI Architecture]	PKIv3-TASD_Production-Platform_v002
[Training]	- Formation Operateurs FR - Formation PKI - Operators Training EN - PKI Training
[Security Policy]	87203860-INF-GRP-EN Group IS Security Policy

End of document