



SCOOP@F Certificate Policy

Deliverable 2.4.4.9

Activity 2: Studies

Sub-activity 2.4 > Specifications

Version 3.00

Publication date: 21/01/2019



Co-financed by the Connecting Europe
Facility of the European Union

Information on the document

Document: Scoop@F Certificate Policy

Date of publication: 21/01/2019

Responsible, Entity: IDnomic, TelecomParisTech, Renault, PSA and French Ministry in charge of Transport

Status: Version 3.00 – Approved

Publication History

Version	Date	Contributor(s)	Updates & changes	Diffusion
3.00	21/01/2019	Telecom ParisTech + IDNOMIC	Consolidation of the deliverable for release 3: Harmonization of key words	Release 3

Reference to the version administration

Version number to be composed of 3 digits > vR.XY

- **R** corresponds to the release number: it is upgraded each time SC Studies validates the diffusion of a new release,
- **X** is the major version number: it is upgraded each time SC Studies validates the deliverable,
- **Y** is the minor version number: it is upgraded each time a contributor changes anything.

Once the deliverable is approved, its version number is upgraded from vR.XY to vR.(X+1)0

Once the deliverable is release, its version number is upgraded from vR.XY to v(R+1).00

As illustration:

- 0.03 > Work in progress version
- 0.10 > Del. Approved by SC Studies but not released
- 2.00 > Del. approved & released (in release 2)
- 2.05 > Del. Updated - in progress version

Table of Contents

1.	Introduction	10
1.1	Definitions and Acronyms	10
1.1.1	Definitions	10
1.1.2	Acronyms	15
1.1.3	References	17
1.2	Overview	17
1.3	Document Name and Identification	18
1.4	PKI Components	18
1.4.1	Policy Management Authority (PMA)	19
1.4.2	Root Certificate Authority (RCA)	19
1.4.3	Long Term Certification Authority (LTCA)	20
1.4.5	Pseudonym Certification Authority (PCA)	22
1.4.6	Operational Authority (OA)	23
1.4.7	Distribution Center (DC)	23
1.4.8	Other Participants	23
1.5	Certificate and Private Key Usage	25
1.5.1	Appropriate Certificate Use	25
1.5.2	Prohibited Certificate Use	26
1.6	Policy Administration	26
1.6.1	Organization Administering the Document	26
1.6.2	CPS Approval Procedures	26
2.	Publication and Repository Responsibilities	27
2.1.	Repositories	27
2.1.1.	RCA and DC URL	27
2.1.2.	CRL signed by RCA	28
2.2.	Publication of Certification Information	28
2.3.	Time or Frequency of Publication	28
2.4.	Access Controls on Repositories	29
3.	Identification and Authentication	30
3.1.	Naming	30
3.1.1.	Types of Names	30

3.1.2.	Need for Names to Be Meaningful	30
3.1.3.	Anonymity or Pseudonymity of Certificate	31
3.1.4.	Rules for Interpreting Various Name Forms	31
3.1.5.	Uniqueness of Names	31
3.1.6.	Recognition, Authentication, and Role of Trademarks	31
3.2.	Initial Identity Validation.....	31
3.2.1.	Method to Prove Possession of Private Key	31
3.2.2.	Authentication of Organization Identity	32
3.2.3.	Authentication of Physical Person Identity	33
3.2.4.	Validation of Authority	34
3.2.5.	Non-Verified Subscriber Information	34
3.2.6.	Criteria for Interoperation	34
3.3.	Identification and Authentication for Re-key Requests.....	35
3.3.1.	Identification and Authentication for Routine Re-key.....	35
3.3.2.	Identification and Authentication for Re-key After Revocation/Deactivation	35
3.3.3.	Identification and Authentication for Revocation/Deactivation Request.....	35
3.3.3.1.	RCA, LTCA and PCA for CA certificate	35
3.3.3.2.	LTC	35
3.3.3.3.	PC	35
4.	Certificate Life-Cycle Operational Requirements.....	36
4.1.	Certificate Application.....	36
4.1.1.	Who Can Submit a Certificate Application?.....	36
4.1.2.	Enrollment Process and Responsibilities	36
4.2.	Certificate Application Processing	38
4.2.1.	Performing Identification and Authentication Functions.....	38
4.2.2.	Approval or Rejection of Certificate Applications.....	39
4.2.3.	Time to Process Certificate Applications	40
4.3.	Certificate Issuance.....	41
4.3.1.	CA Actions during Certificate Issuance	41
4.3.2.	Notification to Subscriber by the CA of Issuance of Certificate	42
4.4.	Certificate Acceptance	42
4.4.1.	Conducting Certificate Acceptance	42
4.4.2.	Publication of the Certificate by the DC.....	42
4.4.3.	Notification of Certificate Issuance by the CA to Other Entities	42
4.5.	Key Pair and Certificate Usage	43
4.5.1.	Private Key and Certificate Usage.....	43

4.5.2.	Relying Party Public Key and Certificate Usage	43
4.6.	Certificate Renewal	43
4.7.	Certificate Re-key	43
4.7.1.	RCA	43
4.7.2.	LTCA and PCA	43
4.7.3.	LTC	43
4.7.4.	PC	44
4.8.	Certificate Modification	44
4.9.	Certificate Revocation and Suspension and ITS deactivation	44
4.9.1.	Circumstances for revocation or deactivation	44
4.9.2.	Who Can Request Revocation or Deactivation	45
4.9.3.	Revocation and Deactivation Request Procedure	46
4.9.4.	Revocation and Deactivation Request Grace Period	47
4.9.5.	Timeframe within which the Revocation and/or Deactivation Request Must be Processed	47
4.9.6.	Revocation and Deactivation Checking Requirement for Relying Parties	48
4.9.7.	CRL and deactivation status Issuance Frequency	48
4.9.8.	Maximum Latency for CRLs and deactivation status	49
4.9.9.	On-line Revocation/Deactivation Status Checking Availability	49
4.9.10.	On-line Revocation/Deactivation Checking Requirements	49
4.9.11.	Other Forms of Revocation/Deactivation Advertisements Available	49
4.9.12.	Specific Requirements in the Event of Private Key Compromise	49
4.9.13.	Suspension	50
4.10.	Certificate Status Services	50
4.10.1.	Operational Features	50
4.10.2.	Service Availability	50
4.11.	End of Subscription	50
4.12.	Key Escrow and Recovery	51
4.12.1.	Subscriber	51
4.12.2.	Session Key Encapsulation and Recovery Policy and Practices	51
5.	Facility, Management and Operational Controls	52
5.1.	Physical Controls	52
5.1.1.	Site Location and Construction	52
5.1.2.	Physical Access	53
5.1.3.	Power and Air Conditioning	54
5.1.4.	Water Exposures	54

5.1.5.	Fire Prevention and Protection	54
5.1.6.	Media Storage	54
5.1.7.	Waste Disposal	55
5.1.8.	Off-site Backup.....	55
5.2.	Procedural Controls.....	55
5.2.1.	Trusted Roles	55
5.2.2.	Number of Persons Required per Task	56
5.2.3.	Identification and Authentication for Each Role	57
5.2.4.	Roles Requiring Segregation of Duties	57
5.3.	Personnel Controls.....	57
5.3.1.	Qualifications, Experience, and Clearance Requirements	57
5.3.2.	Background Check Procedures.....	57
5.3.3.	Training Requirements	58
5.3.4.	Retraining Frequency and Requirements	58
5.3.5.	Job Rotation Frequency and Sequence	58
5.3.6.	Sanctions for Unauthorized Actions	58
5.3.7.	Independent Contractor Requirements	58
5.3.8.	Documentation Supplied to Personnel	58
5.4.	Audit Logging Procedures	59
5.4.1.	Types of Events Recorded	59
5.4.2.	Log Processing Frequency.....	60
5.4.3.	Retention Period for Audit Logs.....	60
5.4.4.	Protection of Audit Log	60
5.4.5.	Audit Log Backup Procedures	60
5.4.6.	Audit Collection System (Internal vs. External)	60
5.4.7.	Event-Causing Subject Notification	61
5.4.8.	Vulnerability Assessments	61
5.5.	Records Archival	61
5.5.1.	Types of Records Archived	61
5.5.2.	Archive Retention Period.....	62
5.5.3.	Archive Protection	62
5.5.4.	Archive Backup Procedures	62
5.5.5.	Requirements for Record Time-Stamping	62
5.5.6.	Archive Collection System (Internal or External)	63
5.5.7.	Procedures to Obtain and Verify Archive Information.....	63
5.6.	Key Changeover.....	63

5.6.1.	RCA.....	63
5.6.2.	CA Certificate	63
5.7.	Compromise and Disaster Recovery.....	63
5.7.1.	Incident and Compromise Handling Procedures	63
5.7.2.	Corruption of Computing Resources, Software, and/or Data	64
5.7.3.	Entity Private Key Compromise Procedures	64
5.7.4.	Business Continuity Capabilities after Disaster	65
5.8.	Termination and transfer	65
5.8.1.	RCA.....	65
5.8.2.	CA	65
6.	Technical Security Controls	66
6.1.	Key Pair Generation and Installation	66
6.1.1.	Key Pair Generation	66
6.1.2.	Private Key Delivery	67
6.1.3.	Public Key Delivery to Certificate Issuer.....	67
6.1.4.	RCA Public Key Delivery to Relying Parties	68
6.1.5.	Key Sizes and cryptographic algorithm	68
6.1.6.	Public Key Parameters Generation and Quality Checking	69
6.1.7.	Key Usage Purpose	69
6.2.	Private Key Protection and Cryptographic Module Engineering Controls.....	69
6.2.1.	Cryptographic Module Standards and Controls.....	69
6.2.2.	Private Key (N out of M) Multi-Person Control.....	70
6.2.3.	Private Key Escrow	70
6.2.4.	Private Key Backup	70
6.2.5.	Private Key Archival	71
6.2.6.	Private Key Transfer into or from a Cryptographic Module.....	71
6.2.7.	Private Key Storage on Cryptographic Module	72
6.2.8.	Method of Activating Private Key.....	72
6.2.9.	Method of Deactivating Private Key	73
6.2.10.	Method of Destroying Private Key	74
6.2.11.	Cryptographic Module Rating	74
6.3.	Other Aspects of Key Pair Management	75
6.3.1.	Public Key Archival.....	75
6.3.2.	Certificate Operational Periods and Key Pair Usage Periods.....	75
6.4.	Activation Data	76
6.4.1.	Activation Data Generation and Installation	76

6.4.2.	Activation Data Protection	77
6.4.3.	Other Aspects of Activation Data.....	77
6.5.	Computer Security Controls	77
6.5.1.	Specific Computer Security Technical Requirements.....	77
6.5.2.	Computer Security Rating	79
6.6.	Life Cycle Technical Controls	79
6.6.1.	System Development Controls	79
6.6.2.	Security Management Controls	80
6.6.3.	Life Cycle Security Controls	80
6.7.	Network Security Controls	80
6.7.1.	RCA.....	80
6.7.2.	LTCA and PCA.....	80
6.8.	Time-Stamping	81
7.	Certificate, CRL and TSL.....	82
7.1.	Certificate Profile	82
7.1.1.	Version Number	82
7.1.2.	Certificate Content.....	82
7.1.3.	Algorithm Object Identifiers	83
7.1.4.	Name Form	83
7.1.5.	Name Constraints.....	83
7.1.6.	Certificate Policy Object Identifier.....	83
7.1.7.	Usage of Policy Constraints Extension.....	83
7.1.8.	Policy Qualifiers Syntax and Semantics	83
7.1.9.	Processing Semantics for the Critical Certificate Policy Extension.....	83
7.2.	CRL Profile	83
7.3.	TSL Profile	83
8.	Compliance Audit and Other Assessments	85
8.1.	Frequency or Circumstances of Assessment	85
8.2.	Identity/Qualifications of Assessor.....	85
8.3.	Topics Covered by Assessment.....	85
8.4.	Actions Taken as a Result of Deficiency	85
8.5.	Communication of Results	85
9.	Other Business and Legal Matters.....	86
9.1.	Fees	86
9.1.1.	Certificate Issuance or Renewal Fees.....	86
9.1.2.	Certificate Access Fees.....	86

9.1.3.	Revocation or Status Information Access Fees.....	86
9.1.4.	Fees for Other Services	86
9.1.5.	Refund Policy	86
9.1.6.	Fines List.....	86
9.2.	Financial Responsibility	86
9.3.	Confidentiality of Business Information	86
9.3.1.	Scope of Confidential Information	86
9.3.2.	Information Not Within the Scope of Confidential Information	87
9.3.3.	Responsibility to Protect Confidential Information	87
9.4.	Privacy of Personal Information	87
9.4.1.	Privacy Plan	87
9.4.2.	Information Treated as Private	87
9.4.3.	Information Not Deemed Private	87
9.4.4.	Responsibility to Protect Private Information	88
9.4.5.	Notice and Consent to use Private Information	88
9.4.6.	Disclosure Pursuant to Judicial or Administrative Process	88
9.4.7.	Other Information Disclosure Circumstances	88
9.5.	Intellectual Property Rights	88
9.6.	Representations and Warranties	88
9.7.	Disclaimers of Warranties	88
9.8.	Limitations of Liability	88
9.9.	Indemnities	89
9.10.	Term and Termination	89
9.10.1.	Term.....	89
9.10.2.	Termination	89
9.10.3.	Effect of Termination and Survival.....	89
9.11.	Individual Notices and Communications with Participants.....	89
9.12.	Amendments	89
9.12.1.	Procedure for Amendment	89
9.12.2.	Notification Mechanism and Period	90
9.12.3.	Circumstances under Which OID Must Be Changed.....	90
9.13.	Dispute Resolution Provisions.....	90
9.14.	Governing Law	90
9.15.	Compliance with Applicable Law	90
9.16.	Miscellaneous Provisions	90
9.16.1.	Force Majeure	90

1. Introduction

1.1 Definitions and Acronyms

1.1.1 Definitions

Term	Definition
Activation Data	Secret data (e.g.: password, PIN code or OTP) that is used to perform cryptographic operations using a Private Key.
Audit	An independent review and examination of documentation, records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
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.
Authentication data	Particular technical activation data (as OTP or authentication certificate) used by a Subscriber to be authenticated by Protect and Sign (Personal signature) service in order to sign a document according a Consent Protocol.
Availability	The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004]. It means that an electronic data stored using means (hard disk, paper ...) can be still readable and have the same meaning after and during its storage.
Certificate	A certificate is a data structure digitally signed by a Certification Authority.
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.
Certificate Revocation List (CRL)	A list of revoked certificates that is created and signed by an RCA. A certificate is added to the list if revoked and then removed from it when it reaches the end of the certificate's

	validity period.
Certificate Validity Period	The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate.
Certification Path (also called trusted path or trusted certification chain)	A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA Certificate (trust anchor), CA Certificate and the ITS certificates signed by the CA.
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.
Common Criteria	Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].
Cryptographic domain (for HSM)	Trusted environment that contains one or several keys and managed with dedicated activation data. This trusted environment is deployed in a Hardware Security Module (HSM) to activate and use keys.
Delegated Third Party	Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate issuance process by performing or fulfilling one or more of the CA's CP and CPS.

Disaster Recovery Plan	A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CP/CPS.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the Subscriber within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
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 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 CA keys, and in some cases the keys of some applications (Subscribers).
Hash Function	A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties: <ul style="list-style-type: none"> - It is computationally infeasible to find for a given output an input which maps to this output; - It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].
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.
Integrity	Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.
Interoperability	Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to

	undertake common or related activities.
Key Ceremony (KC)	A Key Ceremony (KC) is an operation enabling the management (generation and destruction) of cryptographic key pairs and CA life-cycle (certificate signature and revocation). A key ceremony requires a minimum number of trusted employees whom represent the owner of the PKI.
Key Generation	The process of creating a Private Key and Public Key pair.
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	Also named entity. Department, agency, partnership, trust, joint venture or other association.
PIN	Personal Identification Number. See activation data for definition
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Pseudonymity	Ability of a user to use a resource or service without disclosing its user identity while still being accountable for that use.
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 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.
Public/Private Key Pair (also named 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.
Registration	The process whereby an entity or ITS applies to a Certification Authority for a Certificate.
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.
Trusted Role	Those individuals who perform a security role that is critical to the operation or integrity of this PKI.
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.
-------------------	---

1.1.2 Acronyms

Acronym	Means
AA	Authorization Authority
CPOC	C-ITS Point of Contact
CA	Certification Authority
CAM	Cooperative Awareness Message
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
DC	Distribution Center
DENM	Decentralized Environmental Notification Message
DN	Distinguished Name
EA	Enrollment Authority
EAL	Evaluation assurance level, ISO 15408 (Common Criteria) norm for certification of security products
EC	Enrollment Credentials
ECDSA	Elliptic Curves Digital Signature Algorithm.
FIPS	United States of America, Federal Information Processing Standards

HSM	Hardware Security Module
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transport System
C-ITS-S	Cooperative Intelligent Transport System Station
R-ITS-S	ITSS-Roadside Unit
V-ITS-S	ITSS-Vehicle
LCM	Life Cycle Manager
LTC	Long Term Certificate
LTCA	Long Term Certificate Authority
NTP	Network Time Protocol (RFC 5905 for version 4)
OID	Object Identifier
PC	Pseudonym Certificate
PCA	Pseudonym Certificate Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request For Comment

SHA	Secure Hash Algorithm
TC	Trusted Contact
TLM	Trusted List Manager
TSL	Trust Service List

1.1.3References

This CP is based on:

- [SCOOP@F-PQP]: SCOOP@F Steering Committee Project Quality Plan
- [RFC3647]: "Certificate Policy and Certification Practices Framework" issued by the Internet Engineering Task Force (IETF). In compliance with the IETF RFC 3647, this CP is divided into nine parts that cover the security controls and practices and procedures for certificate within the EC C-ITS PKI. As requested in [RFC3647], section headings that are not applicable will have the statement "Not applicable."
- [ETSI-TS-102-941] v1.1.1: Achieving trust and privacy management in Intelligent Transportation Systems (ITS) requires the establishment and maintenance of trusted relationships between all C-ITS-S and authorities, which is ensured through the use of public key certificates and Public Key Infrastructure (PKI).
- [ETSI-TS-103-097] v1.2.1: defines the structure and content of all certificate covered by the present CP.
- [ISO/IEC 14516-2]: Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third-Party services
- [SCOOP. 2.4.4.5]: PKI system requirements specifications
- [SCOOP. 2.4.4.6]: PKI architecture and technical specifications (v2).

1.2 Overview

This document defines the Certificate Policy (CP) for the Public Key Infrastructure (PKI) supporting the deployment of Cooperative-Intelligent Transport System (C-ITS) in the context of SCOOP@F project.

It describes the PKI participants, the data formats and processes required for managing Certificate life cycle within deployed C-ITS.

This Certificate Policy (CP), is the principal statement of policy governing the SCOOP@F Public Key Infrastructure (PKI); it is strictly applicable in the context of SCOOP@F deployment in France during the pilot phase.

It presents the requirements, principles and procedures that PKI component implement to create and manage Root Certification Authority (RCA), Long Term Certification Authority (LTCA), Pseudonym Certification Authority (PCA), Long Term Certificate (LTC) and Pseudonym Certificate (PC).

In this CP, the term CA (Certification Authority) is used indistinctly for RCA, LTCA and/or PCA.

The CP gives the security requirements applicable to all PKI services while the associated Certification Practice Statement (CPS) give more details on practices enforced by each entity participating in the PKI activities.

The present CP represents the common requirements that RCA, LTCAs and PCAs should enforce to issue certificates.

The trusted links are built as follow:

- RCA trust common anchor: RCA certificate generated and managed by the French Ministry in charge of transport per this CP.
- LTCA certificate: certificate issued by the RCA per this CP.
- LTC certificate: certificates issued by the LTCA per this CP.
- PCA certificate: certificate issued by the RCA per this CP.
- PC certificate: certificates issued by the PCA per this CP.

SCOOP@F Root CA (RCA) certificate is available in SCOOP@F TSL (Trust Service List), to provide trust to Relying Party. Being signed by SCOOP@F RCA means that all certificates the LTCA and PCA (CA) delivers will be recognized everywhere, at any time, in the C-ITS application services with an identical level of trust.

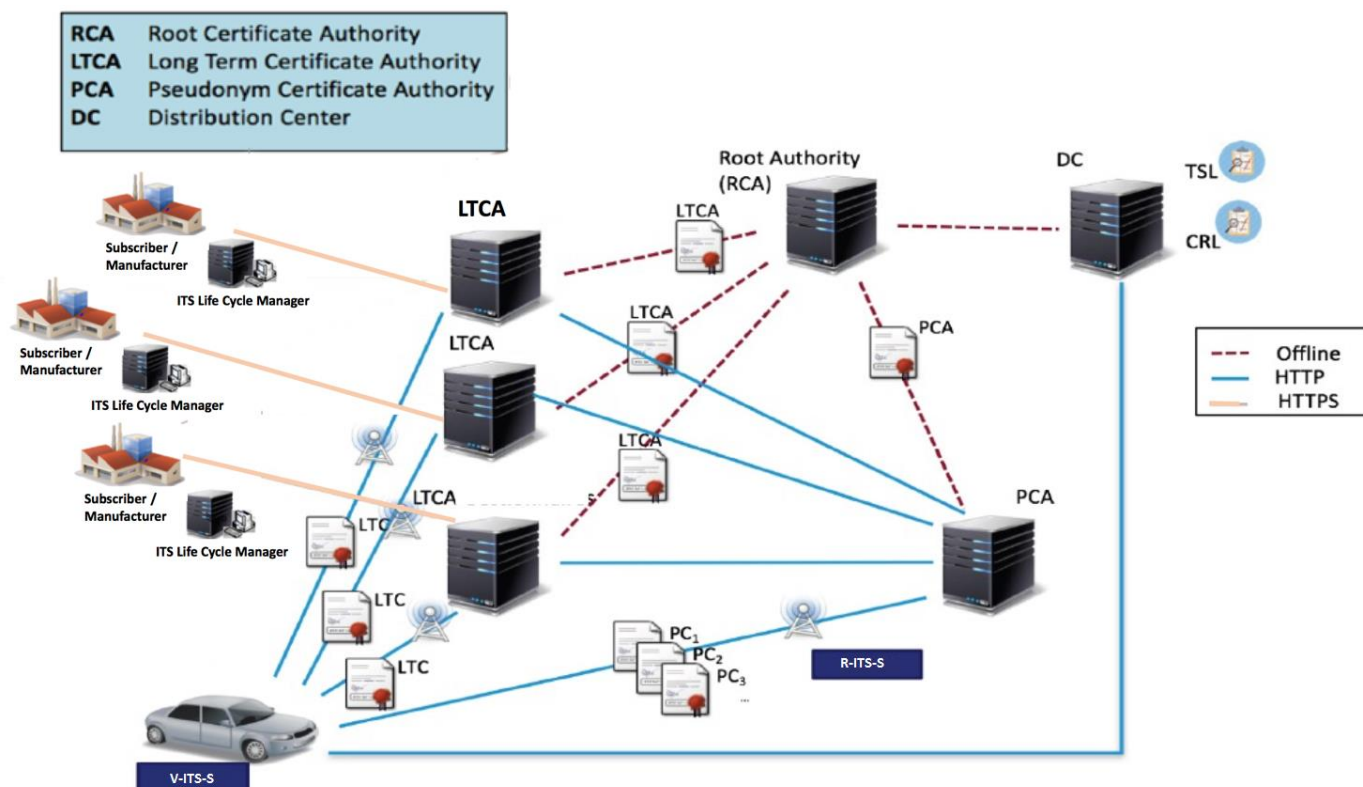
1.3 Document Name and Identification

This CP is the SCOOP@F Project property.

This CP is named "SCOOP@F Certificate Policy".

1.4 PKI Components

The PKI is composed of the components described hereafter, in compliance with the following architecture:



1.4.1 Policy Management Authority (PMA)

The PMA is the PKI lead authority and is managed by the French partners of the SCOOP@F Steering Committee (members or nominated substitutes). It is represented by the SCOOP@F Project Manager.

The PMA defines the organization of PKI components and services. It is in charge of nominating the PKI entities and verifying the compliance of the services they deliver with applicable sections of the CP and their corresponding CPS.

PMA assumes the following:

- Approves PKI services to be delivered by the PKI infrastructure;
- Approves the Certificate Policy and any potential changes
- Approves Certification Practice Statement (CPS) and any potential changes
- Approves compliance between security practice documents and related policies (for instance Certification practice);
- Approves CA creation and CA revocation;
- Approves the procedure to accept external RCA certificate;
- Approves external RCA certificate,
- Arbitrates disputes relating to the PKI services and the use of certificates and ensures that the resolution of such disputes is published;
- Ensures information contained in TSL are true and usable.
- Approves the publication of the CP, CA certificates, TSL, CRL and useful URL.
- Establishes agreement with External Entity and LTCA and PCA.

SCOOP@F Risk analysis is excluded from the scope of this CP.

PMA may perform a Risk Assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate or certificate process.
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate or certificate process.
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the PKI components implements to counter such threats.

PMA may involve external entity regarding tasks to be performed. External entity acts only for temporary mission and do not belong to PMA.

1.4.2 Root Certificate Authority (RCA)

RCA designates the RCA for SCOOP@F ITS services and infrastructure.

The Direction Générale des Infrastructures, des Transports et de la Mer (DGITM) is the RCA owner.

A RCA is a CA characterized by having a self-signed certificate (issuer and signer is the same). RCA can't be revoked in a normal manner (i.e. being included in a Certificate Revocation List), and, when used as a Trust Anchor, must be transmitted or made available to any Relying Parties by secured mechanisms outlined in section 6.1.4.

A RCA is represented by an authorized person named “Authorized Representative”. The Authorized Representative is appointed by the PMA.

RCA is always used offline and never connected to any network. The RCA certificate is self-signed. RCA never receives a certificate from another CA (never certified or cross-certified with another external CA).

The RCA supports the following PKI services:

- Generation of Root CA key pair and self-signed certificate.
- Generation of CA key pairs and certificates.
- Signature of TSL and CRL.
- Revocation of CA certificates.
- Update the CRL/TSL
- Rekey of CA certificates.
- Log trail generation.

The RCA has the responsibility to:

- 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).
- 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.

1.4.3 Long Term Certification Authority (LTCA)

LTCAs are either owned by an entity designated by PMA and/or by an external legal entity for C-ITS services. RCA can sign several LTCA certificates.

LTCA has the responsibility to:

- Manage C-ITS-S status.
- Sign LTC certificate.
- Authenticate PCA using TSL signed by RCA that has signed LTCA.
- Manage PCA validation request for PC certificate request.
- Protect and guarantee integrity and confidentiality of its activation data and/or private key.
- Only use its 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).
- Realize internal audit of the PKI component used by CA to manage Certificate.
- Document its internal procedures to complete its 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 establish between CA's entity and PMA.

- Transmit right public keys to be certified by RCA.
- Generates and uses CA's key pair in a EAL4+ or FIPS 140-2 level-3 certified HSM.
- 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.
- Establishes contract with C-ITS-S Manufacturer.
- Communicates only with PCA authenticated with RCA validation information communicated by DC.
- Respond to request from PMA.
- Only issue and manage type of 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 Certificate.

A LTCA is represented by an authorized person named "Authorized Representative". The Authorized Representative is appointed by the legal entity that owns the LTCA.

An authorized representative can manage several LTCAs. The authorized representative is responsible for LTCA certificate request and LTCA revocation request.

LTCA can only issue LTC and validate requests sent by a PCA for PC certificate request from a C-ITS-S produced by an C-ITS-S Manufacturer and for which the C-ITS-S is already registered by this LTCA.

LTCA included in a TSL cannot start operation without prior approval by the PMA.

A LTCA operates its services according to this CP and its corresponding CPS.

A LTCA that wishes to have a certificate signed by a RCA shall send a "LTCA request" to the PMA (refer to section 4). In case of a LTCA owned by an external entity different than the RCA, a contract shall be signed between the external entity and the PMA before the LTCA certificate can be signed by the RCA. LTCA is responsible for conducting internal audit of its PKI components to check compliance with the present CP and its own CPS.

1.4.3.1 Registration Authority (LTCA-RA)

A LTCA-RA is owned by an entity designated by its LTCA.

A LTCA-RA is used to:

- Authenticate ITS-S Manufacturer to register C-ITS-S;
- Authenticate ITS-S deactivation request;
- Manage communication with PCA and DC.

A LTCA-RA has the responsibility to:

- Authenticate C-ITS-S Manufacturer, ITS LCM and PMA.
- Submit accurate and complete information to the LTCA.
- Alert PMA when there is a security incident about the LTCA services that the OA performed.
- Respect the CP and corresponding CPS.
- Protect its information system and guarantee the security of the data transmitted to the PKI.

If the LTCA designates a legal entity different from the LTCA's legal entity as a LTCA-RA, then a contract or legal document, has to be established between the LTCA and this legal entity in order to cover the LTCA-RA services addressed by this legal entity.

The LTCA CPS shall give details on how a LTCA-RA is organized and performs its operation according to the type of certificates delivered by LTCA-RA services.

A LTCA-RA operates its services according to this CP and its corresponding CPS. A LTCA-RA cannot start operation without prior approval of the LTCA owner.

1.4.4 Pseudonym Certification Authority (PCA)

PCAs are either owned by an entity designated by the PMA for C-ITS-S services and/or by external legal entity. RCA can sign several PCA.

PCA is responsible for:

- Managing C-ITS-S request.
- Signing PC certificate.
- Authenticating LTCA using TSL issued by RCA.
- Managing communication with LTCA and DC.
- Protect and guarantee integrity and confidentiality of its activation data and/or private key.
- Only use its 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).
- Realize internal audit of the PKI component used by CA to manage Certificate.
- 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 CA's entity and PMA.
- Transmit right public keys to be certified by RCA.
- Generates and uses CA's key pair in a EAL4+ or FIPS 140-2 level-3 certified HSM.
- 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.
- Establishes contract with Manufacturer.
- Communicates only with LTCA authenticated with RCA validation information communicated by DC.
- Only issue and manage type of 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 Certificate.
- Submit accurate and complete information to the LTCA.
- Protect its information system and guarantee the security of the data transmitted to the PKI.

PCA is represented by the Direction Générale des Infrastructures, des Transports et de la Mer (DGITM). The Authorized Representative is appointed by the legal entity that owns the PCA.

An authorized representative can manage several PCAs. The authorized representative is responsible for PCA certificate request and PCA revocation request.

A PCA is managed by the legal entity that owns the PCA. PCA can only issue PCs for C-ITS-S which have been authorized.

PCA included in the TSL cannot start operation without prior approval of the PMA.

A PCA operates its services according to this CP and the corresponding CPS.

PCA that wishes its certificate to be signed by RCA shall send a “PCA request” to the PMA (refer to section 4). In case of PCA owned by an external entity different than the RCA, a contract shall be signed between the external entity and the PMA before the PCA certificate can be signed by the RCA. PCA’s legal entity is responsible for conducting internal audit of its PKI components to check compliance with the present CP and its own CPS.

1.4.5 Operational Authority (OA)

The Operational Authority (OA) is the entity that hosts and manages all the software and hardware used to support PKI services described in this CP. The OA is the entity which sets up and performs all operations supporting the PKI services. The CPS gives details on how each service is provided to each PKI component.

When same OA hosts both LTCA and PCA, it shall guarantee any conflict about data privacy. It shall guarantee separation of duties for privacy reasons, i.e. all technical and organizational measures to ensure information held by the LTCA necessary for the PCA to re-identify pseudonym certificates is kept separately and no authorized person can access both LTCA and PCA certificate information within the OA.

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

1.4.6 Distribution Center (DC)

The DC is owned by the Direction Générale des Infrastructures, des Transports et de la Mer (DGITM).

The DC provides the following PKI services:

- Publication service (refer to section 2).
- Log trail generation.

DC shall update information from an External Authority Entity (e.g. other EU Member State, C-ITS-S), whom respective RCA is contained in TSL, and publish it for C-ITS-S applications and CA needs.

The DC cannot start operation without prior approval of the PMA.

1.4.7 Other Participants

1.4.7.1 External Root Certificate Authority (E-RCA)

An E-RCA is the designated RCA of an External Legal Entity, different from the SCOOP@F members (another C-ITS-S Manufacturer for example).

An E-RCA has same responsibility as the RCA and has a self-signed certificate.

1.4.7.2 External Long-Term Certification Authority (E-LTCA)

External LTCA (E-LTCA) certificate is signed by an E-RCA. An E-LTCA has the same responsibility as a LTCA towards a C-ITS-S Manufacturer it has a contract with.

1.4.7.3 External Pseudonym Certification Authority (E-PCA)

External PCA certificate is signed by an E-RCA. E-PCA has the same responsibility as a PCA.

1.4.7.4 External Distribution Center (E-DC)

E-DC is designated by an E-RCA. E-DC has the same responsibility as a DC.

1.4.7.5 Subscriber (C-ITS-S owner)

Subscriber is the owner and operator of the C-ITS-S. It can be a Car Manufacturer or a Road Operator within SCOOP@F.

The Subscriber has the responsibility to:

- Respect the CP and corresponding CPS.
- Alert LTCA and PMA in case of incident about C-ITS-S management.
- Submit accurate and complete information for C-ITS-S to the LTCA.
- Personalize C-ITS-S with up to date RCA, LTCA and DC information.
- Submit deactivation, suspension and resume request for C-ITS-S immediately when reason appear for it.
- Decide to activate or not the C-ITS-S component.

The subscriber can delegate part or whole its responsibilities to the C-ITS-S Manufacturer.

1.4.7.6 ITS Life Cycle Manager (ITS LCM)

ITS LCM is an entity authorized to maintain and update C-ITS-S component.
In SCOOP@F, ITS LCM role is supported by the Subscriber.

1.4.7.7 C-ITS-S Manufacturer

The C-ITS-S Manufacturer installs necessary information for security management in C-ITS-S at manufacturing. More precisely, the C-ITS-S manufacturer bootstraps the process for manufacturing a trusted C-ITS-S in production site, i.e. generates and stores securely all required crypto-material in security module (C-ITS-S Technical key pairs), import RCA and LTCA certificates in C-ITS-S.

C-ITS-S can be installed in vehicles and roadside stations. In this CP, C-ITS-S is the component that receives the LTC and PC certificate and has a C-ITS-S Technical key.

The C-ITS-S Manufacturer may be in charge (by delegation of the ITS LCM) of providing new C-ITS-S in the LTCA database, to make it eligible to request LTC later.

The C-ITS-S Manufacturer has the responsibility, during the whole C-ITS-S manufacturing cycle, to:

- Respect the CP and corresponding CPS.
- Protect and guarantee integrity and confidentiality of its activation data and/or C-ITS-S Technical private key.

1.4.7.8 Relying Party for PC

Relying Parties for PC are entities that rely on the validity of the binding between a message sent by a C-ITS-S and its PC certificate. A Relying Party is responsible for checking the validity of a PC certificate according to the C-ITS-S application service.

Relying party for PC in SCOOP@F is the C-ITS-S.

1.4.7.9 Relying Party for RCA, E-RCA, E-CA and CA certificates

Relying Parties are entities that rely on the validity of the binding between an identity and a public key. A Relying Party is responsible for checking the validity of a RCA and a CA certificate, at least by checking the appropriate certificate status information (using CRLs) for the CA, TSL and DC information.

Relying Parties for RCA and CAs are LTCAs, PCA and C-ITS-S.

Relying Parties for E-RCA and E-CAs are the C-ITS-S.

1.4.7.10 Relying Party for LTC

LTCA relies on the validity of the binding of a C-ITS-S identifier to an C-ITS-S Technical public key. LTCA is responsible for checking the validity of a LTC certificate, at least by checking the appropriate C-ITS-S status information using LTCA database.

Only an LTCA which has a registered C-ITS-S can deliver a LTC certificate.

1.5 Certificate and Private Key Usage

1.5.1 Appropriate Certificate Use

1.5.1.1 RCA

RCA certificate shall be only used to validate CAs, TSL and CRLs.

RCA private key shall be only allowed to sign the following:

- RCA Certificate
- CA certificate;
- CRL;
- TSL.

1.5.1.2 LTCA

LTCA certificate with signature (i.e. non-repudiation) key usage shall only be used to verify LTC certificates and messages signed and delivered by LTCA.

LTCA certificate with encryption key usage shall only be used to encrypt messages transmitted by PCA.

LTCA signature private key is allowed to sign the following:

- Response to LTC request;
- Response to PC validation request;
- LTC certificate.

LTCA encryption private key is allowed to decrypt:

- requests transmitted by PCA to validate the PC request;
- LTC request sent by an C-ITS-S

1.5.1.3 PCA

PCA certificate with signature (i.e. non-repudiation) key usage shall only be used to verify PC certificates and delivered messages signed by PCA.

PCA certificate with encryption key usage shall only be used to encrypt message transmitted by LTCA.

PCA signature private key is allowed to sign the following:

- CA Certificate Request,
- PC certificate,
- Messages for LTCA.

PCA encryption private key is allowed to decrypt:

- Message transmitted by LTCA,
- Message transmitted during PC request by a C-ITS-S.

1.5.1.4 C-ITS-S

C-ITS-S technical private key is used to sign the LTC request.

C-ITS-S technical public key is used by the LTCA to verify the LTC request.

C-ITS-S PC private key is used to sign part of PC certificate request and C-ITS-S messages.

C-ITS-S PC public key is used to verify part of PC certificate request and message signed by C-ITS-S.

1.5.2 Prohibited Certificate Use

This CP addresses no other uses than the ones stated in section 1.5.1.

1.6 Policy Administration

1.6.1 Organization Administering the Document

PMA is responsible for all aspects of this CP and the associated CPS.

The organization administering, maintaining the CP and submitting it for approval at the PMA is the OA.

1.6.2 CPS Approval Procedures

Amendments shall either be in the form of a new CPS (with a sum up of the modifications) or an update notice that contains the modifications and the references to the previous CPS. The creation or modification of the existing CPS is at the discretion of the PMA. A new CPS automatically replaces the previous one and becomes operational as soon as the PMA has approved it.

CPS PMA approval can only be delivered after compliance with this CP has been verified.

2. Publication and Repository Responsibilities

2.1. Repositories

The DC is responsible for making available the any published information related to the PKI services and the C-ITS-S services.

The DC shall be deployed in order to provide high levels of reliability within an agreed timeframe, 24 out of 24 hours, 7 out of 7 days. An unavailability time period should be agreed in order to ensure a minimum level of service continuity. A service level agreement must be defined with a requirement set at 98% for service availability.

SCOOP@F, through PMA, could distribute its TSL to External Legal Entity acting as E-RCA.

TSL contains the following data:

- DC URL
- LTCA certificate
- LTCA URL
- PCA certificate
- PCA URL
- List of E-RCA certificate approved by PMA

2.1.1. RCA and DC URL

For RCA certificate and DC URL to be distributed to other participants, the primary distribution channel shall be bilateral exchange between PMA and Relying Party.

For E-RCA certificate and E-DC URL to be distributed to SCOOP@F the primary distribution channel shall be bilateral exchange between PMA and External Entity. EU Member States which currently do not have bilateral agreements should establish such agreements and communication channels with other participating EU Members States, such as the European C-ITS Policy Authority.

PMA manages the out of band communication of the RCA certificate and DC URL to the External Entity (E-RCA) and reception of the E-RCA certificate and E-DC URL. PMA and External Entity use specific forms to communicate this information, in a way securing the authenticity and integrity of the data, as described in CPS involving the External Entity C-ITS-S Coordinator (refer to section 3.2) and the European Policy Authority and Trusted List Manager.

Before including an E-RCA certificate, E-DC URL in TSL, PMA should establish an agreement with the E-RCA's legal entity in order to have the publication authorization and to be sure of the verification of the E-RCA certificate as described above.

After verification, PMA transmits the E-RCA certificate and E-DC URL to the RCA to be included in the signed TSL.

Restoration of the RCA key is done during a key ceremony (refer to section 6.2.8). After having signed the new TSL, RCA key shall be deactivated (refer to section 6.2.9).

RCA receiving a new E-RCA certificate, either through first method of communication as described above or using the E-TSL signed by the E-RCA collected as described above, shall check the validity and authenticity of the certificate:

- If the certificate is correct according to syntax, authenticity and validity, the PMA shall update its TSL with E-RCA certificate.
- If the certificate is not correct, PMA shall inform the External Entity ITS Coordinator and the European Trusted List Manager

In case of a new RCA certificate issuance (e.g. after a security incident), this new RCA certificate must be distributed as an initial RCA certificate according to the bilateral agreement established with PMA (refer to the initial distribution detailed at the beginning of this section).

2.1.2. CRL signed by RCA

For CRLs issued by RCA, DC is the primary channel for a Relying Party.

2.2. Publication of Certification Information

The following data are published as follow:

- CP: <http://scoop-dc.servicepci.com/certificate-policy/>
- RCA certificate: <http://scoop-dc.servicepci.com/getcacerts/>
- CRL: DC URL: <http://scoop-dc.servicepci.com/getcrl/4712D46C9C818A49>
- TSL: DC URL: <http://scoop-dc.servicepci.com/gettsl/4712D46C9C818A49>

CPS and all documents referenced by CPS are not published for security reasons because they contain sensitive details about means, organization and procedures implemented by OA. These documents shall be made available to auditors as required during any audit performed on PMA request.

2.3. Time or Frequency of Publication

Information identified in section 2.2 is made available:

- CP:
 - Before start of service for the initial CP.
 - No later than 1 week after any CP update or replacement is approved by the PMA.
- RCA and CA certificates:
 - Before start of service for the initial CA and no later than 48 hours after generation of CA certificates following a renewal or re-key.
- TSL:
 - No later than 48 hours after any TSL update or replacement is approved by the PMA.
- CRL:
 - No later than 48 hours after any CRL generation.

2.4. Access Controls on Repositories

Information published in a repository is public information. The DC shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

The naming used in the certificates shall be compliant with ETSI-TS-103-097.
Subject name in certificates are limited to 32 bytes.

3.1.1.1. RCA

Naming conventions shall be approved by PMA.
The subject name of RCA certificate shall contain identifier that identifies at minimum the legal entity owning RCA.
The SubjectType for RCA shall be “root_ca”.

3.1.1.2. LTCA

Naming conventions shall be approved by PMA.
The subject name of LTCA certificate shall contain identifier that identifies at minimum the legal entity owning LTCA.
The SubjectType for LTCA shall be “enrollment_authority”.

3.1.1.3. PCA

Naming conventions shall be approved by PMA.
The subject name of PCA certificate shall contains identifier that identifies at minimum the legal entity owning PCA.
The SubjectType for PCA shall be “authorization_authority”.

3.1.1.4. LTC

Naming conventions shall be approved by PMA.
The SubjectType for LTC shall be “enrollment_credential”.

3.1.1.5. PC

Naming conventions shall be approved by PMA.
The subject name shall be empty.
The SubjectType for PC shall be “authorization_ticket”.

3.1.2. Need for Names to Be Meaningful

Refer to section 3.1.

3.1.3. Anonymity or Pseudonymity of Certificate

RCA, LTCA, PCA and LTC are not anonymous.

PC uses a pseudonym defined by PCA.

PCA shall ensure that Pseudonymity of a C-ITS-S is established by provisioning the C-ITS-S with a PC that does not contain any names or information that may link the subject to its real identity.

3.1.4. Rules for Interpreting Various Name Forms

Relying parties shall use the subject name contained in the certificate (refer to section 3.1) to identify the legal entity owner of RCA, LTCA, PCA and C-ITS-S through LTC.

PCA shall ensure that Pseudonymity of a C-ITS-S is established by provisioning the C-ITS-S with Authorization Tickets that do not contain any names or information that may link the subject to its real identity.

3.1.5. Uniqueness of Names

Subject name contained in the certificate of RCA and CA (refer to section 3.1) are unique in the RCA trust domain.

PMA controls that RCA and CA certificates are unique by controlling the Subject name used in the RCA and CA certificates and by approving RCA and CA creation.

Not applicable for PC.

3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulations.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

3.2.1.1. RCA

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

3.2.1.2. LTCA

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

3.2.1.3. PCA

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

3.2.1.4. PC

Proof of the PC possession of the private key is obtained through procedures to generate the private key (refer to section 6.1.1) that corresponds to the public key to be certified, and through the public key transmission method (refer to section 6.1.3). Such procedures should also demonstrate the legal identity of the owner of the private key, as duly approved by PMA.

3.2.1.5. LTC

Proof of the LTC possession of the private key is obtained through procedures to generate the private key (refer to section 6.1.1) that corresponds to the public key to be certified, and through the public key transmission method (refer to section 6.1.3). Such procedures should also demonstrate the legal identity of the owner of the private key, as duly approved by PMA.

3.2.2. Authentication of Organization Identity

3.2.2.1. RCA

The PMA authenticates and appoints The Direction Générale des Infrastructures, des Transports et de la Mer (DGITM) as Organization Identity of the RCA.

Prior to issuance of RCA, PMA shall ensure the existence of the legal entity.

3.2.2.2. LTCA and PCA for CA certificate

The PMA authenticates all CA's Organization Identity that own a CA to be included in the RCA's TSL.

Prior to issuing CA certificate, PMA shall ensure the existence of the CA's entity. This shall include a verification of suitable proofs of physical and legal existence.

Evidence shall be provided, and verified by PMA, of:

- Full name and legal status of the CA entity.
- Any relevant existing registration information (e.g. company registration as SIREN or SIRET) of the CA entity, consistent with the national law of country where entity is officially registered or other applicable identification practices if there are no national ones.

PMA produces an authorization of the CA's legal entity to be LTCA or PCA. This authorization shall be given by PMA whatever the form of the evidence produced.

3.2.2.3. Subscriber

Evidence shall be provided, and verified by PMA, of:

- Full name and legal status of the Subscriber.

- Any relevant existing registration information (e.g. company registration like SIREN or SIRET) of the Subscriber, consistent with the national law of country where Subscriber is officially registered or other applicable identification practices if there are no national ones.
- Authorization of the Subscriber to use LTCA. This authorization shall be given by PMA whatever the form of the evidence produced by PMA.

3.2.2.4. LTCA and PCA mutual authentication

Both LTCA and PCA use the same rules that are the following:

- PCA/LTCA checks if LTCA/PCA certificate is included in the TSL and if it is not revoked (present in the CRL). If it is, authentication is valid.
- Verify the signature during request/response for validation of PC request

3.2.2.5. External Entity

PMA authenticates External Entity as the organization that owns the E-RCA which issues E-LTCA and E-PCA certificates to be used in the TSL.

The authentication process shall permit to authenticate the entity acting as PMA for the E-RCA.

3.2.3. Authentication of Physical Person Identity

3.2.3.1. RCA

Evidence of the individual identity of a person who has a trusted role (refer to section 5.2) for RCA key ceremony, is an authorized representative for RCA or PMA or witness for RCA key ceremony is checked by the PMA and OA against a physical person during a face to face meeting (refer to section 5.2) or an equivalent method, which 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 shall be done by a trusted person/entity in charge of security operation (refer to section 5.2).

PMA records a unique identification number and the ID document presented for each individual and verifier person.

3.2.3.2. LTCA and PCA

Evidence of the individual identity of a person who has a trusted role (refer to section 5.2) for CA key ceremony, is an authorized representative for CA or PMA or Witness for CA key ceremony is checked by the PMA and OA against a physical person during a face to face meeting (refer to section 5.2) or an equivalent method, which 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 person in charge of security operation (refer to section 5.2).

PMA records a unique identification number and the ID document presented for each individual and verifier person.

3.2.3.3. Subscriber

Identity evidence of the Subscriber trusted contact is checked by the LTCA-RA against a physical person during a face to face meeting or an equivalent method, which provides the same level of security assurance, described in the LTCA CPS and approved by PMA.

Evidence of the individual is verified by the LTCA-RA using one (1) National Government-issued ID document that contains a picture of the individual.

LTCA-RA records a unique identification number and the ID document presented for each individual and verifier person.

Subscriber trusted contact is authenticated only once in order to initiate trusted communication with LTCA-RA. During first authentication, Subscriber trusted contact gives, and/or establishes with LTCA-RA, authentication means to be used for further trusted communication, between the LTCA-RA and the Subscriber trusted contact as a human and/or an IT system under the Subscriber control.

After successful authentication, Subscriber transmits, under responsibility of Subscriber trusted contact, C-ITS-S information to LTCA-RA. This information is required by LTCA-RA to authenticate LTC and PC certificate request from C-ITS-S.

3.2.4. Validation of Authority

The PMA appoints and authorizes at least one person from the OA responsible (e.g. security officer) for the request of new certificates and renewals (see section 3.2.3).

3.2.5. Non-Verified Subscriber Information

There is no non-verified information used by the PMA to fill a RCA and CA Certificate.

There is no non-verified information used by LTCA to fill a LTC Certificate.

There is no non-verified information used by PCA to fill a PC Certificate.

3.2.6. Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the PMA.

The CA certificate is signed by RCA approved by PMA; CA is never certified or cross-certified with another external CA or RCA.

RCA, LTCA, PCA, LTC and PC are managed according to ETSI-TS-102-941 and therefore interoperable for ITS EU services.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

Same procedures as described in section 3.2 apply.

3.3.2. Identification and Authentication for Re-key After Revocation/Deactivation

Same procedures as described in section 3.2 apply.

For CA, before to apply the procedure, the PMA has to investigate in order to decide if the renewal certificate is possible.

For C-ITS-S, in parallel of the procedure, the LTCA has to investigate and wait the audit report conclusion realized after the deactivation in order to decide if the renewal certificate is still possible with this kind of C-ITS-S. In case of serious security incident in C-ITS-S services protocol, PMA shall be alerted by LTCA (refer to section 5.7).

3.3.3. Identification and Authentication for Revocation/Deactivation Request

3.3.3.1. RCA, LTCA and PCA for CA certificate

Same procedures as described in section 3.2 apply.

3.3.3.2. LTC

Deactivation requestor authentication is done according to LTCA-RA procedure approved by PMA (refer to section 4.9).

3.3.3.3. PC

Not applicable.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

Sections 4.1, 4.2, 4.3 and 4.4 specify the requirements for an initial application for certificate issuance. Sections 4.6, 4.7 and 4.8 specify the requirements for certificate renewal.

4.1.1. Who Can Submit a Certificate Application?

4.1.1.1. RCA

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

4.1.1.2. LTCA and PCA for CA certificate request

The authorized representative of the CA shall submit the CA certificate request to the RCA.

4.1.1.3. LTC

Subscriber or C-ITS-S Manufacturer (by way of delegation from the Subscriber) accept voluntarily to register its C-ITS-S in the LTCA. Then C-ITS-S manages automatically LTC request without requiring any Subscriber interaction.

4.1.1.4. PC

Before requesting a PC, C-ITS-S shall have a LTC.
Then C-ITS-S manages automatically PC request without requiring any Subscriber interaction.

4.1.2. Enrollment Process and Responsibilities

4.1.2.1. RCA

The enrollment process is based on a signed procedure that contains at a minimum the following information:

- Identity to set in the RCA certificate (refer to section 3.1).
- PMA 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.
- Rights to be included in the RCA certificate such as ITS AID, SSP.
- PMA representative identity that requests the RCA creation.

The RCA certificate request shall be signed by the authorized representative. If the signature is electronic signature, then PMA shall first authorize means to be used for electronic signature and validation of the electronic signature of the RCA certificate request.

Associated to the RCA certificate request, the RCA authorized representative shall join its copy of a National Government-issued ID containing its picture. PMA stores a copy of the Authorized representative's ID.

4.1.2.2. LTCA and PCA for CA certificate request

CA certificates requests must be authorized by the PMA prior to issuance. The issuance process includes documenting the following information to be contained in the CA certificate request:

- Identity to set in the CA certificate (refer to section 3.1).
- Legal Entity which owns 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.
- The Certificate Request associated with the generated key pairs (refer to section 6.1.1). Certificate Request shall be included in the application if the CA's key pairs have been generated by CA's entity in its own OA before the key ceremony to issue CA certificate.
- Identity of the RCA to be used to sign the CA certificate.
- Validity period of the CA certificate.
- Cryptographic information of the CA certificate.
- Rights to be included in the CA certificate.
- 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 CA certificate request shall be signed by the authorized representative.

Associated to the CA certificate request, the Authorized representative shall join a copy of its National Government-issued ID containing its picture. PMA stores a copy of the Authorized representative's ID.

The following information shall be given to the PMA:

- CA's CP and CPS.
- Technical and organizational architecture description of the PKI and procedure used by CA and RA.
- URL of the CA service (URL of LTCA or PCA service to be used by C-ITS-S) to be included in the TSL.
- Any other information or documents requested by PMA in order to audit and to control CA certificate request with the present CP requirements.

If the CA is owned by an entity different than the entity that owns the RCA, before issuing a CA certificate request, CA and PMA shall sign a contract related to the RCA service (refer to section 4.2).

4.1.2.3. LTC

When a LTC is needed, C-ITS-S generates a key pair (refer to section 6.1.1) and creates a certificate request according to ETSI-TS-102-941.

Certificate request contains the C-ITS-S identifier and requested “aid_ssp_list”, C-ITS-S LTC public key and response encryption key (used by PCA for return message).

C-ITS-S signs the LTC certificate request using its C-ITS-S Technical private key.

ITS-S sends the certificate request to the configured LTCA-RA URL (refer to section 6.1.4).

4.1.2.4. PC

When a PC is needed, C-ITS-S generates a key pair (refer to section 6.1.1) and creates a certificate request according to ETSI-TS-102-941.

In order to preserve C-ITS-S anonymity, the certificate request includes 3 parts; the first is intended for the PCA, the second is intended for the LTCA (referred to as PCA and LTCA parts) and the third is common to LTCA and PCA:

- LTCA part: signature of the certificate request and LTC identifier.
- PCA part: contains the public key(s) of PC for C-ITS-S.
- Common part: LTCA identifier, requested starting date, requested “aid_ssp_list” and response encryption key (used by PCA for return message).

C-ITS-S signs the PC certificate request using its LTC private key.

C-ITS-S encrypts the certificate request as follow:

- LTCA part encrypted with LTCA encryption key.
- LTCA, PCA and common part encrypted with PCA encryption key.

C-ITS-S sends its certificate request to PCA’s URL.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.1.1. RCA

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 3.2, and to verify that the information in RCA certificate request is accurate for the RCA.

4.2.1.2. LTCA and PCA for CA certificate request

Requests are submitted by an authorized representative of the CA 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 3.2, and to verify that the information in CA Certificate request is accurate for the CA.

4.2.1.3. LTC

Before a C-ITS-S can request an LTC certificate, C-ITS-S Manufacturer shall transmit C-ITS-S information to the LTCA-RA. LTCA-RA authenticates the C-ITS-S Manufacturer (refer to section 3.2.2 and 3.2.3). LTCA-RA register the C-ITS-S information in its database. This operation is done only once by C-ITS-S Manufacturer for each C-ITS-S. After, only updated status of C-ITS-S is transmitted to LTCA-RA by C-ITS-S Manufacturer and C-ITS-S LCM.

LTCA-RA authenticates and verifies that the information in LTC request is accurate for a C-ITS-S (refer to section 3.2.3).

4.2.1.4. PC

PCA receives the PC request.

PCA has to authenticate the LTCA (refer to section 3.2.2).

If PCA is not able to authenticate the LTCA, the PC certificate request is rejected.

PCA signs the PC request, only the LTCA and common part, using its signature key and encrypt the PC request using the LTCA encryption key.

LTCA-RA authenticates the certificate request from PCA (refer to section 3.2.2).

LTCA-RA authenticates and verifies that the information in PC request is accurate for a C-ITS-S (refer to section 3.2.3).

4.2.2. Approval or Rejection of Certificate Applications

4.2.2.1. LTCA and PCA for CA certificate request

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

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

The PMA shall be responsible for approving or rejecting the CA certificate request. In the case where the CA certificate request is complete and compliant with this CP, the PMA approves the CA certificate request and continue the application process. In the case where the CA certificate request is rejected, the PMA will ask to re-submit a new CA certificate request with all required information.

PMA may audit the CA's PKI as defined in section 8. PMA studies audit report of the CA's PKI. The PMA either determines that the CA's PKI meets the compliance audit requirements or that the CA's PKI is not able to address remaining issues. When CA's PKI does not meet the compliance audit requirement, then CA's PKI shall modify its practice to fulfill the discrepancy.

If CA's PKI is not able or not willing to address remaining discrepancies, then PMA ends the process and RCA cannot deliver the CA certificate. If CA's PKI fulfills the audit requirement, then CA certificate can be issued.

A CA which root certificate is signed by RCA can only issue certificates approved by PMA (refer to section 4.1). If a CA's entity wants to issue other type of certificate, the new type of Certificate shall be declared to the PMA and approved by it following the processes described in section 4.1 and 4.2. Depending on the type of these new certificates, it might be necessary to issue a new CA certificate with a new key pair.

4.2.2.2. LTC

LTC request control and approval is performed by LTCA-RA. If the certificate request is correct and valid, then the LTCA-RA transmits it to the LTCA to generate the requested certificate. If the certificate request is not correct, LTCA-RA rejects it. If C-ITS-S still wants a LTC certificate, it shall make a new certificate request.

4.2.2.3. PC

PC request control and approval is performed by LTCA-RA. LTCA-RA generates a status, starting date and duration for PC in case of acceptance of the request, signed with its LTCA private signature key and encrypted with PCA public encryption key, for the certificate validation request to be returned to PCA.

LTCA-RA returns the hash and the response code of the certificate validation request to the PCA. PCA authenticates the LTCA-RA and verifies the status answer (refer to section 3.2.2).

If the certificate request is correct and valid, the PCA issues the requested certificate. If the certificate request is not correct, then PCA rejects it. If C-ITS-S still wants a PC certificate, it shall make a new certificate request.

4.2.3. Time to Process Certificate Applications

4.2.3.1. RCA

Certificate application are processed during working day.

4.2.3.2. LTCA and PCA for CA certificate application

CA certificate application are processed during working day according to the agreement and contract between RCA and CA.

4.2.3.3. LTC

LTCA shall respond (verification and response) in less than 1 second.

4.2.3.4. PC

PCA shall respond (verification and response) in less than 1 second.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

4.3.1.1. RCA

The RCA certificate and its key pair are generated during a key ceremony (refer to section 6.1.1). RCA private key is activated to sign its own RCA certificate. The RCA certificate is issued with the TSL.

4.3.1.2. LTCA and PCA for CA certificate whom CA's key pair are performed by PMA's OA

The following actions must occur during a CA Key Ceremony, which shall be witnessed by a PMA witness at least (CA may have also a witness):

- Issuance of 2 CA keys (refer to section 6.1.1).
- Backup of CA private keys (refer to section 6.2.4).
- Generation of CA Certificate request.
- RCA private key is activated to sign CA certificate containing the 2 CA public key (refer to section 6.2.6, 6.2.7 and 6.2.8).
- At the end of the key ceremony the CA private keys are deactivated (refer to section 6.2.9), CA keys are destroyed inside the HSM (refer to section 6.2.10) and only exist on backup format (refer to section 6.2.4).

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9), RCA public and private keys are destroyed inside the HSM (refer to section 6.2.10) and only exist on backup format (refer to section 6.2.4).

4.3.1.3. LTCA and PCA for CA certificate whom CA's key pair are not performed by PMA's OA

Not applicable.

4.3.1.4. LTC

LTCA generates a LTC certificate.

LTCA sends the LTC to the C-ITS-S.

Exchanged messages between entities are protected in terms of confidentiality and integrity.

4.3.1.5. PC

PCA generates a PC certificate.

PCA sends the PC to the C-ITS-S.

Exchanged messages between entities are protected in terms of confidentiality and integrity.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Not applicable.

4.4. Certificate Acceptance

4.4.1. Conducting Certificate Acceptance

4.4.1.1. RCA

Not applicable.

4.4.1.2. LTCA and PCA for CA certificate acceptance

Not applicable.

4.4.1.3. LTC

Not applicable

4.4.1.4. PC

Not applicable.

4.4.2. Publication of the Certificate by the DC

RCA, CA and E-CA certificates are published in TSL as detailed in section 2.

Relying party can verify the certificate using information published by PMA (refer to section 2.2).

LTC and PC certificate are not published.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Notification of RCA and CA certificates issuance is provided by publishing RCA and CA certificates (refer to section 2.2).

PMA informs C-ITS-S services as well as participating External Entity and EU Member State representative when a RCA is issued.

There is no notification of LTC and PC issuance.

4.5. Key Pair and Certificate Usage

4.5.1. Private Key and Certificate Usage

RCA, LTCA and PCA shall use their Private Keys for the purposes set forth in section 1.5. Usage of a key pair and the associated certificate shall also be performed as indicated in the certificate itself, via extensions related to key pair usage (refer to section 6.1.7).

4.5.2. 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 to authenticate LTC and PC certificates.

Relying parties have to be aware of the security rules to be deployed in the C-ITS-S for the usage of a LTCA, PCA, RCA, PC and LTC certificates.

RCA, LTCA, PCA, LTC and PC certificates cannot be used without preliminary check from Relying party.

4.6. Certificate Renewal

Not allowed.

4.7. Certificate Re-key

Certificate re-key shall be processed when a key pair reaches the end of its life (refer to section 6.3.2), the end of operational use, or when the public key is compromised. A new key pair shall be generated in all cases.

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

4.7.1. RCA

Not applicable.

4.7.2. LTCA and PCA

The CA certificate request has to be submitted in a due delay in order to be sure to have a new CA certificate and operational CA's key pair before the expiration of the current CA's private key (refer to section 5.6.2 and 6.3.2). The date of submission has also to take into account the time required for approval (refer to section 4.2.3).

4.7.3. LTC

Not allowed.

4.7.4. PC

Not allowed.

4.8. Certificate Modification

Not applicable.

4.9. Certificate Revocation and Suspension and ITS deactivation

4.9.1. Circumstances for revocation or deactivation

4.9.1.1. RCA

A revoked RCA certificate means all certificates signed by RCA are revoked, when the binding between the certificate and its associated public key is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The private key is suspected 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.

4.9.1.2. LTCA and PCA

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

- The RCA is revoked.
- The CA private key is suspected compromised or is compromised.
- The entity owning the CA has not respected the contract with the PMA.
- The CA can be shown to have violated the stipulations of the present CP.
- The CA can be shown to have violated the stipulations of its CPS.
- End of the CA services.
- Privilege attributes asserted in the CA's certificate are reduced.
- Change in the key length or algorithm is recommended by an international standard institute.
- CA's representative requests the CA to be revoked by transmitting a signed CA revocation request to the PMA.
- PMA obtains evidence that the CA certificate was misused.
- CA's representative notifies the PMA that the original CA certificate request was not authorized and does not retroactively grant authorization.
- 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.
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement
- The technical content or format of the certificate presents an unacceptable risk for ITS Application or Relying Parties (e.g. security standard might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such certificates should be revoked and replaced by RCAs within a given period of time).

4.9.1.3. LTC

LTC cannot be revoked or deactivated. Only C-ITS-S can be deactivated especially for the following reasons:

- The LTCA is revoked.
- C-ITS-S is compromised.
- C-ITS-S identity information is incorrectly filled.
- The certificate has been lost or compromised.
- The LTCA's OA failed to comply with the necessary obligations and security rules in the CP and CPS and requirements set in referenced documents in section 1.1.
- The end of the service mentioned in the certificate.
- C-ITS-S technical key is compromised.

4.9.1.4. PC

Not applicable.

4.9.2. Who Can Request Revocation or Deactivation

4.9.2.1. RCA certificate revocation

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

4.9.2.2. CA certificate revocation

It is the responsibility of the authorized representative to request revocation of the said CA certificate of the CA he/she represents.

PMA has also the authority to request for CA certificate revocation.

4.9.2.3. ITS-S deactivation

PMA, LTCA-RA and ITS-S LCM can submit a deactivation request especially in the following cases:

- Identity information filled incorrectly.
- The certificate corresponding to the private key has been lost or compromised.
- The end of the service mentioned in the certificate.
- C-ITS-S technical key is compromised.

- C-ITS-S is compromised.

4.9.2.4. LTC and PC revocation

Not applicable.

4.9.3. Revocation and Deactivation Request Procedure

4.9.3.1. RCA certificate

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

Only the PMA can decide to deactivate a RCA, according to its rules (refer to [SCOOP@F-PQP]).

PMA informs all SCOOP@F participants (including external participants).

A last TSL and CRL are issued before revocation of the RCA.

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

4.9.3.2. LTCA and PCA certificate

Revocation of the CA certificate requires also deactivation of all LTC certificates CA has issued.

The revocation of a CA certificate is decided by the PMA according to its rules (refer to [SCOOP@F-PQP]).

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 attendees (refer to section 3.2) using the list provided by an authorized representative (witness) and the list of OA's PKI trusted role.

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

RCA key pair, which have to be used for the revocation operation, is undertaken and witnessed in a physically secure environment (refer to section 5.1) by individuals filling trusted roles (refer to section 5.2) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees.

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

At the end of the key ceremony the RCA private key is deactivated (refer to section 6.2.9), RCA key is destroyed inside the HSM (refer to section 6.2.10) and only exist on backup format (refer to section 6.2.4).

The current RCA issued CRL is replaced by the new one in DC as described in section 2.2.

PMA can decide in this particular case to also request the destruction of the CA private key backup and CA key in HSM hosted by CA's OA.

PMA informs all SCOOP@F participants (including external participants) about the revocation of CA certificate (refer to section 2).

4.9.3.3. C-ITS-S

Deactivation requestor creates the deactivation request for a particular C-ITS-S or for a list of C-ITS-S, that has to be deactivated. The requestor also informs the PMA about C-ITS-S deactivation.

Deactivation requests are authenticated by the LTCA-RA.

The LTCA-RA authenticates the deactivation request it receives (refer to section 3.3.3).

The LTCA-RA transmits the deactivation request to the LTCA.

The LTCA authenticates the LTCA-RA.

The LTCA deactivates the C-ITS-S in its database.

LTCA-RA notifies the deactivation requestor of the success of the operation.

There is no publication of C-ITS-S status. Only LTCA and requestor know the status of C-ITS-S.

4.9.3.4. PC

Not applicable.

4.9.4. Revocation and Deactivation Request Grace Period

There is no revocation and deactivation grace period. Responsible parties must request revocation and/or deactivation as soon as they identify the circumstances under which revocation is required.

4.9.5. Timeframe within which the Revocation and/or Deactivation Request Must be Processed

PMA shall begin investigation of a certificate revocation request within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted, in less than 7 days, based on at least the following criteria:

- The nature of the alleged problem.
- The number of Certificate Problem Reports received about a particular certificate.
- The entity making the complaint (for example, a complaint from a law enforcement official should carry more weight than a complaint from a Subscriber alleging that it did not receive the goods it ordered);
- Relevant legislation.

The RCA shall process a revocation decision as soon as possible, not to exceed 7 days.

LTCA shall process deactivation as soon as possible after receiving the deactivation request, not to exceed 72 hours.

4.9.6. Revocation and Deactivation Checking Requirement for Relying Parties

4.9.6.1. RCA and LTCA and PCA for CA certificate

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. How often new revocation data should be obtained is determined by the Relying Party. If it is temporarily impossible to obtain revocation information, 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 CP. Such use may occasionally be necessary to meet urgent operational needs.

The PMA shall provide Relying Parties, C-ITS-S Application Software Suppliers, 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. The PMA shall publicly disclose the instructions through a readily accessible online means (refer to section 2).

4.9.6.2. LTC

Use of deactivated C-ITS-S technical key and/or LTC could have damaging or catastrophic consequences in certain applications. How often new deactivation data should be obtained is determined by the LTCA. If it is temporarily impossible to obtain deactivation information, the LTCA must either reject use of the LTC and/or C-ITS-S technical key, or make an informed decision to accept the risk, responsibility, and consequences for using a LTC and/or C-ITS-S technical key whose authenticity cannot be guaranteed to the standards of this CP. Such use may occasionally be necessary to meet urgent operational needs.

4.9.6.3. PC

Not applicable.

4.9.7. CRL and deactivation status Issuance Frequency

4.9.7.1. RCA and LTCA and PCA for CA certificate

RCA issues CRL at least every 3 years.

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

DC ensures that superseded CRLs are removed from the repository upon posting of the latest CRL.

4.9.7.2. LTC

Not applicable

4.9.7.3. PC

Not applicable.

4.9.8. Maximum Latency for CRLs and deactivation status

4.9.8.1. RCA and LTCA and PCA for CA certificate

RCA issues CRL at least every 3 years. CRL is valid for 3 years and 3 months. Renewal period is 3 years.

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

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

4.9.8.2. LTC

Not applicable.

4.9.8.3. PC

Not applicable.

4.9.9. On-line Revocation/Deactivation Status Checking Availability

Not applicable.

4.9.10. On-line Revocation/Deactivation Checking Requirements

Not applicable.

4.9.11. Other Forms of Revocation/Deactivation Advertisements Available

Not applicable.

4.9.12. Specific Requirements in the Event of Private 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 shall be published at a minimum on the Publication Service website and possibly by other means (other institutional websites, newspapers ...).

4.9.13. Suspension

4.9.13.1. Circumstances for Suspension

Circumstances for LTC to be suspended could be especially:

- C-ITS-S Hardware and/or software failures,
- Suspected misbehavior.

4.9.13.2. Who can Request Suspension

C-ITS-S LCM could submit a suspension request.

4.9.13.3. Procedure for Suspension/Resume Request

Suspension/resume requestor creates the suspension/resume request for a particular C-ITS-S or for a list of C-ITS-S that has to be deactivated.

Suspension/resume requests are authenticated by the LTCA-RA.

The LTCA-RA authenticates the suspension/resume request it receives (refer to section 3.3).

There is no publication of C-ITS-S status. Only LTCA and requestor know the status of C-ITS-S.

4.9.13.4. Limits on Suspension Period

There is no limit for suspension.

4.10. Certificate Status Services

4.10.1. Operational Features

Not applicable.

4.10.2. Service Availability

Not applicable.

4.11. End of Subscription

CA Certificates covered by this CP that have expired prior to or upon end of subscription are not required to be revoked.

When the RCA PKI components ends its relationship with the OA, then the OA transfers all material and files related to the PKI infrastructure to an entity appointed by the PMA.

When a CA PKI components ends its relationship with the OA, then the OA transfers all material and files related to the PKI infrastructure to an entity appointed by the CA.

When the LTCA ends its relationship with a Subscriber, then LTCA deactivates all C-ITS-S operated by the Subscriber.

In case SCOOP@F ends its relationship with an External Entity, then the registration information (refer to section 2) that allows communication with External Entity (E-RCA, E-LTCA and E-PCA) is removed from TSL.

4.12. Key Escrow and Recovery

4.12.1. Subscriber

4.12.1.1. Which key pair can be escrowed

Not applicable.

4.12.1.2. Who Can Submit a Recovery Application?

Not applicable.

4.12.1.3. Recovery Process and Responsibilities

Not applicable.

4.12.1.4. Performing Identification and Authentication

Not applicable.

4.12.1.5. Approval or Rejection of Recovery Applications

Not applicable.

4.12.1.6. KEA and KRA Actions during key pair recovery

Not applicable.

4.12.1.7. KEA and KRA Availability

Not applicable.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management and Operational Controls

5.1. Physical Controls

5.1.1. Site Location and Construction

OA is located in a country approved by PMA.

5.1.1.1. 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 ...) shall be consistent with facilities used to house high value and sensitive information. RCA shall be operated in a dedicated physical area separated from other PKI component physical area.

The OA implements policies and procedures to ensure that the physical environments, in which the RCA equipment are installed are maintained with a high level of security that guarantees:

- Isolation from outside networks (RCA is never connected to any kind of network).
- Separation into a series of progressively secure physical perimeter (at least 2).
- 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 multiple access controls.

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

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

These security principles are applied during initial Key Ceremony: RCA is put off-line after this initial Key Ceremony.

5.1.1.2. CA, RA and DC

The location and construction of the facility of the OA housing CA, RA, and DC equipment and data (log, archive, HSM, server, Subscriber request form, network security component) shall be 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, shall provide robust protection against unauthorized access to equipment and records.

OA for RCA's CA is located in France. CA's OA shall be installed in location approved by PMA.

The OA shall implement policies and procedures to ensure that the physical environments, in which CA, RA and DC equipment are installed, are maintained with a high level of security that guarantees:

- Separation into a series of progressively secure physical perimeter (at least 2).
- 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.
- Two-factor authentication (for example; using biometrics and badge) to go in and out in the CA, DC and RA physical secured area.
- Two persons' physical access controls to both the cryptographic module and computer system shall be required.
- CA, RA and DC equipment and data (server, HSM, log, archive ...) are stored in cabinet in dedicated 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 used mechanisms include at minimum:

- 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 and supervision tools to continually monitor the OA facility housing equipment on a 24x7x365 basis. The OA facility is never left unattended.

5.1.2. Physical Access

5.1.2.1. RCA, CAs, RA and DC

Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, ...) shall always be protected from unauthorized access and damage.

The minimum physical security mechanisms shall be:

- Store all removable media and paper containing sensitive plain-text information in secure containers.
- Monitor, either manually or electronically, unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Any non-authorized individual entering secure areas shall always be under oversight by an authorized employee.
- Ensure an access log is maintained and inspected periodically.
- Provide at least 2 layers of increasing security such as perimeter, building, and operational room.
- Access to cabinet used for equipment is dedicated to the OA's trusted roles only.
- Require two trusted role physical access controls to both the cryptographic HSM and activation data.
- CA backup key shall be stored in a safe that fit the requirements set for RCA safe (refer to section 5.1.1.1 and 5.1.2.1).

A security check of the OA facility housing equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation.
- For off-line component, all equipment is shut down.
- Any security containers (temper envelop, safe ...) are properly secured.
- Physical security systems (e.g., door locks, vent covers, electricity ...) are functioning properly.
- The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in safe. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and shall not be stored with the cryptographic module in a way to avoid only one person having access to private key.

A person or group of trusted roles shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3. Power and Air Conditioning

The OA ensures that power and air conditioning facilities are sufficient to support the operation of the PKI system, using primary and back-up installations.

5.1.4. Water Exposures

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

5.1.5. Fire Prevention and Protection

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

5.1.6. Media Storage

Media used within the OA are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the retaining period.

Sensitive data shall be protected against being through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

OA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets compliant with the risk analysis.

5.1.7. Waste Disposal

All media used for the storage of sensitive data such as keys, activation data or files shall be destroyed before being released for disposal.

5.1.8. Off-site Backup

5.1.8.1. RCA

Full back-ups of off-line PKI components, sufficient to recover from system failure, are made after PKI KC and after each new key pair generation. Back-up copies of essential business information (key pair, CRL and TSL) 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.

5.1.8.2. CA, RA and DC

Full back-ups of PKI systems on-line, sufficient to recover from system failure, are made after PKI deployment and on a daily basis. Back-up copies of essential business information 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

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 PMA 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.

For RCA, all personnel are formally appointed to trusted roles by the PMA/OA.

CA is responsible to define and documented trusted roles and associated operation.

PMA controls that CA's trusted roles are compliant with the present CP and standards used by CA (refer to section 4.1.2).

5.2.2. Number of Persons Required per Task

The number of persons who provide PKI services is detailed in the CPS for RCA and CA's entity documents. 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 shall serve in a trusted role as defined in section 5.2.1.

RCA keys are under triple control at minimum.

CA keys are under dual control at minimum.

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

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

It is forbidden to own privileges (role) for the following operation at the same time:

- An individual owning a role in PKI system operation shall not be involved in any other operation.
- An individual owning a role in security operation shall 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 shall 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 CA audit) operation shall not be involved in any other operation except security operation. This rule does not apply to any kind of external auditor which can't have any role in the PKI.
- An individual owning a role in on-line PKI Software administration shall not be involved in on-line PKI software operation.
- 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 (this rule applies only for RCA and CA).

CA entity is responsible to define and implement trusted roles and associated operation according segregation rules set in standard taken as reference (refer to section 4.1.2). CA entity

shall document the segregation of duty for all trusted role used to manage CA and RA. PMA controls that CA's entity trusted roles segregation is compliant with the present CP and standard used by CA (refer to section 4.1.2).

5.2.3. Identification and Authentication for Each Role

All necessary checks must be completed before any individual enters a trusted role within the PKI components.

All persons assigned to a role, as described in this CP, are identified and authenticated so as to guarantee that said role enables them to perform their PKI duties. The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4. Roles Requiring Segregation of Duties

Segregation of duties may be enforced using PKI equipment, procedures or both. PKI component employees are individually appointed to trusted roles for operations defined in section 5.2.1.

No individual shall be assigned more than one identity unless approved by the PMA for RCA's OA and by the CA entity for CA's OA.

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

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

PMA, CA entity and OA components employ a sufficient number of personnel who possess expert knowledge, experience and appropriate qualifications necessary for the job functions and services provided. PKI personnel fulfill the requirements of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness. PKI personnel shall be appointed to trusted roles by the PMA and CA entity for their respective roles.

5.3.2. Background Check Procedures

PMA, CA entity and OA employees filling trusted roles shall be free from conflicting interests that might prejudice the impartiality of the PKI operations. The CA entity and OA shall not appoint to trusted roles or management any individual who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position.

5.3.3. Training Requirements

The PMA, CA entity and OA ensure that all personnel performing duties with respect to operations receive comprehensive training in:

- PKI security principles and mechanisms.
- Software versions used in the PKI system.
- PKI business processes and workflows.
- Duties they are expected to perform.
- Dispute operations and procedures.
- Sufficient IT knowledge.
- Disaster recovery and business continuity procedures.

5.3.4. Retraining Frequency and Requirements

Individuals filling trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan, and the execution of said plan shall be documented.

5.3.5. Job Rotation Frequency and Sequence

The PMA, CA entity and OA Entity ensure that any change in staff will not affect the security of the system.

5.3.6. Sanctions for Unauthorized Actions

Appropriate administrative disciplinary sanctions are applied to any PKI component's personnel violating the present CP and the CA's CP.

5.3.7. Independent Contractor Requirements

Contractors employed to perform PKI component functions are subject to the all personnel controls defined in section 5.3. Contractors can perform PKI system operations (refer to section 5.2) with approval of the PMA or the CA entity according to the PKI component.

5.3.8. Documentation Supplied to Personnel

PKI components make available to their personnel the present CP and the corresponding CPS, and any relevant statutes and policies. Other technical, operational and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

Audit log files are generated by OA and PMA for all events related to security and PKI services. In accordance with National Privacy regulation, audit log shall not permit access to private data concerning C-ITS-S (refer to section 9.3.3).

When possible, security audit logs shall be automatically collected. When not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it. All data related to a personal identity are encrypted and protected against non-authorized access. OA should comply with Privacy regulation and demonstrate the protection against such attempt by implementing encryption mechanism and privacy data isolation in a way where OA cannot link certificate life cycle activity log with private data.

Logging will include the following topics for each PKI component and each OA:

- Physical facility access.
- Trusted roles management.
- Logical access.
- Backup management.
- Log management.
- Data from the authentication process for Subscribers and PKI components.
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls.
- Acceptance and rejection of certificate requests.
- C-ITS-S Manufacturer registration.
- C-ITS-S registration.
- Certificate creation.
- Certificate renewal.
- C-ITS-S deactivation.
- C-ITS-S suspension.
- C-ITS-S resume.
- LTC and PC certificate creation.
- HSM management.
- Key creation, use and destruction.
- Activation data management.
- Role management.
- IT and network management, as they pertain to the PKI systems.
- PKI documentation management.
- Security management (Successful and unsuccessful PKI system access attempts, PKI and security system actions performed, Security profile changes, System crashes, hardware failures and other anomalies, Firewall and router activities; and entries to and exits from the OA facility).

At minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of event.

- Trusted date and time the event occurred.
- Result of the event: success or failure where appropriate.
- Identity of the entity and/or operator that caused the event.
- Identity for which the event is addressed.
- Cause of the event.

5.4.2. Log Processing Frequency

PKI operation audit logs are 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 Log

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

Event log containing information which can lead to personal identification, are encrypted in such a way that only authorized persons can read 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 Log Backup Procedures

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 Collection System (Internal vs. External)

Audit processes shall be invoked at system start up, and end only at system shutdown. The audit collection system has to maintain the integrity and availability of all data collected. If data collected are linked to any kind of private information, the audit collection system has to protect

the confidentiality. If necessary, the audit collection system 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.

5.4.7. Event-Causing Subject Notification

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

5.4.8. Vulnerability Assessments

The role in charge of conducting audit and roles in charge of realizing PKI system operation 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.

For vulnerability, the following rules apply:

- Implement detection and prevention organizational and/or technical controls under the control of the OA to protect PKI systems against viruses and malicious software.
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
- Undergo or perform a vulnerability scan (i) after any system or network changes that the PMA determines are significant for CA's component and DC, and (ii) at least once per month, on public and private IP addresses identified by the OA as the PKI's systems (for CA, RA, DC).
- Undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications that the PMA for CA's PKI component determines are significant.
- For online system, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable vulnerability or penetration test; and
- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

5.5. Records Archival

5.5.1. Types of Records Archived

PKI components archived records shall be sufficiently detailed to establish the proper operation of the PKI or the validity of a certificate. At minimum, the following data shall be archived:

- PKI events records:
 - Physical facility access log of OA (one year minimum).
 - Video facility access log of OA (one month according privacy rule in France).
 - Video of key ceremony for CA only (minimum 10 years).
 - Trusted roles management log for OA (minimum 10 years).

- IT access log for OA (5 years minimum).
- CA key creation, use and destruction log (minimum 5 years).
- LTC and PC certificate creation, use and destruction log (minimum 2 years).
- Activation data management log for OA (minimum 5 years).
- IT and network log for OA (minimum 5 years).
- PKI documentation for OA (minimum 5 years).
- Security incident and audit report for OA (minimum 10 years).
- System equipment, software and configuration (minimum 5 years).
- The PMA shall retain all documentation relating to certificate requests and the verification thereof, and all RCA and CA certificates, CRL and TSL thereof, for at least 7 years after any certificate based on that documentation ceases to be valid:
 - PKI audit documentation kept by PMA.
 - CP document kept by PMA.
 - CPS documents kept by PMA.
 - Contract between PMA and different entities kept by PMA.
 - Certificates (or other revocation information) kept by CA.
 - Certificate request records in RCA system.
 - Other data or applications sufficient to verify archive contents.
 - All work related to or from the PMA and compliance auditors.

The CA entity shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

PMA and CA shall retain any audit logs generated in a way to make it available to its auditor upon request.

5.5.2. Archive Retention Period

The minimum retention period for archived data is defined in section 5.5.1. The PMA and CA decide, according the archive owner, to delete or keep all or part of the archives at the end of the retention period of each archive.

5.5.3. Archive Protection

The archives are created in such a way that they cannot be easily deleted or destroyed within their defined retention period. Archive protection ensures that only authorized people can access them.

Archives are held in a manner that ensures integrity, authenticity and confidentiality of data.

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements for Record Time-Stamping

Time stamping services for PKI are not mandatory.

The records and log data have a trusted time defined by the PKI. Details are given in section 6.8.

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 and Verify Archive Information

Media storing PKI archive information are verified upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorized PMA and OA personnel are allowed to access archives.

5.6. Key Changeover

5.6.1. RCA

RCA private key validity period is defined in compliance with cryptographic security recommendations for key size length. RCA certificate has a validity period defined in section 6.3.2.

RCA cannot generate CA certificate whose validity period would be superior to the RCA certificate validity period. A new key pair for RCA requires a new RCA certificate to be generated. Previous RCA certificates shall be used for validation process of the certification path for all CA certificates signed by this previous RCA. Current RCA private key shall be used to sign current CRL and revoke if it is necessary the previous CA signed by the previous RCA.

The PMA reserves rights to take decision to change key at any time.

5.6.2. CA Certificate

The CA private key validity period is defined in compliance with cryptographic security recommendations for key size length. The CA certificate validity period is defined in section 6.3.

The CA cannot generate Certificates whose validity period would be superior to the CA certificate validity period.

The Certificate has a fixed validity period which cannot be changed due to end of life of CA.

Previous CA certificates shall be used for the validation process of the certification path for all Certificates signed by the previous by the previous CA private key.

The PMA reserves the right to change the key at any time.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

This system shall be supported by the PMA computing infrastructure and its incident, compromise and business continuity plans. These plans shall be periodically tested, reviewed and updated, as directed by the PMA and according the risk analysis.

If a PKI component for RCA detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the PMA in order to determine if the PKI needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI has been compromised. In addition, the PMA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the PMA business continuity plan.

Incident, Compromise and Business continuity are covered in the CPS, which may also rely upon other enterprise resources and plans for implementation.

If a PKI component (for CA entity) detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the CA entity in order to determine if the PKI component needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI component has been compromised. In addition, the CA entity determines which services are to be maintained and how, in accordance with the CA entity business continuity plan. CA entity shall alert PMA in case of a compromised PKI component.

Incident, Compromise and Business continuity are covered in the CA entity documentation, which may also rely upon other enterprise resources and plans for implementation.

PMA alerts with precise consequence of the incident Relying Parties and External Entities which are under agreement with PMA for ITS context in order to allow them to activate their own incident management plan.

5.7.2. Corruption of Computing Resources, Software, and/or Data

If PKI equipment is damaged or rendered inoperative, but signature keys are not destroyed, the operation is re-established as quickly as possible, with priority given to the ability to generate certificate status information.

5.7.3. Entity Private Key Compromise Procedures

If a RCA and/or CA key is compromised, lost, destroyed or suspected of being compromised:

- The PMA investigates on the “key-issue” and revokes the associated certificate.
- A new key pair is generated and a new certificate is created.
- The RCA’s entity alerts the CA and External Entity with which an agreement exists.

If a CA key is compromised, lost, destroyed or suspected of being compromised:

- The CA’s entity investigates on the “key-issue” and revokes the associated certificate.
- A new key pair is generated and a new certificate is created.
- The CA’s entity alerts the PMA.

When any of the algorithms, or associated parameters, used by the RCA and/or CA or C-ITS-S becomes insufficient for its remaining intended usage then the PMA shall inform the CA entity and External Entity with which an agreement exists and changes the used algorithms.

5.7.4. Business Continuity Capabilities after Disaster

The business continuity plan addresses all necessary operations as described in section 5.7.1.

5.8. Termination and transfer

5.8.1. RCA

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

- Alerts External Entity with which an agreement exists.
- Revokes all CA certificate under the RCA.
- Destroys the RCA private key.
- Communicates last revocation status information (CRL signed by RCA) to the relying party indicating clearly that it is the latest revocation information.
- CA signed by the RCA stops delivering certificates according to and referring to this CP.
- In case of compromising RCA, PMA and OA both use secure means to notify Relying Parties (RP) and C-ITS-S Manufacturer to delete all trust certificates representing RCA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to termination of the PKI.
- Archived records are transferred to an appropriate authority.

5.8.2. CA

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

- Informs PMA by register letter.
- Destroys the CA private key.
- Transfers its database to entity appointed by PMA.
- Stops to deliver Certificates.
- During the transfer of database and until transfer is fully operational in a new entity, maintains capability to authorize request from PMA.
- In the case of a compromised CA, the CA entity uses secure means to notify Relying Parties and relying parties that they must not trust Certificate identified in the list provided by CA.
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to an entity designated by PMA.

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

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.

RCA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1.1 and 5.1.2.1) by personnel filling trusted roles (refer to section 5.2) under at least dual supervision (Ceremony Master and Security Officer). 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).

Witnesses (RCA representatives) are individuals other than operational personnel who perform the key ceremony. As trusted role, witness can only have "HSM activation" and "Key pair protection" role. RCA activation and initialization are under the control of RCA activation data holders. During the key ceremony, the RCA key pair is backed up (refer to section 6.2).

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

6.1.1.2. LTCA and PCA whom CA's key pair are generated by PMA's OA

After the PMA agrees to the generation of the CA, 2 key pairs and Certificate Request, containing the 2 public keys, are generated for the same CA. One key pair for signature operation and another one for encryption operation.

The operation of the CA key pairs and certificate requests 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.

CA key pairs generation is undertaken and witnessed in a physically secure environment (refer to section 5.1.1.1 and 5.1.2.1) by individuals filling trusted roles (refer to section 5.2) under at least dual supervision (Ceremony Master and Security Officer). Private Key activation data are distributed to activation data holders that are trusted employees. CA keys generation is carried out within a hardware security module (refer to section 6.2). Witnesses, at least one from PMA, are individuals other than the operational personnel who perform the key ceremony. As trusted role, witness can only have "HSM activation" and "Key pair protection" role. CA activation and initialization is under the control of CA activation data holders. During the key ceremony, CA key pairs are backed up (refer to section 6.2).

After key ceremony, CA key pairs are securely transferred to HSM (refer to section 6.2.6.2) in the online environment (refer to section 5.1.1.2 and 5.1.2.1).

The key pair and certificate generation process shall create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. Trail created during key ceremony is done in order to have an Auditor be able to issue a report opining that the RCA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair (refer to section 8.1).

6.1.1.3. C-ITS-S Technical key

C-ITS-S Manufacturer is responsible for the generation in a secured environment of the C-ITS-S technical key. Either C-ITS-S technical key is directly generated inside the C-ITS-S component or outside the C-ITS-S component. When C-ITS-S Manufacturer generates C-ITS-S technical key outside the C-ITS-S component, the generation shall be made in a trusted environment that guarantees confidentiality, integrity and non-disclosure of C-ITS-S technical key. The generation process shall guarantee nothing else than a C-ITS-S component can read in clear text the C-ITS-S technical private key. C-ITS-S Manufacturer shall destroy C-ITS-S technical private key in the generation system used to generate C-ITS-S technical key after having successfully transferred C-ITS-S technical key inside the C-ITS-S component (refer to section 6.2.10. Communication channel to transfer C-ITS-S technical key in the C-ITS-S component shall use trusted channel (refer to section 6.2.6).

6.1.1.4. LTC

The C-ITS-S shall generate the LTC key pair in a way to be sure the private key is under its sole control.

6.1.1.5. PC

The C-ITS-S shall generate the PC key pair in a way to be sure the private key is under its sole control.

6.1.2. Private Key Delivery

Not applicable.

6.1.3. Public Key Delivery to Certificate Issuer

6.1.3.1. RCA

The delivery of RCA public key is done during the key ceremony.

6.1.3.2. LTCA and PCA

CA public keys are securely delivered to the relevant RCA for certificate issuance during key ceremonies (for set up of the PKI, refer to section 6.1.1) or during the registration process (refer

to section 4.1 and 4.2). The delivery mechanism shall bind the CA's verified identity to the public key. If cryptography is used to achieve this binding, it shall be at least as strong as the CA keys used to sign the certificate.

6.1.3.3. LTC

LTC public key is delivered to the LTCA in a signed message by C-ITS-S. C-ITS-S signs the certificate request, containing the LTC public key, with its C-ITS-S technical private key.

6.1.3.4. PC

PC public key is delivered to the PCA in a signed message by C-ITS-S. C-ITS-S signs the certificate request, containing the PC public key, with its C-ITS-S LTC private key.

6.1.4. RCA Public Key Delivery to Relying Parties

Refer to section 2 for downloading and distribution of the RCA certificate.

RCA certificate is also delivered by PMA to C-ITS-S Manufacturer.

C-ITS-S Manufacturer is responsible for personalizing C-ITS-S component with the following data:

- RCA certificate which issued LTCA certificate used by the C-ITS-S Manufacturer;
- DC URL of the RCA;
- LTCA certificate signed by the RCA;
- LTCA URL.

If a C-ITS-S LCM personalizes an C-ITS-S component, then it shall do it with the following data:

- RCA certificate which issued LTCA certificate used by the C-ITS-S Manufacturer with which the ITS LCM has an agreement;
- DC URL of the RCA;
- LTCA certificate signed by the RCA;
- LTCA URL.

6.1.5. Key Sizes and cryptographic algorithm

There are several cryptographic requirements concerning signature algorithm, encryption algorithm and key length (see [ISO/IEC 14516-2] and [ETSI 103 097]) defined in the following paragraphs. In order to ensure the capacity to change cryptographic specification, especially in case of known vulnerabilities or compromised algorithm and to guarantee trusted signed certificates all along the life cycle of the PKI, several cryptographic requirements are defined to provide a crypto-agility capacity.

6.1.5.1. RCA

The key pair algorithm is Elliptic Curves Digital Signature Algorithm (ECDSA) with SHA-256 with a key length of 256 bits (ECDSA_nistP256_with_SHA256).

6.1.5.2. LTCA and PCA

The key pair algorithm is Elliptic Curves Digital Signature Algorithm (ECDSA) with SHA-256 with a key length of 256 bits (ECDSA_nistP256_with_SHA256).

6.1.5.3. ITS-S Technical key

The key pair algorithm is Elliptic Curves Digital Signature Algorithm with SHA-256 with a key length of 256 bits (NIST P-256).

6.1.5.4. LTC

The key pair algorithm is Elliptic Curves Digital Signature Algorithm with SHA-256 with a key length of 256 bits (NIST P-256).

6.1.5.5. PC

The key pair algorithm is Elliptic Curves Digital Signature Algorithm with SHA-256 with a key length of 256 bits (NIST P-256).

6.1.6. Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard [ETSI-TS-103-097] that defines the crypto-algorithm for the parameters that are to be used.

Random numbers for keys shall be generated in FIPS 140-2 Level 3 or Common Criteria EAL 4+ validated hardware cryptographic modules (refer to section 6.2).

6.1.7. Key Usage Purpose

Not applicable.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

The RCA and CAs generates their key pairs and stores their private keys within an HSM that is certified according to the rating specified in section 6.2.11.

ITS-S Manufacturer generates ITS-S key pairs and stores its private keys within an HSM, that is compliant with section 6.2.11.3.

ITS-S generates ITS-S key pairs and stores its private keys within a chip (or security module) that is compliant with section 6.2.11.4.

6.2.2. Private Key (N out of M) Multi-Person Control

6.2.2.1. RCA

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

6.2.2.2. LTCA and PCA

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

6.2.2.3. ITS Technical key

When C-ITS-S Manufacturer generates the C-ITS-S technical key, C-ITS-S Manufacturer implements technical and procedural mechanisms that require the participation of at least one trusted individual authorization to perform sensitive cryptographic operations to personalize C-ITS-S.

6.2.2.4. LTC and PC

C-ITS-S is the sole component authorized to use its private key.

6.2.3. Private Key Escrow

Not applicable.

6.2.4. Private Key Backup

6.2.4.1. RCA

RCA private signature keys shall be backed-up under the same multi-person control (minimum 3) as RCA operational signature operation. All back-up copy of the signature key shall be stored in the RCA off-site location (refer to section 5.1.8) and the number of back-up copy is controlled by trusted roles.

6.2.4.2. LTCA and PCA

CA private signature keys shall be backed-up under the same multi-person control (minimum 2) as the operational ones. All back-up copy of the signature key shall be stored in the CA off-site location (refer to section 5.1.8) and the number of back-up copies is controlled by trusted roles.

6.2.4.3. ITS-S Technical key

Not applicable.

6.2.4.4. LTC and PC

Not applicable.

6.2.5. Private Key Archival

6.2.5.1. RCA

Not applicable.

6.2.5.2. LTCA and PCA

Not applicable.

6.2.5.3. ITS-S Technical key

Not applicable.

6.2.5.4. LTC and PC

Not applicable.

6.2.6. Private Key Transfer into or from a Cryptographic Module

6.2.6.1. RCA Private Key

In case of private key transfer, the RCA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1 by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2).

RCA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored into HSMs, RCA private keys are encrypted. An encrypted RCA 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 filling trusted roles.

6.2.6.2. LTCA and PCA Private Key

In case of private key transfer, then the CA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2.1, by direct token-to-token copy or via a trusted transfer under N out of M multi-person control (Refer to section 6.2.2).

CA 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 filling trusted roles.

6.2.6.3. C-ITS-S Technical key

When C-ITS-S Manufacturer generates C-ITS-S technical key outside the C-ITS-S, the communication path between C-ITS-S and C-ITS-S Manufacturer C-ITS-S technical key generation system shall be protected in a way to guarantee integrity and confidentiality of the C-ITS-S technical key and non-disclosure of the C-ITS-S technical key.

6.2.6.4. LTC and PC

Not applicable.

6.2.7. Private Key Storage on Cryptographic Module

6.2.7.1. RCA

The HSM may store private keys in any form as long as the keys are not accessible without authentication mechanisms compliant with the ones mentioned in the security policy attached to the HSM approved use.

6.2.7.2. LTCA and PCA

The HSM may store CA private keys in any form as long as the keys are not accessible without authentication mechanisms compliant with the ones mentioned in the security policy attached to the HSM approved use.

6.2.7.3. C-ITS-S Technical key

ITS technical private key shall be stored in the C-ITS-S chip.

6.2.7.4. LTC and PC

LTC and PC private key(s) shall be stored in the C-ITS-S chip

6.2.8. Method of Activating Private Key

6.2.8.1. RCA

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

6.2.8.2. LTCA and PCA

Several trusted roles with activation data are required to realize the initial activation of the HSM that contains the key pair corresponding to the CA certificate. Once the HSM containing the CA key are operational, only the authorized services of the PKI system can use the CA key pair within the HSM.

6.2.8.3. C-ITS-S Technical key

C-ITS-S technical private key is only activated by C-ITS-S component.

6.2.8.4. LTC and PC

LTC and PC private keys are only activated by C-ITS-S component.

6.2.9. Method of Deactivating Private Key

6.2.9.1. RCA

RCA HSM that has been activated is never left unattended or otherwise available to unauthorized access. After use, HSM is deactivated. and is removed and stored in a secure location (refer to section 5.1) to avoid its use without authorization and strongly authenticated roles. After deactivation, the use of the HSM based RCA key pair shall require the presence of the trusted roles with the activation data in order to reactivate the said RCA key pair (refer to section 6.2.8.2).

6.2.9.2. LTCA and PCA

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

After use, HSM is deactivated. After deactivation, the use of the HSM based CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said CA key pair (refer to section 6.2.8.3).

The HSM automatically deactivates itself if there is an incident.

6.2.9.3. ITS-S Technical key

ITS-S technical key can only be deactivated by C-ITS-S component.

6.2.9.4. LTC and PC

LTC and PC private key is only deactivated by C-ITS-S component.

6.2.10. Method of Destroying Private Key

6.2.10.1. RCA

Destroying RCA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization (factory reset) function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the RCA 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 5.1 by personnel filling trusted roles (refer to section 5.2) under at least dual control.

6.2.10.2. LTCA and PCA

Destroying CA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization (factory reset) function of the HSM in a manner that any information cannot be used to recover any part of the private key. All the CA 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 5.1) by personnel filling trusted roles (refer to section 5.2) under at least dual control.

6.2.10.3. C-ITS-S Technical key

C-ITS-S technical key cannot be destroyed.

6.2.10.4. LTC and PC

In case of compromising suspicion, C-ITS-S can destroy its LTC and PC key pair.

6.2.11. Cryptographic Module Rating

6.2.11.1. RCA

A cryptographic module shall be used for:

- Generating, using, administering and storing of private keys;
- Generating and using of random numbers;
- Creating backups of the private keys (optional);
- Deletion of private keys;
- The cryptographic module shall be certified with one of the following Protection Profiles (PPs), with the Assurance Level EAL4 or higher:
 - CEN PP HSM 419221-2 Cryptographic Module for CSP Signing Operations with Backup;
 - CEN PP HSM 419221-4 Cryptographic Module for CSP Signing Operations without Backup;

- CEN PP HSM 419221-5 Cryptographic module for Trust Services.

6.2.11.2. LTCA and PCA

See section 6.2.11.1.

6.2.11.3. ITS-S Technical key

The Hardware Security Module used by C-ITS-S Manufacturer, when C-ITS-S Manufacturer generates the C-ITS-S technical key and C-ITS-S chip used to generate C-ITS-S technical key pairs shall be used for:

- Generating, using, administering and storing of private keys,
- Generating and using of random numbers,
- Secure deletion of a private keys,
- The cryptographic module shall be protected against unauthorized removal, replacement and modification,
- The cryptographic module for C-ITS-S shall be assessed using an approved security evaluation scheme according to suitable Protection Profile that shall be based on ISO 15408 standard (Common Criteria).

6.2.11.4. LTC and PC

See section 6.2.11.3.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Public keys are archived as part of certificate archival as described in section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1. RCA

The maximum operational period for an RCA certificate is fixed by RCA certificate validity period. The maximum operational period for an RCA private key is the end validity period of the valid RCA certificate.

6.3.2.2. LTCA and PCA

The maximum operational period for a CA certificate is determined by PMA. For CA, contract between CA's entity and PMA fix the CA validity period.

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

6.3.2.3. C-ITS-S Technical key

C-ITS-S Technical key has no expiration date. It is used as long as C-ITS-S is valid.

6.3.2.4. LTC

LTC private key can be used as long as the associated certificate is valid.

6.3.2.5. PC

PC private key can be used as long as the associated certificate is valid.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

6.4.1.1. RCA

RCA activation data used to protect HSM containing RCA private keys are generated during the initial key ceremony. The activation data used to unlock private keys, in conjunction with any other access control, shall 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.

The PMA appointed individuals shall 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. LTCA and PCA

CA activation data used to protect HSM containing CA 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, shall 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.

The PMA and/or CA's representative, according the owner of the CA, appointed individuals shall 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.

6.4.1.3. C-ITS-S Technical key, LTC and PC

There is no specific activation data as only C-ITS-S is authorized to activate its private key inside the C-ITS-S chip.

6.4.2. Activation Data Protection

6.4.2.1. RCA

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

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

6.4.2.2. LTCA and PCA

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 CA's representative, 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 filling trusted roles. When they are not used, activation data are always stored in safe (refer to section 5.1).

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

6.4.2.3. C-ITS-S Technical key, LTC and PC

Not applicable.

6.4.3. Other Aspects of Activation Data

Activation data are changed in case hardware security modules are returned to manufacturer for maintenance or destroyed. Before sending an HSM for maintenance, all sensitive information contained in the HSM shall be destroyed (refer to section 6.2.10).

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

6.5.1.1. RCA

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

- authenticated logins for trusted role.
- discretionary access control.
- use of authentication for session communication.
- identification of users.

- domain isolation for process regarding roles using PKI services.
- removal of unwanted services from the PKI components.

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

PKI components that are used for RCA key ceremony operation are not connected to any communication network.

Key ceremony workstations are dedicated to key ceremony operations only.

6.5.1.2. LTCA and PCA, RA, and DC

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:

- authenticated logins for trusted roles.
- discretionary access control.
- use of authentication for session communication.
- user identification.
- domain isolation for processes involving roles using PKI services.
- removal of 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.

The following rules apply:

- Follow a documented procedure for appointing individuals to trusted roles and assigning responsibilities to them on each PKI component.
- Document the responsibilities and tasks assigned to trusted roles and implement “separation of duties” for said trusted roles based on the security-related concerns of the functions to be performed on each PKI component.
- Ensure that only personnel assigned to trusted roles have access to PKI components.
- Ensure that an individual in a trusted role acts only within the scope of said role when performing administrative tasks assigned to that role on the PKI component.
- Require employees and contractors to observe the principle of “least privilege” when accessing, or when configuring access privileges on PKI system (refer to section 5.2).
- Require that each individual in a trusted role use a unique credential created by or assigned to that person in order to authenticate to PKI component.
- If an authentication control used by a trusted role is a username and password, then the handling of those authentications shall be performed in accordance with corporate enterprise security policy.
- Require trusted roles to log out from the PKI service of the PKI component and lock workstations when no longer in use.

- Configure workstations with inactivity time-outs that log the user off and lock the workstation after a set time of inactivity without input from the user (PKI components allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock).
- Review all system accounts and deactivate any accounts that are no longer necessary for operations (at least each 90 days).
- If applicable for a PKI component (means only for a PKI component that uses a different access control system than a certificate for a trusted role) lockout account access to the PKI component after no more than a defined maximum value of failed access attempts, provided that this security measure is supported by the PKI component and does not weaken the security of this authentication control.
- Implement a process (technical and/or organizational) that disables all privileged access of an individual to the PKI component within 24 hours upon termination of the individual's (with trusted role) employment or contracting relationship with the PKI component.
- Enforce strong authentication for administrator access to all PKI components.

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:

- Hardware and software shall be purchased in such a way that ensures any component was not tampered with.
- Hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be 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 shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. PKI hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be 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 shall be documented and controlled. A procedure shall be used for installation and ongoing maintenance of the PKI system. The PKI software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be 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 5.4).

6.6.3. Life Cycle Security Controls

For the software and hardware that are evaluated, the OA (in delegation of the PMA) monitors the maintenance scheme requirements to ensure the same level of trust.

6.7. Network Security Controls

6.7.1. RCA

Key ceremony operations for RCA hosted by OA; are performed in an off-line environment. The key ceremony workstation is never connected to any communication network. RCA components are never connected to any kind of network.

6.7.2. LTCA and PCA

The PKI system shall implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be 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 shall 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 shall be 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 (front-end and back-end like N-Thirds architecture shall be in place). Dedicated and distinct networks zones shall be implemented for RA and CA manage by distinct firewalls.

CA is not directly connected to Internet or ITS network. CA shall be accessible only through RA for ITS operational 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 configurations of the PKI system on at least a weekly basis (for CA) to determine whether any changes have violated the PKI component's security policies.
- Grant administration access to PKI components only to persons filling 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

Electronic or manual procedures shall be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4. Key ceremony uses a manual procedure.

For secured time on audit records, all PKI system components shall regularly synchronize with a time service such as Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a PC and LTC Certificate (made electronically with NTP protocol).
- Initial validity time of a RCA and CA Certificate, CRL and TSL (made manually during key ceremony).

7. Certificate, CRL and TSL

7.1. Certificate Profile

7.1.1. Version Number

The version shall be set to 2 for conformance with version 1.2.1 of the [ETSI-TS-103-097] standard.

7.1.2. Certificate Content

The following SubjectAttribute elements shall be included:

- Encryption_key [OPTIONAL]:
 - LTCA: this field shall contain the public key associated to the LTCA private key used to encrypt/decrypt message.
 - PCA: this field shall contain the public key associated to the LTCA private key used to encrypt/decrypt message.
- Verification_key:
 - RCA: this field shall contain the public key associated to the RCA private key used to sign.
 - LTCA: this field shall contain the public key associated to the LTCA private key used to sign.
 - PCA: this field shall contain the public key associated to the PCA private key used to sign.
 - LTC: this field shall contain the public key associated to the LTC private key used to sign.
 - PC: this field shall contain the public key associated to the PC private key used to sign.
- Assurance_level: the assurance level is unknown for the certificate then the default assurance level 0 shall be used.
- Its_aid_list shall have the following content:
 - RCA: "its_aid_list" is not present.
 - LTCA: "CAM" and "DENM".
 - PCA: "CAM", "DENM" and "CAM-I".
 - LTC: "its_aid_list" is not present.
 - PC: "its_aid_list" is not present.
- Its_aid_ssp_list shall be included and shall contain a list of ITS-AIDs with associated Service Specific Permissions (SSP). For each ITS-AID only one ItsAidSsp shall be used with the following data:
 - RCA: "its_aid_ssp_list" is not present.
 - LTCA: "its_aid_ssp_list" is not present.
 - PCA: "its_aid_ssp_list" is not present.
 - LTC: depends on the type of ITS-S and fixed by the LTCA.
 - PC: depends on the type of ITS-S and fixed by the PCA.

Field “signature” for all kind of Certificate holds the signature value of this certificate signed by the responsible CA.

“ValidityRestriction” field shall include “time_start_and_end” with following starting date:

- RCA, LTCA, PCA and LTC: date of Certificate generation.
- PC: Date could be fixed by LTCA and by ITS-S (with prior validation of the LTCA).

The subject_attributes field shall not contain a field of type “reconstruction_value”.

7.1.3. Algorithm Object Identifiers

There is no specific OID to identify the algorithm.

7.1.4. Name Form

Refer to section 3.1.

7.1.5. Name Constraints

Not applicable.

7.1.6. Certificate Policy Object Identifier

Not applicable.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

Not applicable.

7.1.9. Processing Semantics for the Critical Certificate Policy Extension

Not applicable.

7.2. CRL Profile

CRL profile is defined in document [SCOOP.2.4.4.6].

7.3. TSL Profile

TSL profile is defined in document [SCOOP.2.4.4.6].

8. Compliance Audit and Other Assessments

8.1. Frequency or Circumstances of Assessment

Not applicable.

8.2. Identity/Qualifications of Assessor

Not applicable.

8.3. Topics Covered by Assessment

Not applicable.

8.4. Actions Taken as a Result of Deficiency

Not applicable.

8.5. Communication of Results

Not applicable.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

In the context of SCOOP@F Pilot:

- There are no fees for RCA, LTCA and PCA Certificates issuance;
- There are no fees for LTCA services (LTC issuance) and PCA services (PC issuance);

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.

9.1.6. Fines List

Not applicable.

9.2. Financial Responsibility

Not applicable.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

PMA guarantees a special treatment for confidential information.

The treatment of confidential business information provided by CA's representative in the context of submitting a certificate request for CA will be in accordance with the terms of the contract entered into between the CA's entity and PMA.

CA and OA shall maintain the confidentiality of confidential information that is clearly identified 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 CA and OA treats its own most confidential information.

9.3.2. Information Not Within the Scope of Confidential Information

Not applicable.

9.3.3. Responsibility to Protect Confidential Information

PKI components are responsible for protecting the confidential information they possess in accordance with the applicable laws and contracts. PKI components must not disclose certificate or certificate-related information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction as stated in France.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Any collection and any use of personal data by the CAs are made in strict compliance with legislation and regulations in force on the French territory, particularly in relation to the CNIL and the Article 226-13 (Ordinance No 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002) of the Penal Code: " the disclosure of secret information by a person who is depositary by state or profession or because of a function or a temporary mission, is punishable by one-year imprisonment and a fine of 15,000 Euros".

9.4.2. Information Treated as Private

The information considered as personal are:

- Personal data managed by PKI;
- Subscriber information (C-ITS-S identifier).

9.4.3. Information Not Deemed Private

Not applicable.

9.4.4. Responsibility to Protect Private Information

PMA, OA and PKI entity shall have the responsibility to protect private information and shall refrain from disclosing it unless ordered by law enforcement authority.

9.4.5. Notice and Consent to use Private Information

Accordance with the laws and regulations on French territory, personal information submitted to CAs must not be disclosed or transferred to third parties except in the following circumstances: prior consent of the information owner, court order or other legal authorization.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

The disclosure of confidential information is only made to the authorities empowered officially and exclusively on their specific request in accordance with French law.

9.4.7. Other Information Disclosure Circumstances

Not applicable.

9.5. Intellectual Property Rights

The PMA maintain intellectual ownership of RCA and CA certificates that it publishes. This CP is the property of the PMA. Any service mark, trademark or trade name contained within a certificate or certificate application remain the property of its owner. The RCA key-pairs and corresponding certificate are the property of the PMA.

The CA key-pairs and corresponding certificate are the property of CA's entity.

9.6. Representations and Warranties

Not applicable.

9.7. Disclaimers of Warranties

Not applicable.

9.8. Limitations of Liability

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

CA is liable as regards the accuracy of all information contained in the CA certificate and LTC and PC Certificate management.

9.9. Indemnities

PMA makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these RCA and CA certificates at their own risk. PMA has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.10. Term and Termination

9.10.1. Term

This CP and subsequent versions shall be effective upon approval by the PMA.

9.10.2. Termination

If the PKI services ceases to operate, a public announcement must be made by the PMA for Subscriber (using DC information as stated in section 2) for and ITS application software suppliers, through direct communication managed by PMA. Upon termination of service, the PMA should properly archive its records including certificates issued, CP, CPS, CRL and TSL according to section 5.8.

9.10.3. Effect of Termination and Survival

End of validity of the present CP stops all obligation and liability for the PMA. RCA and CA cannot continue delivering certificates referred to by the present CP (refer to section 5.8).

9.11. Individual Notices and Communications with Participants

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

9.12. Amendments

9.12.1. Procedure for Amendment

The PMA reviews CP and CPS at least yearly and each time new requirements are set that have direct impact on the present CP and PKI services. Additional reviews may be enacted at any time at the discretion of the PMA. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. Prior to approving any changes to this CP, PMA notifies PKI components. According change in the CP, some CA certificate may have to be revoked and re-issued, if it is possible according the new rules set in the CP, again according the new rules to be respected.

If the PMA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by PMA. The PMA collects, sums up and proposes CP modifications according to approval procedures.

9.12.2. Notification Mechanism and Period

The PMA notifies PKI components and Relying Parties on its intention to modify CP/CPS no less than 2 months before entering in a modification process of CP/CPS and according to the scope of modification.

9.12.3. Circumstances under Which OID Must Be Changed

Not applicable.

9.13. Dispute Resolution Provisions

Not applicable.

9.14. Governing Law

Subject to any limits appearing in applicable law, the laws of France, shall govern the enforceability, construction, interpretation, and validity of the CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in France. This governing law provision applies only to the CP. Contract with entities incorporating the CP by reference may have their own governing law provisions, provided that this section 9.1.49.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15. Compliance with Applicable Law

The CP is subject to applicable French and European laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information and topics related to privacy and signature.

CA entity and PMA agree to conform to applicable laws and regulations in their contract.

9.16. Miscellaneous Provisions

9.16.1. Force Majeure

PMA shall not be liable for any failure or delay in its performance under the CP due to causes that are beyond its reasonable control, including, but not limited to, 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.

PMA 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 PMA.