Draft v0.9
PKI System Requirements Specifications

- Contents

1 REVISION HISTORY

Version	Update date	Performed by	Comments
0.1	27/07/14	HBA/RBL	Document creation
0.2	16/09/14	HBA/RBL	Plan update
0.3	17/09/14	EAB/HBA/RBL	Uses cases added, requirements aggregated
0.3.1	22/09/14	HBA	Revised after review
0.3.2	25/09/14	EAB/HBA/RBL	Uses cases modified, requirements added
0.4	02/10/14	EAB/HBA/RBL	Requirements added Part 2 and 3 completed (Lamia)

0.5	21/10/14	EAB/HBA/RBL	Uses cases modified Definitions added
0.6	27/10/14	HBA	Use cases diagram changed Sections added in document purpose Section 3.1 added
0.7	12/11/14	HBA/RBL	Use cases added
0.8	18/11/14	HBA/HL/EA	Revised after review
0.9	25/11/14	HBA/EA	Revised after Brigitte Lonc review

2 INTRODUCTION

2.1 Project description

Tomorrow's vehicles and roads will be connected and communicating. This will push the development of new applications to improve traffic management, road safety, mobility and comfort services. Data exchange (between vehicles and vehicles and between vehicles and road infrastructure) will be based on wireless technologies ITS G5 / 802.11p and the IEEE and ETSI standards for aspects related to security. This automobile revolution creates new technological and economic challenges in the automotive industry: the design of interoperable cooperative vehicles, a system of safety management for communications, and the preparation of reliable and secure systems for future connected autonomous vehicles.

These communication systems, called cooperative ITS (Intelligent Transportation System), will require security and digital trust.

Vehicles, roadside units and Cloud services will use digital certificates in order to secure data exchanges and to trust ITS identities.

The objective of the ISE project is to implement security management infrastructure for these cooperative ITS:

- Design security architecture for ITS cooperative systems,
- Develop PKI (Public Key infrastructure) which manages digital certificate lifecycle,
- Define a process and tools to certify the security of ITS embedded systems,

- Experiment and contribute to the standardization regarding ITS security.

2.2 Document purpose

This document first presents use cases of PKI system.
In a second time, this document describes requirements resulting from these use cases.

2.2.1 TOPICS NOT ADDRESSED

Some topics have been set aside in this first version of the document:

- Misbehavior authority is not addressed in this version of document. Its role is not well defined in standards. It was decided to treat this section as a second step.
- Privacy authority is not addressed in this version of document. It was decided to treat this section as a second step.

2.2.2 DESIGN CHOICES

Several proposals not covered by standards were also made and are described in this document:

- Add a new component called the distribution center (DC) to make available lists like TSL or CRL.
- ETSI TS102941 proposes to associate information to an ITS at "manufacture" stage: globally unique canonical identifier and canonical public/private key pair, contact information for the LTCA and PCA (certificates and network addresses), and trusted root certificates. In order to allow for evolution of the PKI system (cross-certification, addition of new PCAs, renewal of CA certificates), a new signed object is created, Trust-service Status List. This list contains new RCA certificates, PCA certificates and PKI service addresses (PCA and DC). This list is signed by the RCA and can be transmitted over the air.

2.3 Terms definition

Actor: systems and classes of people that interact with the system.

Anonymity: ability of a user to use a resource or service without disclosing its identity.

Authentication: is the act of confirming the truth of an attribute of a single piece of data or entity.

Authorization: is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular.

Certificate Policy (CP): gives the security requirements applicable to all PKI services.

Certification Practice Statement (CPS): gives more details on practices enforced by each components participating in the PKI activities.

Certificate Revocation List (CRL): is a list digitally signed by a CA that contains certificates identities that are no longer valid.

Confidentiality: is a set of rules or a promise that limits access or places restrictions on certain types of information.

Eligibility: The fact that an actor meets all the requirements needed to obtain a certificate. It may be the status of ITS Station or the format of request. This term will be defined more precisely later.

Entity: is defined as an element of the system. An entity exists inside the system.

Integrity: means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

Jurisdictional Access: ability to a legal authority to access to the system data in case of dispute.

Permission: right granted to ITS-S to sign specific application messages.

Privacy: provide a user protection against discovery and misuse of identity by other users. Privacy is decomposed into four keys: anonymity, pseudonymity, unlinkability and unobservability.

Pseudonymity: ability of a user to use a resource or service without disclosing its user identity while still being accountable for that use.

Traceability: capability of keeping track of a given set or type of information to a given degree.

Trust-service Status List (TSL): is a signed list of trust services (RCA certificates, PCA certificates and PKI services addresses, etc.).

Unlinkability: ability of a user to make multiple uses of resources or services without others being able to link these uses together.

Unobservability: ability of a user to use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

2.4 List of abbreviations

CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ITS	Intelligent Transport System
ITS-S	ITS Station
LTC	Long Term Certificate
LTCA	Long Term Certificate Authority
MA	Misbehavior Authority
PC	Pseudonym Certificate
PCA	Pseudonym Certificate Authority
PKI	Public Key Infrastructure
RCA	Root Certificate Authority
TPK	Technical Public Key
TSL	Trust-service Status List
UI	Unique Identifier

3 OPERATIONAL CONCEPT

3.1 Public Key Infrastructure (PKI) basics

3.1.1 WHAT IS A DIGITAL CERTIFICATE?

A digital certificate is a secure digital identity that certifies the identity of the holder – person, device, or organization. Issued by a Certification Authority, it typically contains a user's name, public key, and related information. A digital certificate is tamper-proof and cannot be forged, and is signed by the private key of the Certification Authority which issued it. Any change made to the certificate

after the signature of the authority would be detected once the signature is verified.

Usages of certificate are multiple:

- Strong authentication
- Electronic signature
- Encryption of data

3.1.2 WHAT IS A PUBLIC KEY INFRASTRUCTURE?

A PKI (Public Key Infrastructure) is a set of technical, organizational, and human means that enable a Certification Authority to issue digital certificates. The certificates (and associated cryptographic keys) are the vectors of trust. They enable strong guarantees to be implemented:

- Through use of robust cryptographic techniques

- Through secure and documented procedures of issuance and management

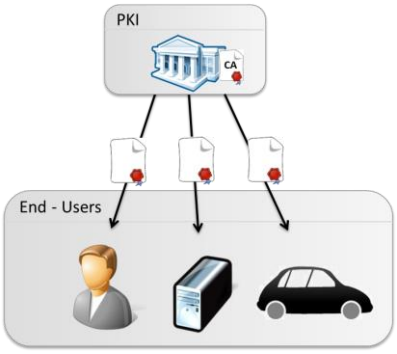

FIGURE 1: PKI END-USERS

As shown in the figure 1, the PKI can issue digital certificates for different types of end-users. ITS Stations are the end-users of the PKI system described in this document.

3.1.3 PUBLIC KEY INFRASTRUCTURE FOR ITS

LTCA	Long Term CA
PCA	Pseudonym CA
LTC	Long Term Certificate
PC	Pseudonym Certificate

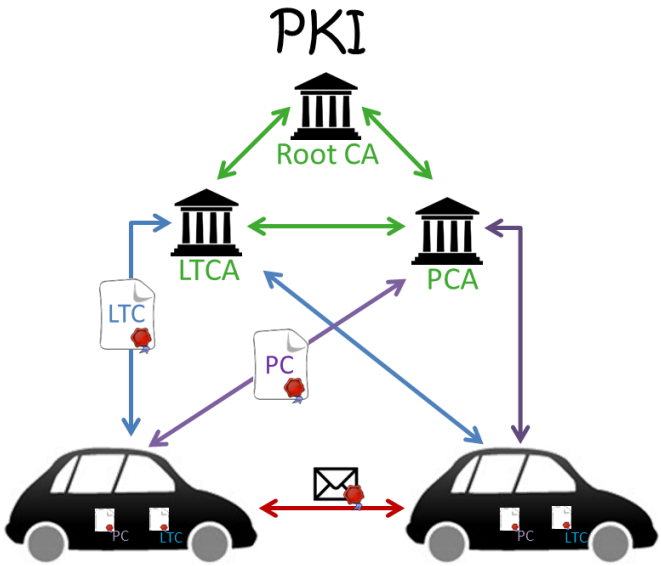

FIGURE 2: PKI FOR ITS

ETSI standards specify trust and privacy management for Intelligent Transport System (ITS) communications.

Trust and privacy management requires secure establishment and maintenance of trust relationships between communicating ITS stations (including revocation when applicable): this may be enabled using security parameters such as identity or properties which are guaranteed by trusted third parties (Certification Authority) : certificates for proof of identity named Long Term Certificate or others such as Pseudonym Certificates (PC). Public key certificates and Public Key Infrastructure (PKI) are used to establish and maintain trust between the ITS-S and between ITS-S and authorities.

The PKI system proposed in this document comprises a hierarchy of CA compliant with the ETSI standards.

3.2Initial architecture

PKI core system for ITS consists of four entities (Figure 3):

- Root certificate authority (RCA)
- Long-Term certificate authority (LTCA)
- Pseudonym certificate authority (PCA)
- Distribution Center (DC)

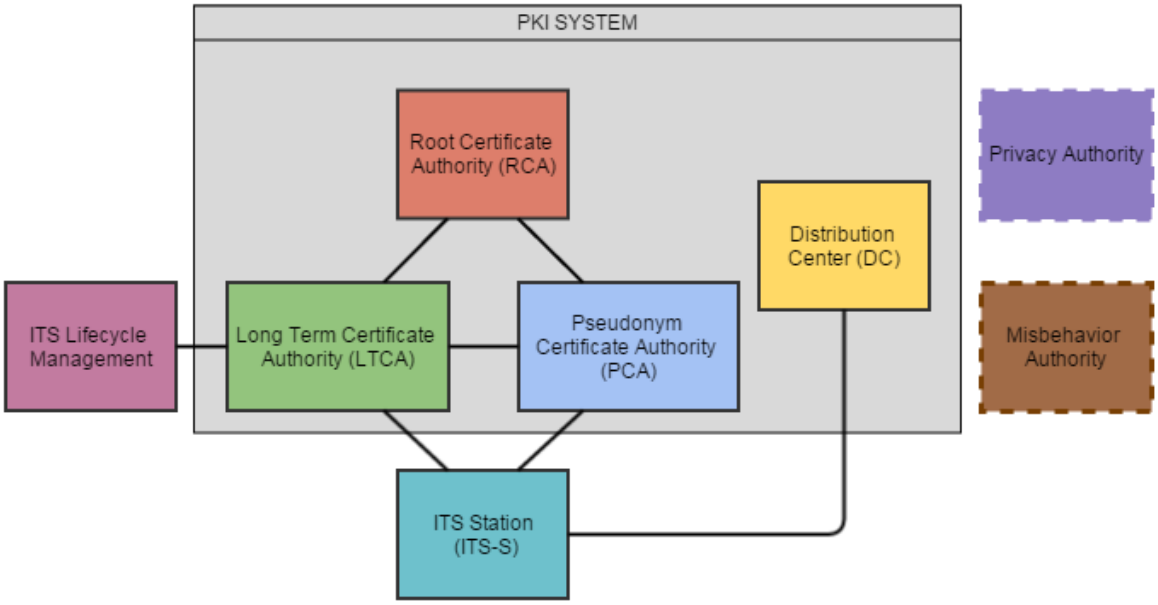

FIGURE 3: MODEL OF PKI SYSTEM

3.3 PKI entities

Entities	Description
Root Certificate Authority (Root CA or RCA)	RCA is the root of trust for all certificates within the PKI hierarchy. Root CA issues certificates for LTCAs and PCAs to authorize them to issue certificates to end entities. It also defines and controls policies among all certificate issuers. The Root CA is required when a new LTCA or PCA shall be created, or when the lifetime of an LTCA or PCA certificate expires.
Long Term Certificate Authority (LTCA)	LTCA issues for each requesting ITS-S a LTC that is valid for a long period. This LTC is used to identify and authenticate the ITS-S within the PKI, and never used in V2X communication for privacy reasons. NOTE: Identified as Enrolment Authority in ETSI Standards.
Pseudonym Certificate Authority (PCA)	PCA issues short lifetime certificates called PC, which are used in V2X communications. Having received the LTC, the ITS-S requests its pseudonym certificate(s) from the PCA. These certificates allow the ITS-S to have specific permissions. The PCA guarantees privacy of requesting ITS-S since it's technically and operationally separated from the LTCA, which is the only authority that knows the real identity of the ITS-S.

	NOTE: Identified as Authorization Authority in ETSI Standards.
Distribution Center (DC)	DC provides ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorized ITS-S or PKI certification authority.

3.4System actors

Actors	Description
ITS Station (ITS-S)	ITS-S is end-user of the system. The system provides it different certificates (LTC or PC) to allow secure communications. ITS-S can be normal vehicles, public safety vehicles, roadside stations, nomadic devices and traffic management centers…
ITS Lifecycle Management	ITS Lifecycle Management manages the lifecycle of ITS-S. ITS Lifecycle Management registers ITS-S in LTCA to allow ITS-S requesting PC and LTC.
Misbehavior Authority (MA)	MA is responsible for processing misbehavior reports and deciding that an ITS-S should be revoked. MA has the ability to detect misused certificates and misbehaving stations and also the ability to revoke misbehaving stations privileges to send messages that others will trust. To help detect misbehaving ITS-S, ITS-S may be required to report misbehaviors they have detected to the MA. *This actor is not addressed in this version of document.*
Privacy Authority (PA)	PA is an authority able to reverse pseudonymity of ITS-S through collaboration with LTCA and PCA. *This actor is not addressed in this version of document.*

3.5 Functionalities

The use cases diagram (Figure 4) reflects only actors addressed in this version of document.

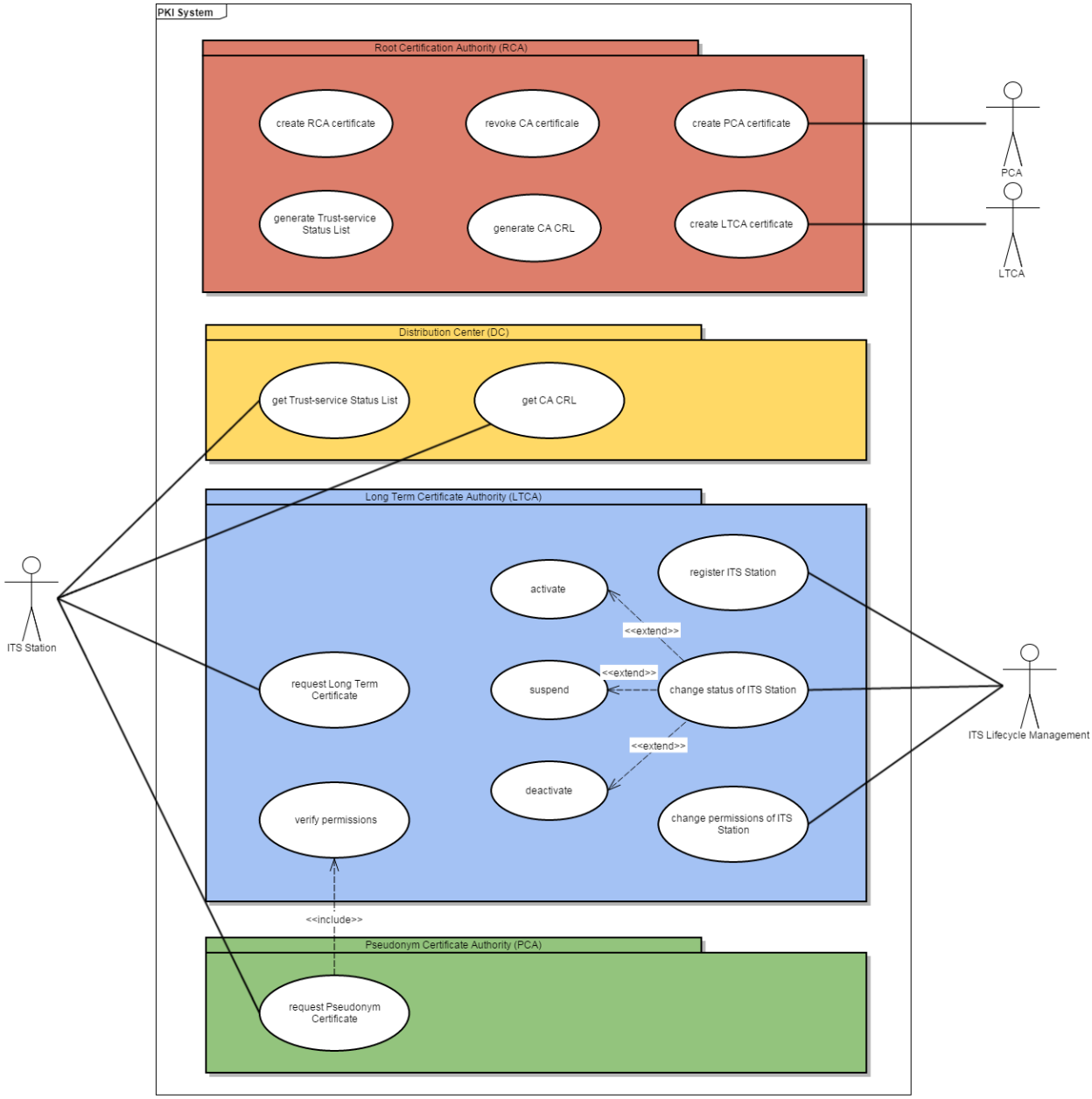

FIGURE 4: USE CASES DIAGRAM OF PKI SYSTEM

3.5.1 RCA COMPONENT FEATURES

A RCA is a CA which is characterized by having itself as the issuer (i.e., it is self-signed). RCA can't be revoked in the normal manner (i.e. being included in an Certificate Revocation List), and, when used as a Trust Anchor must be transmitted or made available to any ITS Station according to secure mechanisms.

RCA is always used and protected offline. RCA is never connected to any network.

The RCA operates its services according to a Certificate Policy (CP) and its corresponding Certification Practice Statement (CPS).

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

The features of RCA component are:

- Creation of RCA key pair and self-signed certificate;
- Issuance of CA (LTCA or PCA) certificates;
- Revocation of CA (LTCA or PCA) certificates;
- Generation of CA CRL;
- Generation of TSL.

3.5.2 LTCA COMPONENT FEATURES

LTCA component implements production of LTC.

The features of LTCA component are:

- Registration of ITS-S
- Management of ITS-S status
- Management of ITS-S permissions
- Issuance of LTC certificates
- Verification of ITS-S permissions for PC request

LTCA component is on-line component from the point of view of the ITS-S, ITS Lifecycle Management and PCA..

3.5.3 PCA COMPONENT FEATURES

PCA component implements PC lifecycle management.

The features of PCA component are:

- Issuance of PC certificates.

PCA component is on-line component from the point of view of the actors.

3.5.4 DC COMPONENT FEATURES

DC component implements the publication of lists like TSL or CRL.

The features of PCA component are:

- Publication of TSL
- Publication of CA CRL

DC component is on-line component from the point of view of the actors.

4 USE CASES ANALYSIS

4.1 Use case 1: create RCA certificate

The RCA component generates new key pair and creates a self-signed certificate.

4.2 Use case 2: create LTCA certificate

4.2.1 SEMI-FORMAL DESCRIPTION

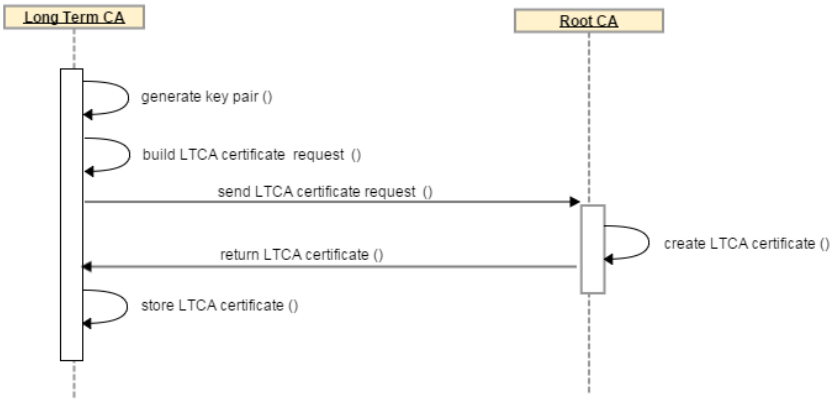

FIGURE 5: CREATE LTCA CERTIFICATE

4.2.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-02*
Use Case Name:	Create LTCA certificate
Priority:	Mandatory
Related Requirement:	

Primary Actor	Long Term Certificate Authority
Description	LTCA requests to RCA a LTCA certificate.
Preconditions	-
Success End Condition	LTCA has a certificate issued by RCA.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) LTCA generates key pair. 2) LTCA builds LTCA certificate request. 3) LTCA sends LTCA certificate request. 4) RCA creates LTCA certificate. 5) RCA returns LTCA certificate. 6) LTCA stores LTCA certificate.
Extensions	-

Variations (Alternatives)	–		
Includes	–		
Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	
Confidentiality		**Jurisdictional Access**	**X**
Integrity	**X**		
Traceability	**X**		

4.3Use case 3: create PCA certificate

4.3.1 SEMI-FORMAL DESCRIPTION

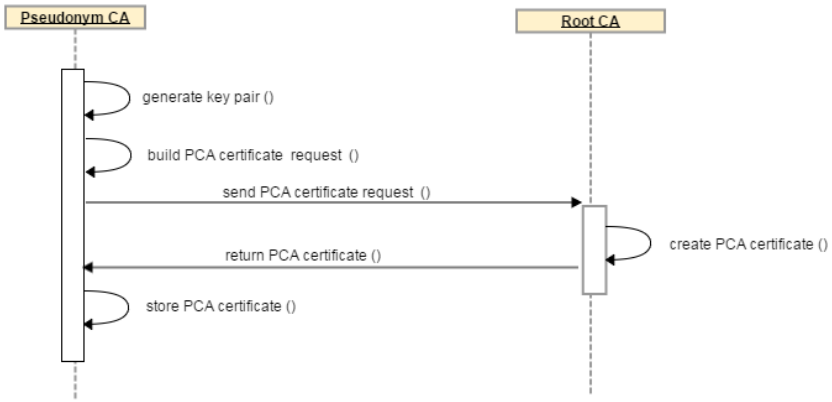

FIGURE 6: CREATE PCA CERTIFICATE

4.3.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-03*
Use Case Name:	Create PCA certificate
Priority:	Mandatory
Related Requirement:	

Primary Actor	Pseudonym Certificate Authority
Description	PCA requests to RCA a PCA certificate.

Preconditions	–
Success End Condition	PCA has a certificate issued by RCA.
Failed End Condition	–
Involved components	–
Main Success Scenario	1) PCA generates key pair. 2) PCA builds PCA certificate request. 3) PCA sends PCA certificate request. 4) RCA creates PCA certificate. 5) RCA returns PCA certificate. 6) PCA stores PCA certificate.
Extensions	–
Variations (Alternatives)	–
Includes	–

Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	
Confidentiality		**Jurisdictional Access**	**X**
Integrity	**X**		
Traceability	**X**		

4.4Use case 4: revoke CA certificate

The RCA component revokes CA certificate.

4.5Use case 5: generate CA CRL

The RCA component generates the CA CRL. The format of CRL will be detailed in the technical specifications of the PKI.

4.6Use case 6: generate Trust-service Status List

The RCA component generates the Trust-service Status List.

The format of TSL will be detailed in the technical specifications of the PKI.

4.7Use case 7: request Long Term Certificate

4.7.1 SEMI-FORMAL DESCRIPTION

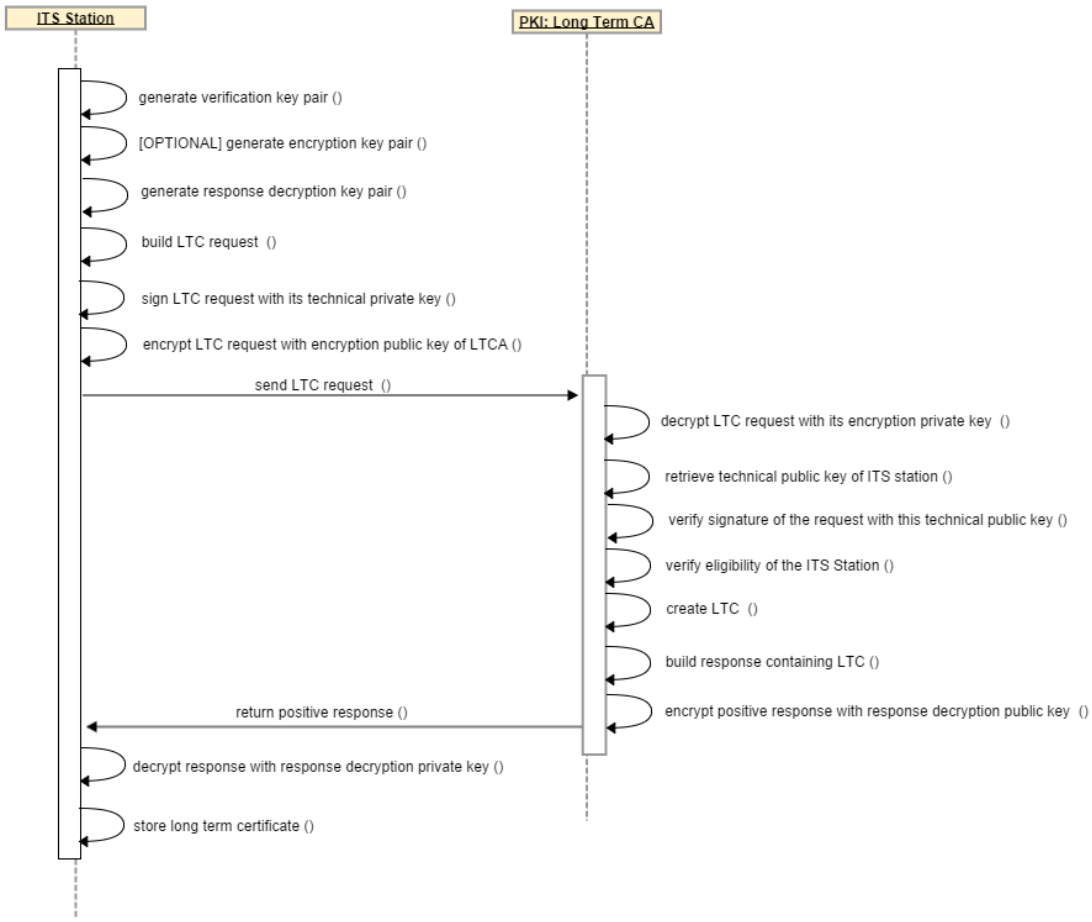

FIGURE 7: REQUEST LONG TERM CERTIFICATE

4.7.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-07*
Use Case Name:	Request long term certificate
Priority:	Mandatory
Related Requirement:	

Primary Actor	ITS Station

Description	ITS Station wants to request long term certificate
Preconditions	ITS Station has its technical key pair, a unique identifier, the address of the LTCA and LTCA certificate. ITS Station is registered in internal database of LTCA.
Success End Condition	ITS Station has new LTC.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) ITS Station generates verification key pair. 2) ITS Station generates response decryption key pair. 3) ITS Station builds LTC request. 4) ITS Station signs this request with its technical private key. 5) ITS Station encrypts this request with encryption public key of LTCA. 6) ITS Station sends this request to LTCA. 7) LTCA decrypts LTC request with its encryption private key. 8) LTCA retrieves from its internal database the technical public key corresponding to the unique identifier of ITS Station. 9) LTCA verifies the signature of the request with this technical public key. 10) LTCA verifies the eligibility of ITS Station. 11) If ITS Station is eligible, LTCA creates the LTC. 12) LTCA builds a positive response containing the created LTC. 13) LTCA encrypts this positive response with response decryption public key to ITS Station. 14) LTCA returns this positive response to ITS Station. 15) ITS Station decrypts this positive response with response decryption private key. 16) ITS Station stores the LTC.
Extensions	10) If ITS Station is not eligible, LTCA doesn't create the LTC. 11) LTCA builds a negative response with a reason. 12) LTCA encrypts this negative response with the response decryption public key to ITS Station. 13) LTCA returns this negative response to ITS Station. 14) ITS Station decrypts this negative response with response.
Variations	ITS Station could also generate encryption key pair and

(Alternatives)	request an LTC containing two key usages.
Includes	

Security Characteristics			
Authentication/ Authorization	X	Anonymity/ Privacy	
Confidentiality	X	Jurisdictional Access	
Integrity	X		
Traceability	X		

4.8Use case 8: request Pseudonym Certificate

4.8.1 SEMI-FORMAL DESCRIPTION

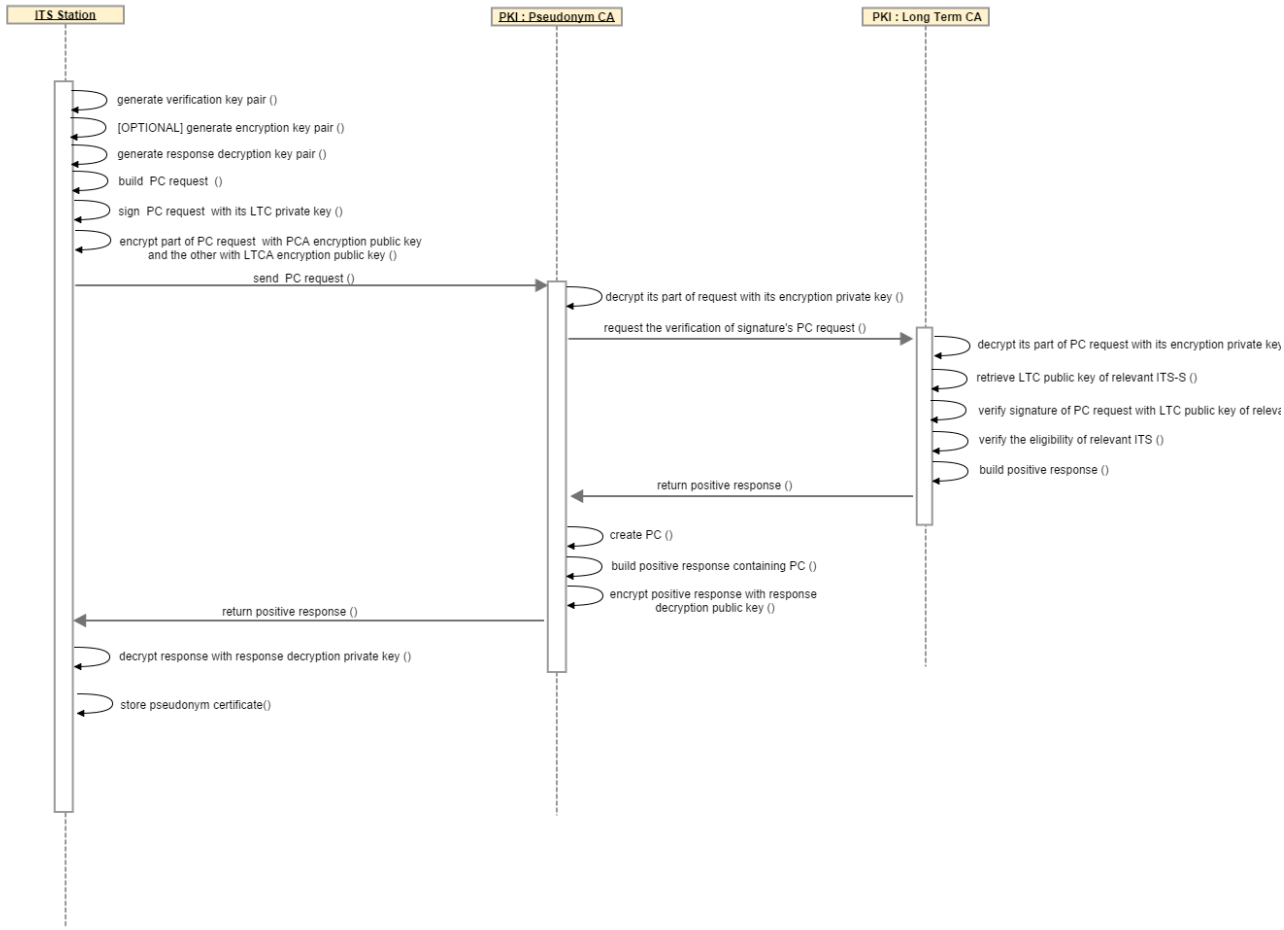

FIGURE 8: REQUEST PSEUDONYM CERTIFICATE

4.8.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-08*
Use Case Name:	Request pseudonym certificate
Priority:	Mandatory
Related Requirement:	

Primary Actor	ITS Station
Description	ITS Station wants to request pseudonym certificate
Preconditions	ITS Station has a LTC and its associated private key, a unique identifier, the address of PCA, PCA certificate and LTCA certificate (and its position?)
Success End Condition	ITS Station has new PC.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) ITS Station generates verification key pair. 2) ITS Station generates response decryption key pair. 3) ITS Station builds PC request. 4) ITS Station signs the PC request with its LTC private key. 5) ITS Station encrypts part of request with PCA encryption public key and the other part with LTCA encryption public key. 6) ITS Station sends this request to PCA. 7) PCA decrypts its part of the request with its encryption private key. 8) PCA requests to LTCA to verify the signature of PC request. 9) LTCA decrypts its part of request with its encryption private key. 10) LTCA retrieves LTC public key of relevant ITS Station. 11) LTCA verifies the signature of PC request with LTC public key of relevant ITS-S. 12) LTCA verifies the eligibility of relevant ITS Station. 13) If the ITS Station is eligible, LTCA builds a positive response to PCA. 14) LTCA returns positive response to PCA. 15) PCA creates a PC.

	16) PCA builds positive response containing the created PC. 17) PCA encrypts this positive response with response decryption public key to ITS Station. 18) PCA returns this positive response to ITS Station. 19) ITS Station decrypts this positive response with response decryption private key. 20) ITS Station stores PC.
Extensions	13) If ITS Station is not eligible, LTCA builds a negative response to PCA. 14) LTCA returns this negative response to PCA. 15) PCA doesn't create a PC. 16) PCA builds the negative response with a reason. 17) PCA encrypts this negative response with response decryption public key to ITS Station. 18) PCA returns this negative response to ITS Station. 19) ITS Station decrypts negative response with response decryption private key.
Variations (Alternatives)	1) ITS Station could also generate encryption key pair and request a PC containing two key usages. 2) ITS-S generates multiple verification key pairs and sends a PC request to obtain multiple PCs from the PCA.
Includes	UC-ISE-07

Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	**x**
Confidentiality	**X**	**Jurisdictional Access**	
Integrity	**X**		
Traceability	**X**		

4.9Use case 9: register ITS Station

4.9.1 SEMI-FORMAL DESCRIPTION

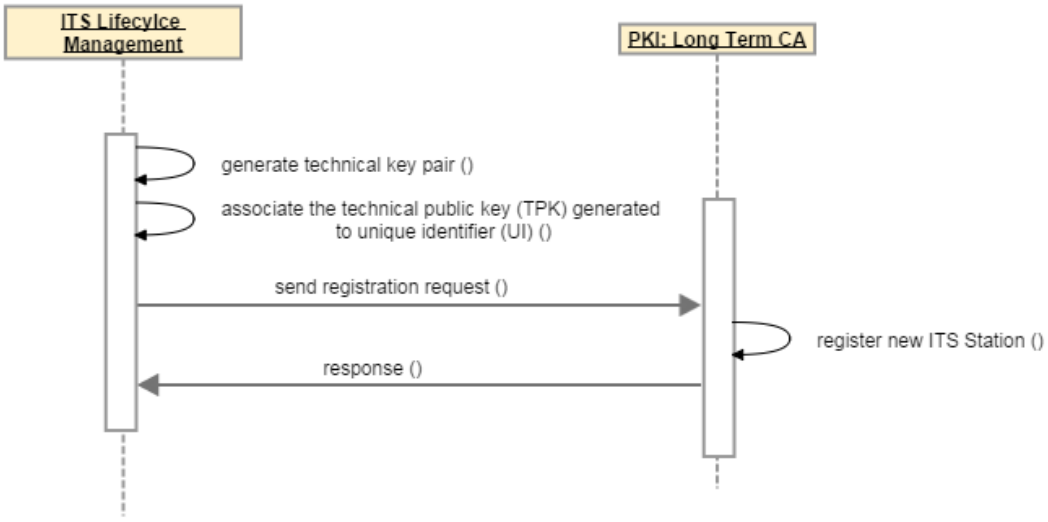

FIGURE 9: REGISTER ITS STATION

4.9.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-09*
Use Case Name:	Register ITS Station
Priority:	*Mandatory*
Related Requirement:	

Primary Actor	ITS Lifecycle Management
Description	ITS Lifecycle Management wants to register ITS Station
Preconditions	-
Success End Condition	ITS Station is registered in internal database of LTCA (status?)
Failed End Condition	-
Involved components	-
Main Success Scenario	1) ITS Lifecycle Management generates the technical key pair. 2) ITS Lifecycle Management associates the technical public key (TPK) to the unique identifier of ITS Station. 3) ITS Lifecycle Management sends registration request to LTCA. 4) LTCA verifies that technical public key or unique identifier is

	not already registered in its internal database. 5) LTCA registers new ITS Station. 6) LTCA returns positive response to ITS Lifecycle Management.
Extensions	5) If technical public key or unique identifier is already registered, LTCA doesn't register ITS Station. 6) LTCA returns negative response with a reason.
Variations (Alternatives)	–
Includes	–

Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	
Confidentiality	**X**	**Jurisdictional Access**	
Integrity	**X**		
Traceability	**X**		

4.10 Use case 10: change state of ITS Station

4.10.1 SEMI-FORMAL DESCRIPTION

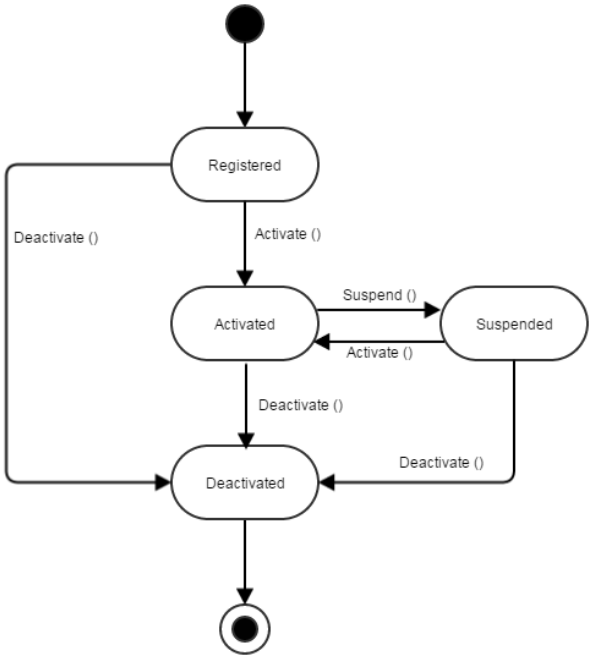

FIGURE 10: STATE DIAGRAM OF ITS STATION

ITS Station passes through a series of states during its life cycle. The figure 8 describes these different states.

States	Description
Registered	ITS Station is registered in internal database of LTCA.
Activated	ITS-S is activated once registered with the LTCA to be allowed to obtain pseudonyms certificates.
Suspended	ITS-S could be suspended for different reasons. This state doesn't allow ITS-S to request pseudonyms certificates.
Deactivated	In case of end life or following a compromise, ITS-S is deactivated.

FIGURE 11 : DESCRIPTION OF ITS STATES

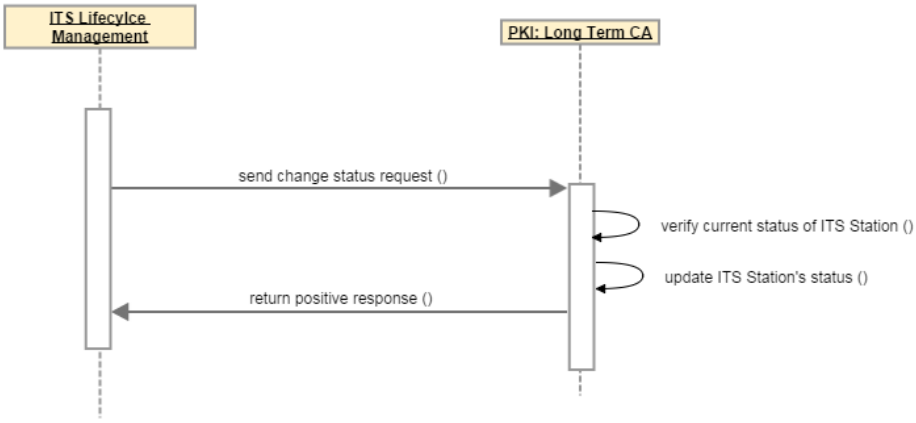

FIGURE 12 : CHANGE STATUS OF ITS STATION

4.10.1 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-10*
Use Case Name:	Change status of ITS Station
Priority:	Mandatory
Related Requirement:	

Primary Actor	ITS Lifecycle Management
Description	ITS Lifecycle Management wants to change status of ITS Station.

Preconditions	ITS Station is registered in internal database of LTCA. ITS Lifecycle Management has the address of LTCA.
Success End Condition	ITS Station status is changed.
Failed End Condition	ITS Station status is unchanged.
Involved components	-
Main Success Scenario	1) ITS Lifecycle Management builds request for changing status of ITS Station. 2) ITS Lifecycle Management sends this request to LTCA. 3) LTCA verifies current status of ITS station. 4) LTCA updates ITS Station's status. 5) LTCA returns a positive response to ITS Lifecycle Management.
Extensions	4) If ITS Station status could not be changed, LTCA doesn't update ITS Status's status. 5) LTCA returns negative response with a reason.
Variations (Alternatives)	-
Includes	UC-ISE-09

Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	
Confidentiality	**X**	**Jurisdictional Access**	
Integrity	**X**		
Traceability	**X**		

4.11 Use case 11: change permissions of ITS Station

4.11.1 SEMI-FORMAL DESCRIPTION

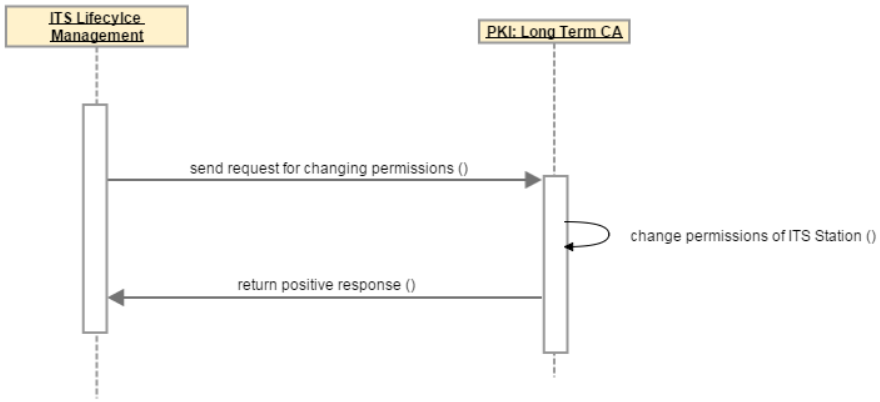

FIGURE 13: CHANGE PERMISSIONS OF ITS STATION

4.11.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-11*
Use Case Name:	Change permissions of ITS Station
Priority:	*Mandatory*
Related Requirement:	

Primary Actor	ITS Lifecycle Management
Description	ITS Lifecycle Management wants to change permissions of ITS Station.
Preconditions	-
Success End Condition	Permissions of ITS Station are changed.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) ITS Lifecycle Management sends request to LTCA. 2) LTCA changes permissions of ITS Station. 3) LTCA returns positive response to ITS Lifecycle Management.
Extensions	-

Variations (Alternatives)	-
Includes	UC-ISE-09

Security Characteristics			
Authentication/ Authorization	**X**	**Anonymity/ Privacy**	
Confidentiality	**X**	**Jurisdictional Access**	
Integrity	**X**		
Traceability	**X**		

4.12 Use case 12: get Trust-service Status List

4.12.1 SEMI-FORMAL DESCRIPTION

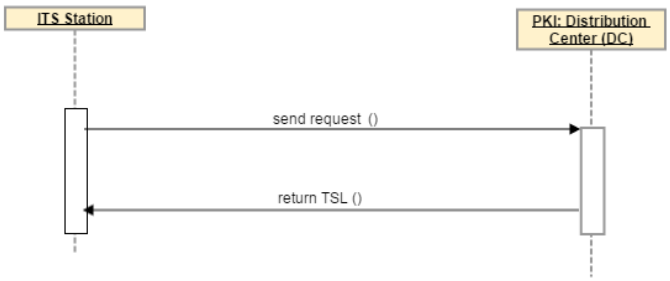

FIGURE 14: GET TRUST-SERVICE STATUS LIST

4.12.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-12*
Use Case Name:	Get Trust-service Status List
Priority:	*Mandatory*
Related Requirement:	

Primary Actor	ITS Station
Description	ITS Station wants to update its internal signed list of trust services (RCA certificates, PCA certificates and PKI services addresses, etc.).

Preconditions	–
Success End Condition	TSL is delivered to ITS Station.
Failed End Condition	–
Involved components	–
Main Success Scenario	1) ITS Station sends request to DC. 2) DC returns TSL.
Extensions	–
Variations (Alternatives)	–
Includes	–

Security Characteristics			
Authentication/ Authorization		**Anonymity/ Privacy**	
Confidentiality		**Jurisdictional Access**	
Integrity	**X**		
Traceability			

4.13 Use case 13: get CA CRL

4.13.1 SEMI-FORMAL DESCRIPTION

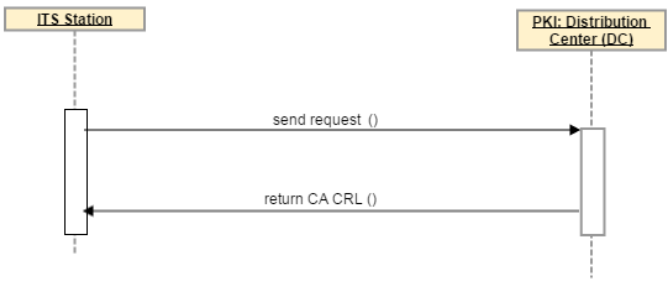

FIGURE 15: GET CA CRL

4.13.2 DETAILED DESCRIPTION

Use Case ID:	*UC-ISE-13*
Use Case Name:	Get CA CRL
Priority:	*Mandatory*
Related Requirement:	

Primary Actor	ITS Station
Description	ITS Station wants
Preconditions	-
Success End Condition	CA CRL is delivered to ITS Station.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) ITS Station sends request to DC. 2) DC returns CA CRL.
Extensions	-
Variations (Alternatives)	-
Includes	-

Security Characteristics			
Authentication/ Authorization		**Anonymity/ Privacy**	
Confidentiality		**Jurisdictional Access**	
Integrity	**X**		
Traceability			

5 SYSTEM REQUIREMENTS

Relevance:

- **Critical – C:** Must be implemented
- **Significant – S:** Should

- **Of Interest – I:** May

Priority:

- **M** = Mandatory
- **O** = Optional

5.1 Functional requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
Functional				
REQ-FUN-1	LTCA MUST be able to issue LTC to ITS-S.	C	M	UC-ISE-07
REQ-FUN-2	PCA MUST be able to issue PC to ITS-S.	C	M	UC-ISE-08
REQ-FUN-3	LTCA MUST be able to verify PC request.	C	M	UC-ISE-08
REQ-FUN-4	LTCA MUST be able to register ITS-S.	C	M	UC-ISE-09
REQ-FUN-5	LTCA MUST be able to suspend temporarily ITS-S.	C	M	UC-ISE-10
REQ-FUN-6	LTCA MUST be able to deactivate permanently ITS-S.	C	M	UC-ISE-10
REQ-FUN-7	LTCA MUST be able to activate ITS-S.	C	M	UC-ISE-10
REQ-FUN-8	DC MUST be able to provide TSL.	C	M	UC-ISE-12
REQ-FUN-9	DC MUST be able to provide CA CRL.	C	M	UC-ISE-13
REQ-FUN-10	RCA MUST be able to create RCA certificate.	C	M	UC-ISE-01
REQ-FUN-11	RCA MUST be able to create LTCA certificate.	C	M	UC-ISE-02
REQ-FUN-12	RCA MUST be able to create PCA certificate.	C	M	UC-ISE-03
REQ-FUN-13	RCA MUST be able to generate TSL.	C	M	UC-ISE-06
REQ-FUN-14	RCA MUST be able to generate CA CRL.	C	M	UC-ISE-05

5.2 Security requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases

Security				
REQ-SEC-1	Communications MUST be protected in integrity.	C	M	All except UC-ISE-12 and UC-ISE-13
REQ-SEC-2	Communications MUST be protected in confidentiality.	C	M	All except UC-ISE-12 and UC-ISE-13
REQ-SEC-3	Communications MUST be protected in authenticity.	C	M	All except UC-ISE-12 and UC-ISE-13
REQ-SEC-4	Internal database of LTCA, PCA SHOULD be protected in integrity.	S	O	UC-ISE-07, UC-ISE-08, UC-ISE-09, UC-ISE-10, UC-ISE-11
REQ-SEC-5	LTCA SHOULD verify unicity of ITS-S canonical public key.	S	O	UC-ISE-09
REQ-SEC-6	LTCA MUST verify unicity of ITS Station canonical identifier.	C	M	UC-ISE-09
REQ-SEC-7	PKI System MUST be designed in a way to respect n-tier architecture model.	C	M	

5.3 Privacy requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
Privacy				
REQ-PRI-1	PCA MUST NOT be able to identify the ITS-S transmitting the PC request.	C	M	UC-ISE-08
REQ-PRI-2	LTCA MUST NOT be able to read content of PC request.	C	M	UC-ISE-08

REQ-PRI-3	PCA MUST NOT be able to link a PC with ITS-S.	C	M	UC-ISE-08
REQ-PRI-4	PCA MUST NOT be able to link PCs as belonging to a same ITS-S.	C	M	UC-ISE-08
REQ-PRI-5	LTCA MUST NOT be able to link a PC with ITS-S.	C	M	UC-ISE-08
REQ-PRI-6	LTCA MUST NOT link PCs as belonging to a same ITS-S.	C	M	UC-ISE-08

5.4 Performance and scalability requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
Performance & Scalability				
REQ-PER-1	PCA MUST provide PC to ITS-S in less than X seconds. Remark: The time values (X) will be added later when realistic times are available)	S	M	UC-ISE-08
REQ-PER-2	PCA and LTCA MUST accept more than X simultaneous connections.	S	M	UC-ISE-08
REQ-PER-3	PCA and LTCA MUST support more than X transactions per second.	S	M	UC-ISE-08
REQ-PER-4	PKI System MUST support more than X requests.	S	M	
REQ-PER-5	PKI System MUST support horizontal scalability.	S	M	
REQ-PER-6	PKI System SHOULD support vertical scalability.	S	M	
REQ-PER-7	PKI System SHOULD be fault resilient.	S	M	
REQ-PER-8	PKI System MUST support general crypto-agility concept, to be more robust and adaptive to the evolution of crypto-analysis attacks (crypto-agility such as increasing the crypto key size or changing the crypto curve	C	M	all

	to a safer one).			

5.5Norms and standards requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
Norms & Standards				
REQ-NOR-1	Certificate format MUST be compliant with REF ETSI TS 103097 [3]	C	M	
REQ-NOR-2	Enrollment and Authorization management services MUST be compliant to ETSI TS 102 941 [2] NOTE: v1.1.3 is the latest available draft.	C	M	UC-ISE-07, UC-ISE-08

5.6Others requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
Interfaces				
System Operations				
Policies & Regulations				
REQ-POL-1	All organizational requirements MUST be done according to RCA policy The RCA MUST operates its services according to a Certificate Policy (CP) and its corresponding Certification Practice Statement (CPS).	C	M	all

6 REFERENCES

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area.

[2] ETSI TS 102 941: ITS; Security; Trust and Privacy Management

[3] ETSI TS 103 097: ITS; Security; Security header and certificate formats

[4] ETSI TS 102 940: ITS; Security; ITS communications security architecture and security management