PKI system requirements specifications (v1.1)

This is the first deliverable of task 2 (ISE Project).

March 2015

IRT SystemX
8, avenue de la Vauve
91120 Palaiseau
contact@irt-systemx.fr
www.irt-systemx.fr
Tél. : +33 (0)1 69 08 05 68

PUBLIC

Revision History

Version number	Update date	Main authors	Summary of changes
1.0	16/12/14	Hafeda BAKHTI (IDNOMIC) Erwann ABALEA (IDNOMIC) Rémi BLANCHER (IDNOMIC) Brigitte LONC (RENAULT) Houda LABIOD (TELECOM PARISTECH)	First stable version
1.1	11/03/15	Hafeda BAKHTI (IDNOMIC) Erwann ABALEA (IDNOMIC)	Changing terminology of entities in accordance with ETSI standards

Table of contents

1 Introduction

1.1 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.

1.2 Document purpose

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

1.2.1 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.

1.2.2 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

EC and AA (certificates and network addresses), and trusted root certificates. In order to allow for evolution of the PKI system (cross-certification, addition of new AAs, renewal of CA certificates), a new signed object is created, Trust-service Status List. This list contains new RCA certificates, EA and AA certificates and PKI service addresses (AA and DC). This list is signed by the RCA and can be transmitted over the air.

1.3 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, 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.

1.4 List of abbreviations

Abbreviations	Synonyms	Description
CP		Certificate Policy
CPS		Certification Practice Statement
CRL		Certificate Revocation List
ITS		Intelligent Transport System
ITS-S		ITS Station
EC	Long Term Certificate (LTC)	Enrolment Credential
EA	Long Term Certificate Authority (LTCA)	Enrolment Authority
MA		Misbehavior Authority
AT	Pseudonym Certificate	Authorization Ticket
AA	Pseudonym Certificate Authority (PCA)	Authorization Authority
PKI		Public Key Infrastructure
RCA		Root Certificate Authority
TPK		Technical Public Key
TSL		Trust-service Status List
UI		Unique Identifier

2 Operational concept

2.1 Public Key Infrastructure (PKI) basics

2.1.1 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

2.1.2 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

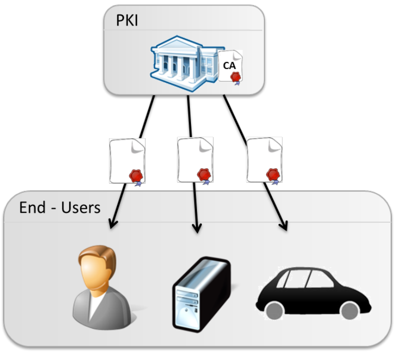

Figure 1: PKI end-users

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.

2.1.3 Public Key Infrastructure for ITS

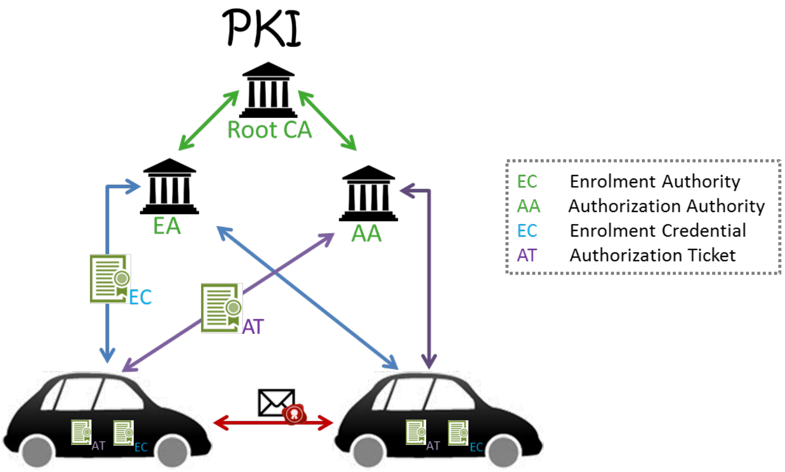

Figure 2: PKI for its

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 Enrolment Credentials or others such as Authorization Tickets (AT). 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.

2.2 Initial architecture

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

- Root certificate authority (RCA)
- Enrolment Authority (EA)
- Authorization Authority (AA)
- Distribution Center (DC)

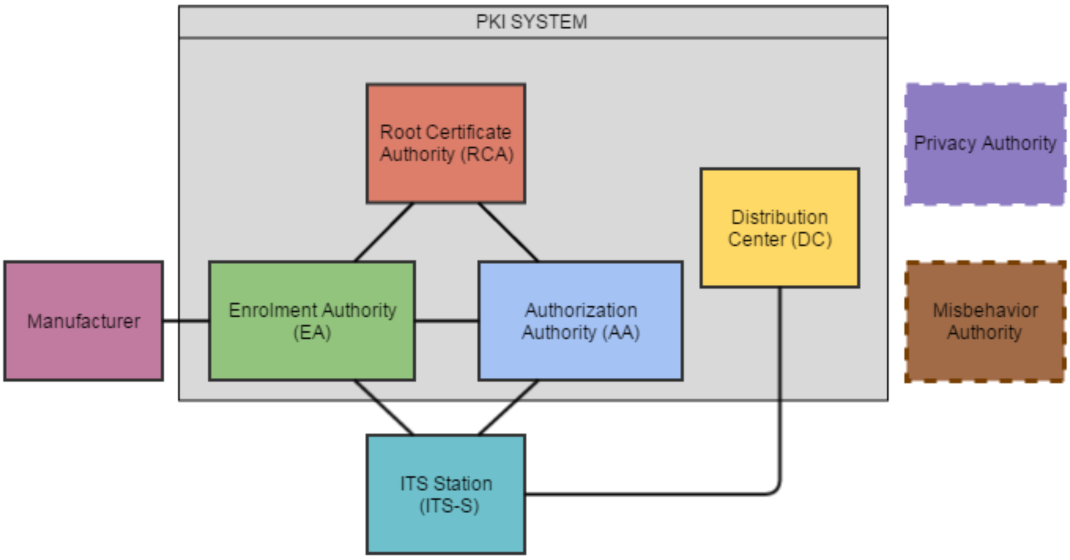

Figure 3: MODEL of pki system

2.3 PKI entities

Entities	Description
Root Certificate Authority (Root CA or RCA)	RCA is the root of trust for all certificates within the PKI hierarchy. Provides EA and AA with proof that it may issue enrolment credentials, respectively authorization tickets. It also defines and controls policies among all certificate issuers. The Root CA is required when a new EA or AA shall be created, or when the lifetime of an EA or AA certificate expires.
Enrolment Authority (EA)	Security management entity responsible for the life cycle management of enrolment credentials. Authenticates an ITS-S and grants it access to ITS communications
Authorization Authority (AA)	Security management entity responsible for issuing, monitoring the use of authorization tickets. AA provides an ITS-S with authoritative proof that it may use specific ITS services. AA 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.
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.

2.4 System 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…
Manufacturer	The "manufacturer" role is to install necessary information for security management in ITS-S at production. More precisely, the manufacturer bootstraps the process for manufacturing a trusted ITS-S in production site, i.e. generates and stores securely required crypto-material in its security module, initializes RCA and EA certificates and network addresses.
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.*

2.5 Functionalities

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

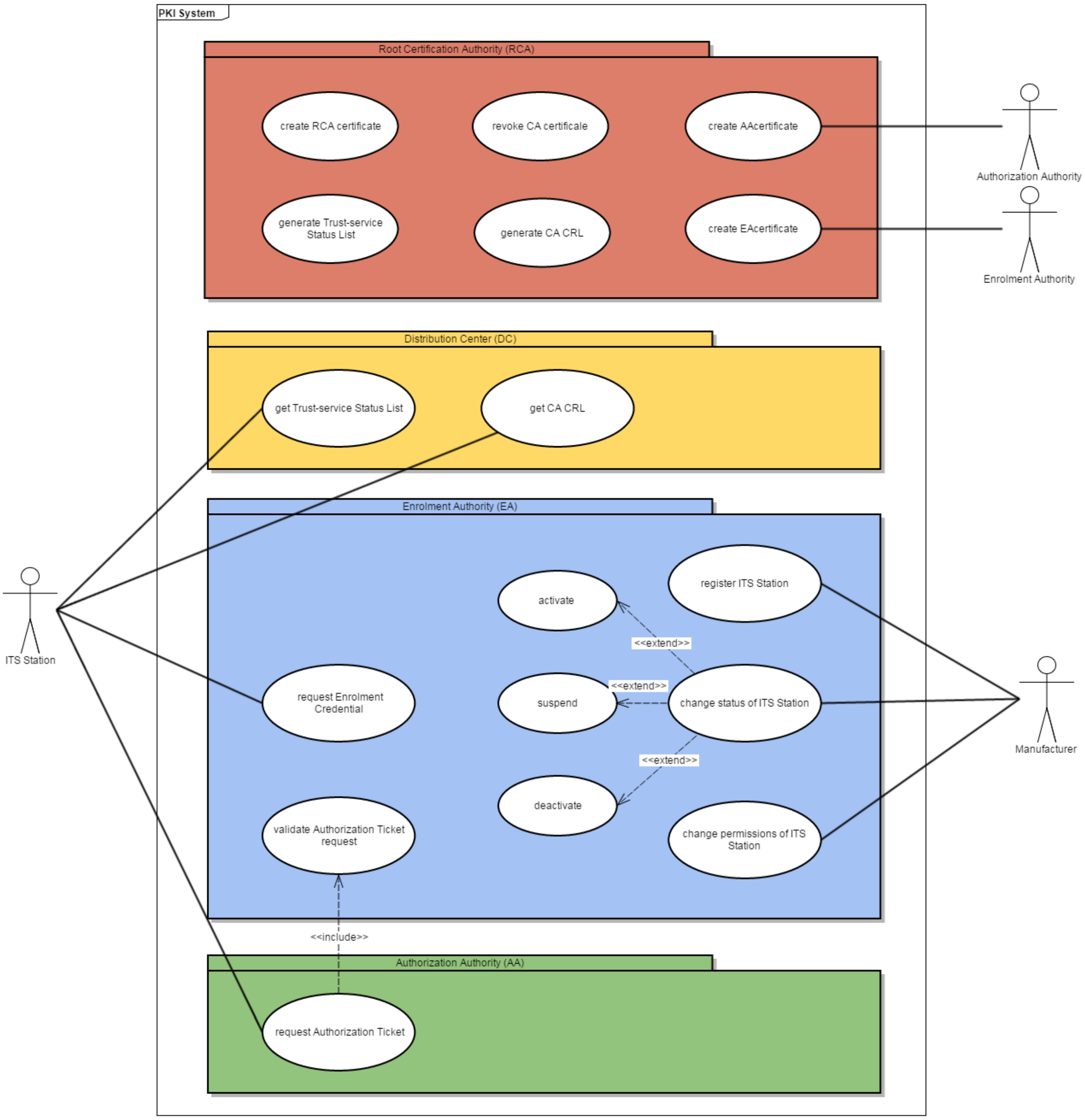

Figure 4: use cases diagram of pki system

2.5.1 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 (EA or AA) certificates;
- Revocation of CA (EA or AA) certificates;
- Generation of CA CRL;
- Generation of TSL.

2.5.2 Enrolment Authority component features

EA component implements production of EC.

The features of EA component are:

- Registration of ITS-S
- Management of ITS-S status
- Management of ITS-S permissions
- Issuance of Enrolment Credentials
- Validation of Authorization Ticket request

EA component is on-line component from the point of view of the manufacturer, ITS-S, and AA…

2.5.3 Authorization Authority Component features

AA component implements AT lifecycle management.

The features of AA component are:

- Issuance of Authorization Tickets

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

2.5.4 DC component features

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

The features of DC component are:

- Publication of TSL
- Publication of CA CRL

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

3 Use cases analysis

3.1 Use case 1: create RCA certificate

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

3.2 Use case 2: create EA certificate

3.2.1 Semi-Formal Description

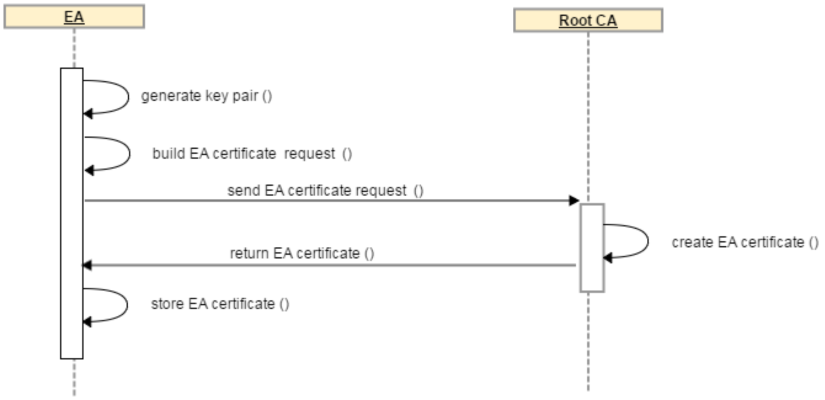

Figure 5: create EA certificate

3.2.2 Detailed Description

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

Primary Actor	Enrolment Authority
Description	EA requests to RCA an EA certificate.
Preconditions	-
Success End Condition	EA has a certificate issued by RCA.
Failed End Condition	-
Involved components	-

Main Success Scenario	1) EA generates key pair. 2) EA builds EA certificate request. 3) EA sends EA certificate request. 4) RCA creates EA certificate. 5) RCA returns EA certificate. 6) EA stores EA certificate.
Extensions	-
Variations (Alternatives)	-
Includes	-

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

3.3 Use case 3: create AA certificate

3.3.1 Semi-Formal Description

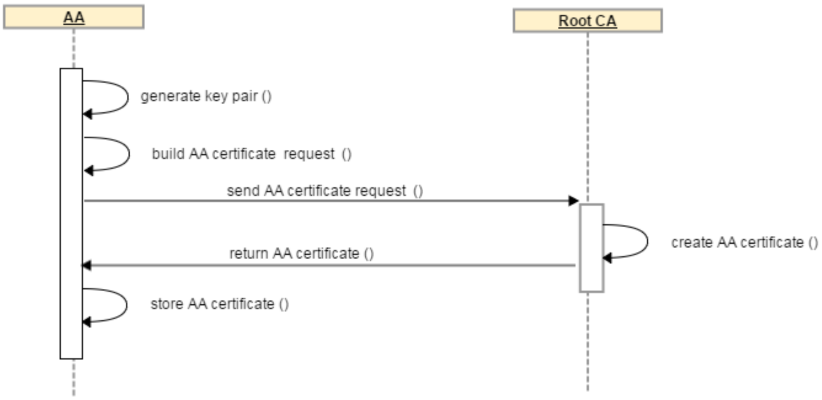

Figure 6: create AA certificate

3.3.2 Detailed Description

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

Requirement:	

Primary Actor	Authorization Authority
Description	AA requests to RCA a AA certificate.
Preconditions	-
Success End Condition	AA has a certificate issued by RCA.
Failed End Condition	-
Involved components	-
Main Success Scenario	1) AA generates key pair. 2) AA builds AA certificate request. 3) AA sends AA certificate request. 4) RCA creates AA certificate. 5) RCA returns AA certificate. 6) AA stores AA certificate.
Extensions	-
Variations (Alternatives)	-
Includes	-
Security Characteristics	

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

3.4 Use case 4: revoke CA certificate

The RCA component revokes CA certificate.

3.5 Use 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.

3.6 Use 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.

3.7 Use case 7: request Enrolment Certificate

3.7.1 Semi-formal description

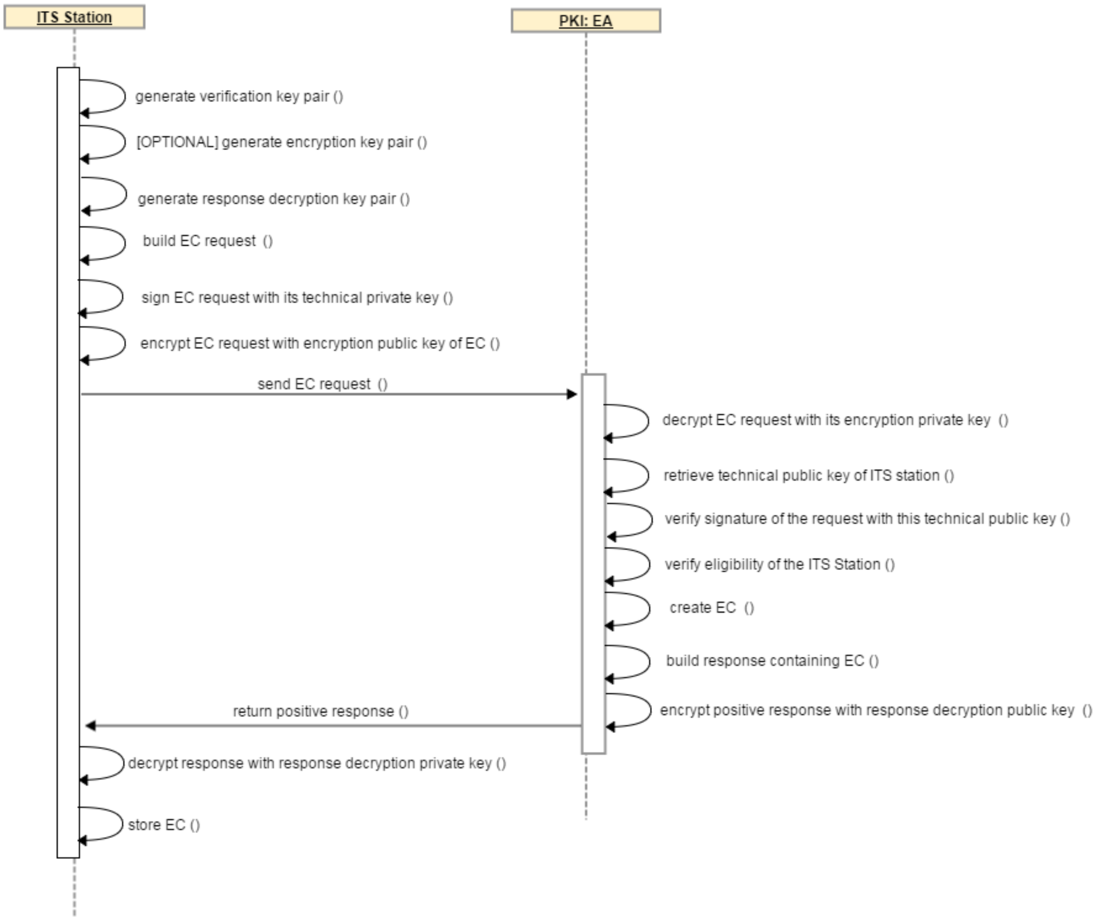
ITS Station
PKI: EA
generate verification key pair ()
[OPTIONAL] generate encryption key pair ()
generate response decryption key pair ()
build EC request ()
sign EC request with its technical private key ()
encrypt EC request with encryption public key of EC ()
send EC request ()
decrypt EC request with its encryption private key ()
retrieve technical public key of ITS station ()
verify signature of the request with this technical public key ()
verify eligibility of the ITS Station ()
create EC ()
build response containing EC ()
encrypt positive response with response decryption public key ()
return positive response ()
decrypt response with response decryption private key ()
store EC ()

Figure 7: request enrolment certificate

3.7.2 Detailed Description

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

Primary Actor	ITS Station
Description	ITS Station wants to request enrolment certificate
Preconditions	ITS Station has its technical key pair, a unique identifier, the address of the EA and EA certificate.

	ITS Station is registered in internal database of EA.
Success End Condition	ITS Station has new EC.
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 EC request. 4) ITS Station signs this request with its technical private key. 5) ITS Station encrypts this request with encryption public key of EA. 6) ITS Station sends this request to EA. 7) EA decrypts EC request with its encryption private key. 8) EA retrieves from its internal database the technical public key corresponding to the unique identifier of ITS Station. 9) EA verifies the signature of the request with this technical public key. 10) EA verifies the eligibility of ITS Station. 11) If ITS Station is eligible, EA creates the EC. 12) EA builds a positive response containing the created EC. 13) EA encrypts this positive response with response decryption public key to ITS Station. 14) EA returns this positive response to ITS Station. 15) ITS Station decrypts this positive response with response decryption private key. 16) ITS Station stores the EC.
Extensions	10) If ITS Station is not eligible, EA doesn't create the EC. 11) EA builds a negative response with a reason. 12) EA encrypts this negative response with the response decryption public key to ITS Station. 13) EA returns this negative response to ITS Station. 14) ITS Station decrypts this negative response with response decryption private key.
Variations (Alternatives)	ITS Station could also generate encryption key pair and request an EC containing two key usages.
Includes	

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

3.8 Use case 8: request Authorization Ticket

3.8.1 Semi-formal description

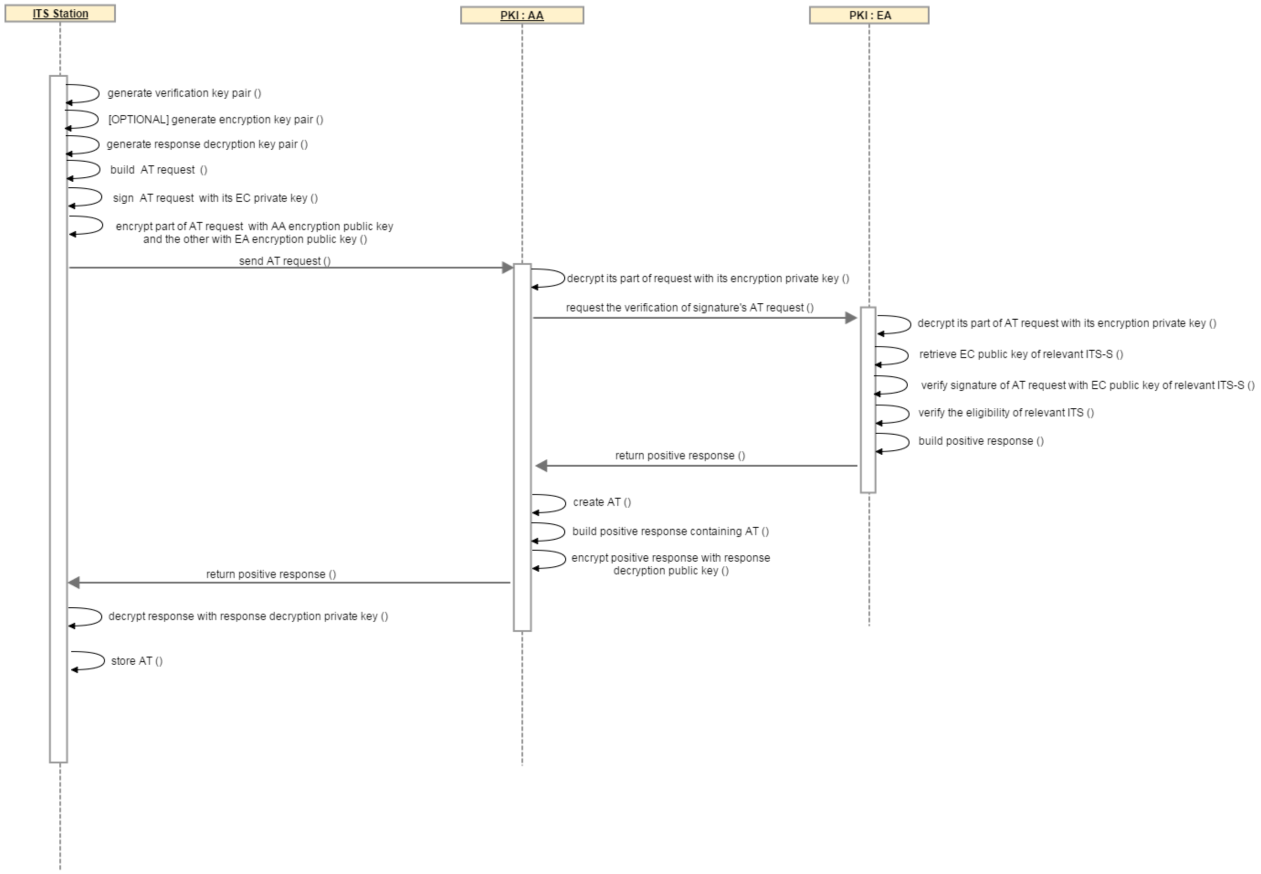
ITS Station
PKI : AA
PKI : EA
generate verification key pair ()
[OPTIONAL] generate encryption key pair ()
generate response decryption key pair ()
build AT request ()
sign AT request with its EC private key ()
encrypt part of AT request with AA encryption public key and the other with EA encryption public key ()
send AT request ()
decrypt its part of request with its encryption private key ()
request the verification of signature's AT request ()
decrypt its part of AT request with its encryption private key ()
retrieve EC public key of relevant ITS-S ()
verify signature of AT request with EC public key of relevant ITS-S ()
verify the eligibility of relevant ITS ()
build positive response ()
return positive response ()
create AT ()
build positive response containing AT ()
encrypt positive response with response decryption public key ()
return positive response ()
decrypt response with response decryption private key ()
store AT ()

Figure 8: request authorization ticket

3.8.2 Detailed description

Use Case ID:	***UC-ISE-08***
Use Case Name:	Request authorization ticket
Priority:	Mandatory
Related Requirement:	

Primary Actor	ITS Station
Description	ITS Station wants to request authorization ticket
Preconditions	ITS Station has an EC and its associated private key, a unique identifier, the address of AA, AA certificate and EA certificate (and its position?)

Success End Condition	ITS Station has new AT.
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 AT request. 4) ITS Station signs the AT request with its EC private key. 5) ITS Station encrypts part of request with AA encryption public key and the other part with EA encryption public key. 6) ITS Station sends this request to AA. 7) AA decrypts its part of the request with its encryption private key. 8) AA requests to EA to verify the signature of AT request. 9) EA decrypts its part of request with its encryption private key. 10) EA retrieves EC public key of relevant ITS Station. 11) EA verifies the signature of AT request with EC public key of relevant ITS-S. 12) EA verifies the eligibility of relevant ITS Station. 13) If the ITS Station is eligible, EA builds a positive response to AA. 14) EA returns positive response to AA. 15) AA creates a AT. 16) AA builds positive response containing the created AT. 17) AA encrypts this positive response with response decryption public key to ITS Station. 18) AA returns this positive response to ITS Station. 19) ITS Station decrypts this positive response with response decryption private key. 20) ITS Station stores AT.
Extensions	13) If ITS Station is not eligible, EA builds a negative response to AA. 14) EA returns this negative response to AA. 15) AA doesn't create a AT. 16) AA builds the negative response with a reason. 17) AA encrypts this negative response with response decryption public key to ITS Station. 18) AA 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 AT containing two key usages. 2) ITS-S generates multiple verification key pairs and sends a AT request to obtain multiple ATs from the AA.
Includes	**UC-ISE-07**

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

Integrity	**X**		
Traceability	**X**		

3.9 Use case 9: register ITS Station

3.9.1 Semi-formal description

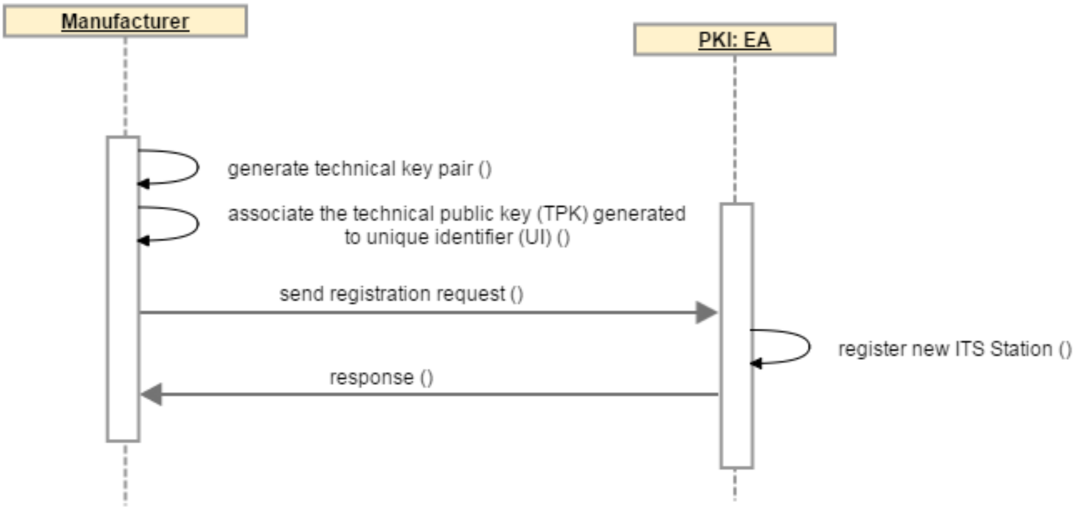
Manufacturer
PKI: EA
generate technical key pair ()
associate the technical public key (TPK) generated to unique identifier (UI) ()
send registration request ()
register new ITS Station ()
response ()

Figure 9: Register its station

3.9.2 Detailed description

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

Primary Actor	Manufacturer
Description	Manufacturer wants to register ITS Station
Preconditions	-
Success End Condition	ITS Station is registered in internal database of EA (status?)
Failed End Condition	-
Involved components	-
Main Success Scenario	1) Manufacturer generates the technical key pair.

	2) Manufacturer associates the technical public key (TPK) to the unique identifier of ITS Station. 3) Manufacturer sends registration request to EA. 4) Manufacturer verifies that technical public key or unique identifier is not already registered in its internal database. 5) EA registers new ITS Station. 6) EA returns positive response to manufacturer.
Extensions	5) If technical public key or unique identifier is already registered, EA doesn’t register ITS Station. 6) EA returns negative response with a reason.
Variations (Alternatives)	-
Includes	-

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

3.10Use case 10: change state of ITS Station

3.10.1Semi-formal description

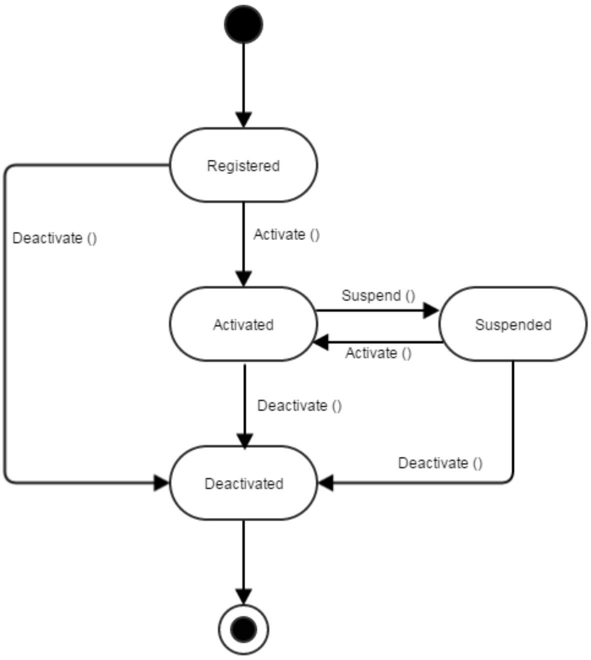

Figure 10: state diagram of its station

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 EA.
Activated	ITS-S is activated once registered with the EA to be allowed to obtain authorization tickets.
Suspended	ITS-S could be suspended for different reasons. This state doesn't allow ITS-S to request authorization tickets.
Deactivated	In case of end life or following a compromise, ITS-S is deactivated.

Figure 11 : description of its STATES

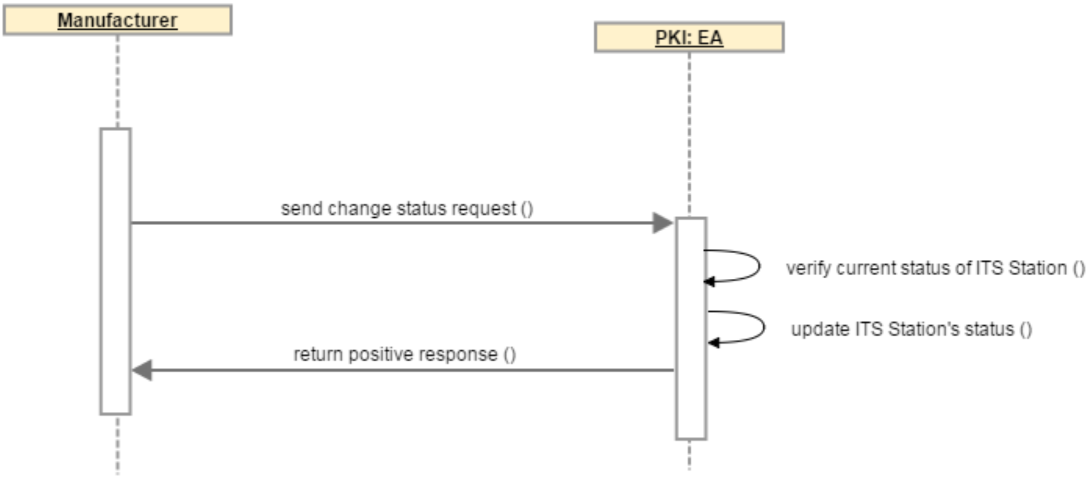
Manufacturer
PKI: EA
send change status request ()
verify current status of ITS Station ()
update ITS Station's status ()
return positive response ()

Figure 12 : change status of its station

3.10.1Detailed description

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

Primary Actor	Manufacturer
Description	Manufacturer wants to change status of ITS Station.

Preconditions	ITS Station is registered in internal database of EA. Manufacturer has the address of EA.
Success End Condition	ITS Station status is changed.
Failed End Condition	ITS Station status is unchanged.
Involved components	-
Main Success Scenario	1) Manufacturer builds request for changing status of ITS Station. 2) Manufacturer sends this request to EA. 3) EA verifies current status of ITS station. 4) EA updates ITS Station's status. 5) EA returns a positive response to manufacturer.
Extensions	4) If ITS Station status could not be changed, EA doesn't update ITS Status's status. 5) EA 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**		

3.11Use case 11: change permissions of ITS Station

3.11.1Semi-formal description

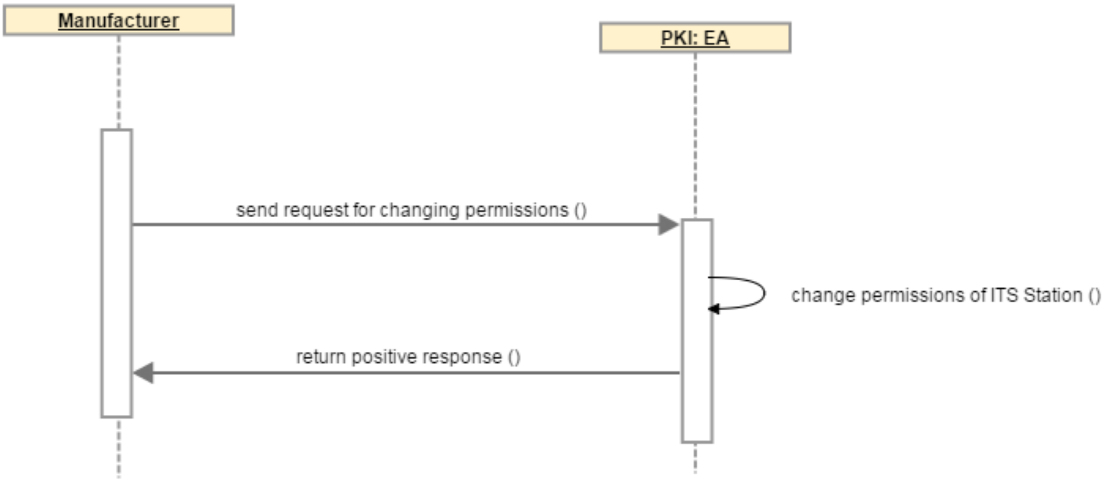
Manufacturer
PKI: EA
send request for changing permissions ()
change permissions of ITS Station ()
return positive response ()

Figure 13: change permissions of its station

3.11.2Detailed description

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

Primary Actor	Manufacturer
Description	Manufacturer 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) Manufacturer sends request to EA. 2) EA changes permissions of ITS Station. 3) EA returns positive response to manufacturer.
Extensions	-
Variations (Alternatives)	-
Includes	UC-ISE-09
Security Characteristics	

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

3.12 Use case 12: get Trust-service Status List

3.12.1 Semi-formal description

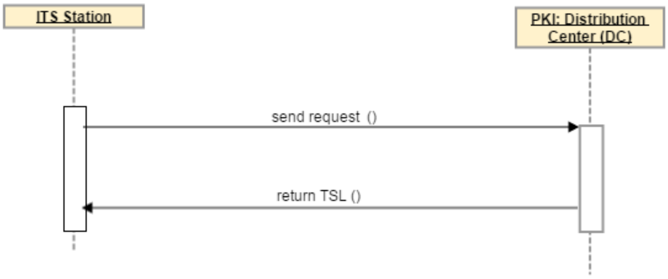

Figure 14: get trust-service status list

3.12.2 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, AA 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			

3.13Use case 13: get CA CRL

3.13.1Semi-formal description

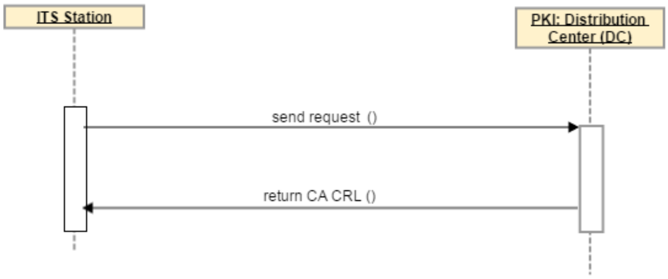

Figure 15: get ca crl

3.13.2Detailed 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			

4 System requirements

Relevance:

- **Critical – C:** Must be implemented
- **Significant – S:** Should
- **Of Interest – I:** May

Priority:

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

4.1 Functional requirements

Requirements IDs	**Description**	**Relevance**	**Priority**	**Linked Use Cases**
	Functional			
REQ-FUN-1	EA MUST be able to issue EC to ITS-S.	C	M	UC-ISE-07
REQ-FUN-2	AA MUST be able to issue AT to ITS-S.	C	M	UC-ISE-08
REQ-FUN-3	EA MUST be able to verify AT request.	C	M	UC-ISE-08

REQ-FUN-4	EA MUST be able to register ITS-S.	C	M	UC-ISE-09
REQ-FUN-5	EA MUST be able to suspend temporarily ITS-S.	C	M	UC-ISE-10
REQ-FUN-6	EA MUST be able to deactivate permanently ITS-S.	C	M	UC-ISE-10
REQ-FUN-7	EA 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 EA certificate.	C	M	UC-ISE-02
REQ-FUN-12	RCA MUST be able to create AA 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

4.2 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 EA, AA 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	EA SHOULD verify unicity of ITS-S canonical public key.	S	O	UC-ISE-09
REQ-SEC-6	EA 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	

4.3 Privacy requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
	Privacy			
REQ-PRI-1	AA MUST NOT be able to identify the ITS-S transmitting the AT request.	C	M	UC-ISE-08
REQ-PRI-2	EA MUST NOT be able to read content of AT request.	C	M	UC-ISE-08
REQ-PRI-3	AA MUST NOT be able to link a AT with ITS-S.	C	M	UC-ISE-08
REQ-PRI-4	AA MUST NOT be able to link ATs as belonging to a same ITS-S.	C	M	UC-ISE-08
REQ-PRI-5	EA MUST NOT be able to link a AT with ITS-S.	C	M	UC-ISE-08
REQ-PRI-6	EA MUST NOT link ATs as belonging to a same ITS-S.	C	M	UC-ISE-08

4.4 Performance and scalability requirements

Requirements IDs	Description	Relevance	Priority	Linked Use Cases
	Performance & Scalability			
REQ-PER-1	AA MUST provide AT 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	AA and EA MUST accept more than X simultaneous connections.	S	M	UC-ISE-08
REQ-PER-3	AA and EA 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 to a safer one).	C	M	all

4.5 Norms and standards requirements

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

4.6 Others 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

5 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.

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

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

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