Milestone 5 - Common set of upgraded specifications for PKI and Common Certificate Policy (CP)

Version number:	1.0
Main author:	Houda LABIOD
Dissemination level:	PU
Lead contractor:	Télécom ParisTech/IMT
Due date:	31/08/2018
Delivery date:	25/09/2018
Delivery date updated document:	

Co-financed by the European Union
Connecting Europe Facility

Grant Agreement No: INEA/CEF/TRAN/M2015/1143833
Action No: 2015-EU-TM-0159-S

CONTROL SHEET

Version history			
Version	**Date**	**Main author**	**Summary of changes**
1.0	20/07/2018	Houda Labiod (IMT)	Final version for peer review
1.0	27/07/2018	Houda Labiod (IMT)	Integration of reviews made by Alan Stevens (DfT), M.C. Esposito (MTES)
1.0	07/08/2018	Houda Labiod (IMT)	Integration of changes by Darren Handley (DfT), Peter Lewyllie (FDMPW), Peter-Paul Schackmann (TNO / NMIE-R)
1.0	11/09/2018	Houda Labiod (IMT)	Last changes by Gilles Ampt (DITCM / NMIE-R), Axel Zandbergen (NMIE-R)
1.0	24/09/2018	Iuliia Skorykova, Giacomo Somma (ERTICO)	Final quality check

	Name	**Date**
Prepared	Houda Labiod (IMT)	20/07/2018
Reviewed	Core Management Team, Advisory Committee, and General Assembly	27/07-11/09/2018
Authorised	Ronald Adams (NMIE-R)	25/09/2018

Circulation	
Recipient	**Date of submission**
INEA	25/09/2018

InterCor consortium	25/09/2018

Authors (full list): Houda Labiod (IMT), Mounira Msahli (IDnomic), Ihsen Boughaba, Remi Blancher, Gilles Ampt (DITCM / NMIE-R), Tim Bracke, Jurgen Latte (FDMPW), Jeroen Avau (FDMPW), Darren Handley, Walter Huberts (RDW / NMIE-R), Hans Dewulf (Dynniq / FDMPW).

Project Coordinator

Ronald Adams

Rijkswaterstaat

Office address: Toekanweg 7, 2035 LC, Haarlem (NL)

Postal address: Postbus 2232, 3500 GE, Utrecht (NL)

Mobile:+31 6 518 480 77

Email: ronald.adams@rws.nl

Legal Disclaimer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TERMS AND ABBREVIATIONS

Term / Abbreviation	Definition
AA	Authorization Authority
AT	Authorization Ticket
BSI	Bundesamt für Sicherheit in der Informationstechnik
C2C-CC	Car to Car Communication Consortium
CA	Certificate Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport System
CP	Certificate Policy
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
DC	Distribution Centre
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	Enrolment Credential
ETSI	European Telecommunications Standard Institute
HMI	Human Machine Interface
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
I2V	Infrastructure to Vehicle
ITS	Intelligent Transport System
ITS-AID	ITS Application Identifier
ITSS	ITS Station
LTC	Long Term Certificate
LTCA	Long-term CA
PA	Policy Authority
PC	Pseudonym Certificate
PCA	Pseudonym CA

PKI	Public Key Infrastructure
RCA	Root Certificate Authority
RSU	Roadside Unit
SPaT	Signal phase and timing
SSP	Specific service permissions
TR	Technical Report
TS	Technical Specification
TLM	Trust List Manager
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
WG	Working group

1. Executive summary

PKI refers to public key infrastructure that enables trust between entities exchanging information while they do not know each other. PKI has proven to be very scalable and reliable for large distributed systems in many industries and around the globe. For ITS services between vehicles (based on V2V communications) and between roadside infrastructure and vehicles (based on I2V and V2I communications), the PKI allows the ITS stations to trust each other if there are no alternative trust options available.

Within the InterCor sub-activity 2.1c, a global PKI system has been developed that supports interoperability between local PKI systems that exist or are under development in the four Member States (Belgium, France, Netherlands and the United Kingdom) participating in the InterCor project.

The main objective of this document is to provide the technical specifications of the public key infrastructures (PKIs) to be developed in the different participating countries. Securing the messages of the different defined C-ITS services will be based on using security materials and credentials related to the PKI specifications. To achieve interoperability between the C-ITS systems developed in the different pilot sites, common PKI specifications are based on stable ETSI security standards agreed by the four InterCor Member States. Following the recommendations of the C-ITS Platform (trust model 2c and certificate policy), the best way to ensure interoperability between the Member State PKIs is that the Root Certificate Authorities (RCAs) use the same certificate policy (CP) and the same security technology (e.g. cryptographic algorithms, certificate formats), which are defined by a single organization. The common set of specifications will aim at putting this trust model into practice over the four countries. A common certificate policy is defined to achieve trust and sufficient interoperability between RCAs by providing a set of minimum organizational and technical requirements.

This document describes the technical specifications to set up the common trust model for the InterCor Project. It defines the proposed trust model and highlights the interoperability requirements in terms of architecture and technical specifications. This document provides the required specifications for PKI / security TESTFEST scenarios illustrating the interactions between ITS Stations belonging to different trust domains.

2. Introduction

Security is a key challenge in implementation of ITS applications knowing the fact that there is a plethora of attacks today that can negatively impact their reliability. To address this challenge, key security requirements shall be defined in order to find secure solutions to combat the above-mentioned attacks.

For securing C-ITS communications, the common understanding is to use asymmetric cryptography and this requires to set up a Public Key Infrastructure (PKI) for the management of security credentials of each ITS Station (ITSS). A key issue is to provide interoperability of secured communications for the various types of vehicular communications: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (I2V) and Vehicle-to-PKI when the ITSS needs to connect to the PKI entities also named Certificate Authorities (CAs) for security management purpose. Another major issue to take into account is the user privacy. Any security credential management system must consider a privacy preserving scheme to protect vehicles' and users' identity according to national and international legislation.

In order to achieve C-ITS interoperability, the development of ITS communications security standards is paramount. For this purpose, dedicated working groups (WG) within standardization organizations address security and privacy issues such as ETSI TC ITS WG5 working group in Europe, Security WG of European C-ITS platform and IEEE 1609.2 working group in U.S.A.

Based on these standards, several PKIs models were designed and implemented in the context of several C-ITS deployment projects in Europe and the U.S.A.

Within the InterCor sub-activity 2.1c, we made an extensive state of the art overview of the Public Key Infrastructure (PKI) architectures proposed for C-ITS pruposes by ETSI, IEEE 1609.2, C2C Communication Consortium and US Security Credential Management System. We also made an exhaustive and in-depth gap analysis comparing the main advanced PKI specifications of C-ITS, described in the C-ITS Platform, SCOOP@F project, and the IEEE1609.2. Based on this investigation, we recommended using the common trust model defined by the C-ITS Platform for the InterCor PKI. The C-ITS Platform trust model presented in C-ITS certificate policy is essentially in total synergy and in line with stable ETSI security standards.

All details related to this study are provided in the following documents:

- InterCor_A2.1.c_001, Reference documentation List [1]
- InterCor_A2.1.c_002, PKIs Trust models [2]

- InterCor_A2.1.c_003, Gap Analysis [3]

One main achievement of the sub-activity 2.1c is the provisioning of a common set of upgraded specifications for InterCor PKI and the associated common Certificate Policy (CP). The adopted common trust model is detailed through the different involved entities and involved communication mechanisms. A common certificate policy (CP) is also defined based on the adopted trust model. The harmonized trust-based system is able to support hybrid communications between the ITS stations and the PKI and enables interoperability.

2.1. Purpose of this document

The purpose of this document is to provide technical specifications of the global PKI system to ensure security and trust for InterCor use cases. It includes four main chapters. In chapter 3 the InterCor PKI architecture with the common trust model is described. In chapter 4 the technical implementation details are presented; these are also used for the PKI / security TESTFEST (InterCor sub-activity 2.2) and/or pilots (InterCor activity 3). Communication protocols between the ITS stations and the PKI servers are highlighted in Chapter 5. In Chapter 6, the InterCor CP is presented. Concluding remarks and future works are given in the last chapter.

2.2. InterCor Contractual References

InterCor (Interoperable Corridors) links the C-ITS corridor initiatives of the Dutch C-ITS Corridor Netherlands-Germany-Austria and the French one defined in SCOOP@F, and extending to the United Kingdom and Belgium C-ITS initiatives.

InterCor is an action co-financed by the European Union under the Grant Agreement number INEA/CEF/TRAN/M2015/1143833. The Project duration is 36 months, effective from the 1st of September 2016 until the 31st of August 2019. It is a contract with the Innovation and Networks Executive Agency (INEA), under the powers delegated by the European Commission.

Communication details of the Agency:

Any communication addressed to the Agency by post or e-mail shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)

Department C – Connecting Europe Facility (CEF)

Unit C3 Transport

B - 1049 Brussels

Fax: +32 (0)2 297 37 27

E-mail addresses: General communication: inea@ec.europa.eu

For submission of requests for payment, reports (except ASRs) and financial statements: INEA-C3@ec.europa.eu

Any communication addressed to the Agency by registered mail, courier service or hand-delivery shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)

Avenue du Bourget, 1

B-1140 Brussels (Evere)

Belgium

TEN-Tec shall be accessed via the following URL:

https://webgate.ec.europa.eu/tentec/

All communication with the INEA or the European Commission shall be done via the Project Coordinator, Mr Ronald Adams

3. InterCor PKI architecture and technical specifications

The InterCor PKI specifications aim at providing trust and security interoperability between different participating countries. In other words, a vehicle from country 1 that is driving in country 2 should be able to exchange secured and trusted messages.

This chapter gives an overview of the PKI architecture to be implemented in the context of the InterCor project. It provides technical specifications in terms of supported protocols as well as the components' roles and information flows.

As a first step, this document defines all entities participating in the trusted C-ITS system in InterCor. To allow assessment of trust in certificates, a detailed description of the central entity which is in charge of InterCor_CTL is provided. Moreover, this InterCor_CTL profile and its management are specified. Secondly, a set of interoperability requirements for the operation of the four European PKIs (France, Netherlands, Belgium/Flanders and United Kingdom) is delineated. This will serve as a baseline for harmonization of the different PKI systems. Then, the last parts are devoted to the specifications of each PKI partner.

Consequently, the following aspects related to the InterCor PKI are detailed:

- The identification and authentication of the principal roles and entities in InterCor PKI.
- The trust relationships between all entities of the InterCor trust model.
- All details about InterCor PKI interfaces and information flows.
- The minimum requirements for the entity in charge of InterCor_CTL and some operational practices including: the addition of new root CA certificates, the temporary or permanent exclusion of existing included root CAs, the publication and the distribution of the InterCor_CTL updates.
- The main interoperability requirements.
- A detailed description of each PKI specifications per partner.

3.1. High-Level Architecture of InterCor PKI

Based on C-ITS platform certificate policy release 1 [4], InterCor partners should implement an adapted simplified but fully compliant trust model. The main security standards to be used are ETSI 103097 version 1.2.1 [5] and ETSI TS 102941 v1.1.1 [6]. For Trust List/CRL formats, the one defined in SCOOP@F project are used.

The InterCor PKI trust architecture differs from the one defined by the C-ITS platform in the sense that it does not support the following entities: Policy Authority, TLM and CPOC.

The InterCor PKI core system consists of five main entities as shown in Figure 1:

- InterCor_CTL repository
- RCA_FR: RCA for France
- RCA_NL: RCA for Netherlands
- RCA_UK: RCA for the United Kingdom
- RCA_BE: RCA for Belgium / Flanders.

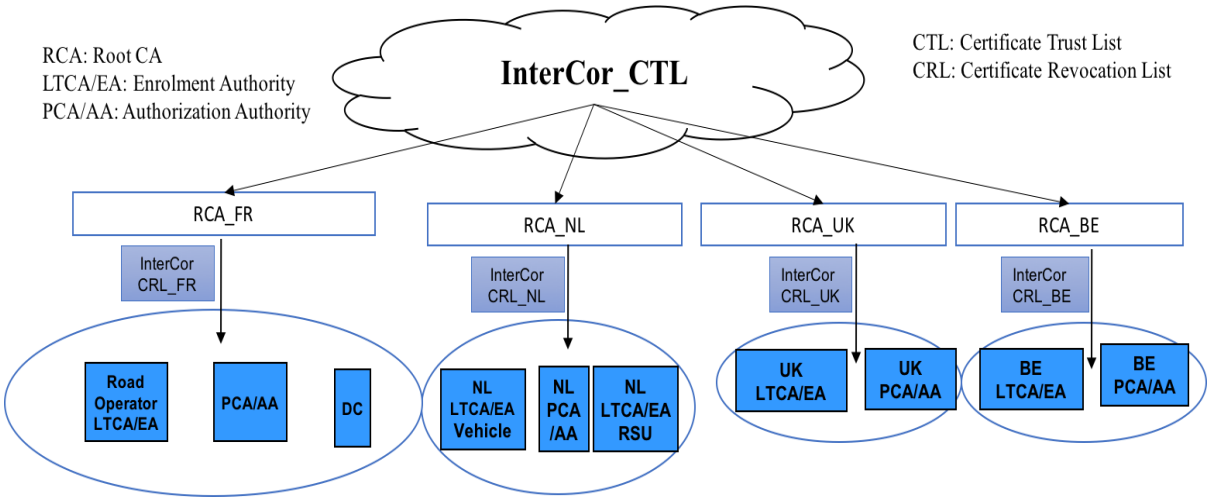

Figure 1: InterCor PKI Model

InterCor_CTL (InterCor Certificate Trust List): containing the RCAs' certificates to be trusted between InterCor partners. It is issued and signed by a trusted entity.

InterCor_CRL_X (InterCor_Certificate Revocation List): For each Member State X (X=NL, FR, UK, BE), only its RCA is responsible for the issuance and the signature of its CRL. This CRL contains the revoked certificates of its sub_CAs. We decide to use a common InterCor_CRL in addition to a common InterCor_CTL. One common InterCor-CRL is generated based on the contents of the four MS CRLs. We also choose the option that the central ownership/management of the InterCor_CTL and InterCor_CRL is under the responsibility of one partner which is the French Ministry of Transport. France thus generates both common InterCor_CTL and common InterCor_CRL data structures and defines the procedure to validate all the required management procedures related to these data structures. More details are given in Chapter 4.

3.1.1. Description of roles

The InterCor PKI model is based on the trust model defined by the C-ITS platform [1]. The roles of the different involved entities are the following:

- **InterCor Certificate Trust List (InterCor_CTL) Repository**

  A French Authority manages the InterCor_CTL Repository.

  This Authority is responsible for:

  - ✓ The operation of the InterCor_CTL according to the common InterCor specifications and the valid CP and regular activity reporting to the policy authority for the overall secure operation of C-ITS trust model.
  - ✓ The reception of RCAs certificates.
  - ✓ The inclusion/exclusion of partners RCAs certificates in/from InterCor_CTL.
  - ✓ The signature of InterCor_CTL.
  - ✓ The publication of the common trust anchor (public key certificate of the InterCor_CTL).
  - ✓ The publication of the InterCor_CTL.

  InterCor_CTL certificate lifecycle management, including distribution of InterCor_CTL certificates, activation, expiration and revocation. The common InterCor_CRL is also managed by this Authority and is stored in the InterCor_CTL Repository.

- **RCAs**

  In each InterCor Member State PKI, the Root Certificate Authority (RCA) is the root of trust for all certificates within the PKI hierarchy. It operates in an offline mode and is responsible for the management of EAs/LTCAs and AAs/PCAs (creation, security requirements authorizing the issuance of certificates to ITSSs). The description of the role of the EAs/LTCAs and AAs/PCAs is given in Chapter 4.

3.1.2. InterCor PKI model: Interfaces and Information flows

This section details the various interactions within this PKI model. Based on the various types of interactions between the ITS stations and the PKIs, the interoperability aspects can be illustrated through a number of levels presented in Figure 2 and described as following.

1. **Interface a: Interaction between ITS stations and within their home PKI**

   This concerns ITS stations in their native system. At this level, the different exchanges between ITS stations and their home PKI are accomplished. These operations cover:

   - Certificates (EC, AT) requests and responses,

- CRL and CTL download,
- Messages signature and verification.

2. Interface b: Interaction between an ITS station and another foreign ITS station

At this level, the exchange between ITS stations belonging to different systems is performed. Assuming the process of certificates acquisition has been carried out, the considered functions are the following:

- Messages signature,
- Messages verification by foreign ITS stations.

3. Interfaces c and c+: Interoperability between PKIs at RCAs' level

The trust established between the different RCAs is considered at this level. The trusted RCAs' certificates are listed in the InterCor_CTL. Furthermore, the CAs' certificates (AAs' certificates, EAs' certificates) have to be exchanged as well as the correspondent CRLs. This interface is necessary to make validation of foreign trust chain.

4. Interface d: Interaction between InterCor_CTL and RCAs

This interface is out of scope of InterCor Project.

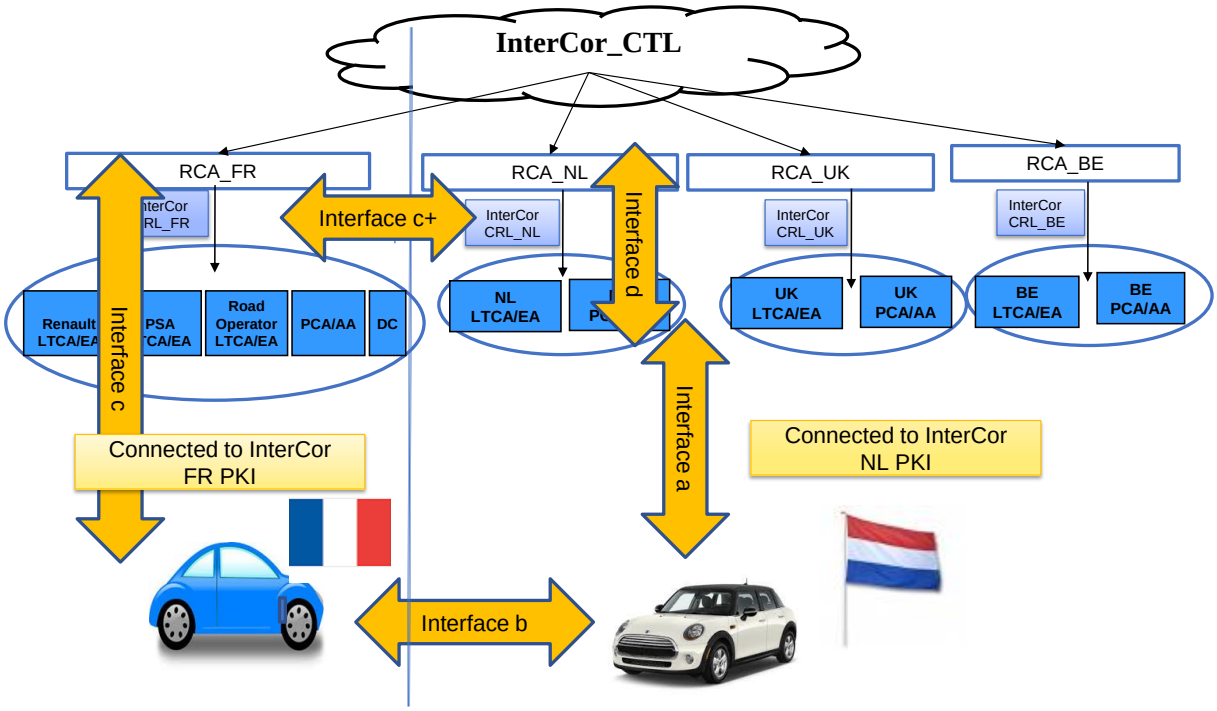

Figure 2: InterCor Trust model – interfaces and information flows

3.2. Interoperability Requirements

The main interoperability subjects are related to cross trust management at the overall system as well as to distribution of the common InterCor_CTL and the common InterCor_CRL.

In order to assure interoperability in the secured exchanges between different ITS stations, some requirements must be satisfied:

- to establish a trust relationship between Member States PKIs at RCAs' level in order to create a global trust domain.
- to provide all the necessary elements such as: InterCor_CTL, InterCor_CRL, trusted CAs' certificates for an ITS station to authenticate exchanged C-ITS messages while it is abroad.
- to define a common mechanism for C-ITS messages signature verification (including the verification of the trust chain).

3.2.1. InterCor Cross-Trust Management: InterCor Certificate Trust List (InterCor_CTL)

In the InterCor model, the Cross-Trust is managed via the distribution of a common InterCor_CTL. The InterCor_CTL is a signed list, which is created, signed and issued by InterCor_CTL Authority and contains the RCAs of the InterCor Trust Model (French, Belgium, United Kingdom and Dutch) to guarantee trust relations.

The format of the InterCor_CTL is defined in ETSI TS 102941 [6]. The InterCor_CTL Profile defines all mandatory and optional data fields contained in the InterCor_CTL, used cryptographic algorithms, as well as the exact InterCor_CTL format and recommendations for processing of the InterCor_CTL. The InterCor_CTL shall be time stamped. The C-ITS stations shall be able to interpret and to process the InterCor_CTL according to [3].

3.2.2. Publication and distribution of the common InterCor_CTL

The different PKI domains are linked based on InterCor_CTL. The InterCor_CTL contains the trusted CAs' certificates in the PKI domain as well as the trusted foreign RCAs' certificates. This list is issued and signed by InterCor_CTL Authority. It aims to provide trust information to all PKIs participants. Thus, it contains all the certificates of trusted RCAs and their access points (URLs), Contact information of the source InterCor_CTL Authority.

3.2.3. Publication of the common InterCor_CRL

The common InterCor_CRL contains the hashedID8 of the revoked CAs' certificates in the InterCor PKI domain. This list is signed by the InterCor_CTL Authority.

3.2.4. Security verification of exchanged data messages

The main objective of the tests that will be performed is to demonstrate the trust interoperability through the verification of data messages authentication and trust chain validation. For this purpose, we select the security standards [5,6] required for signing the sent data messages and for verifying the signature of received data messages as well as the validity of the trust chain.

3.3. French PKI

The French PKI is described in Figure 3. Technical specifications are mainly based on the SCOOP@F project (all details are provided in [7]).

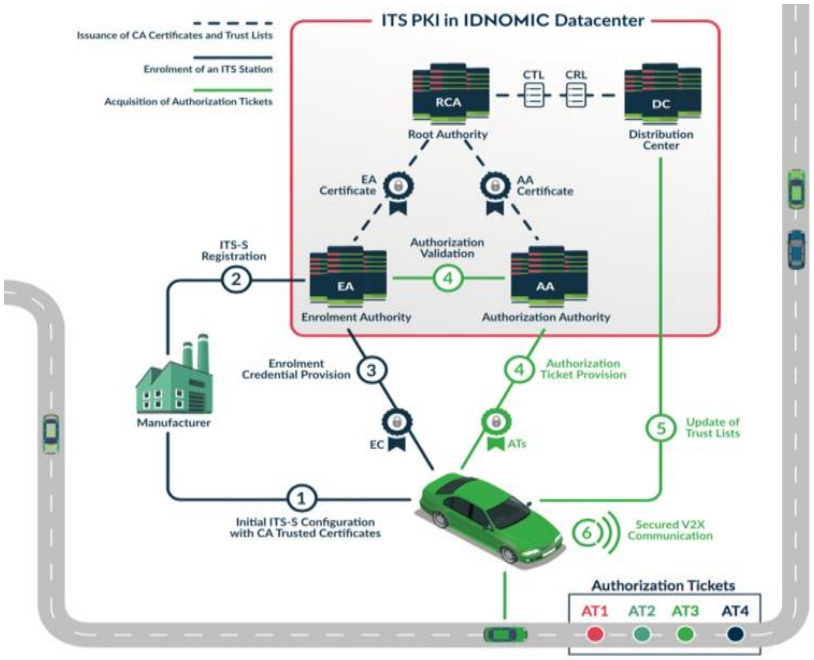

Figure 3: French PKI

3.4. Dutch PKI

The Dutch High level architecture PKI is described in Figure 4. Technical specifications follow the ETSI security standards adopted in InterCor.

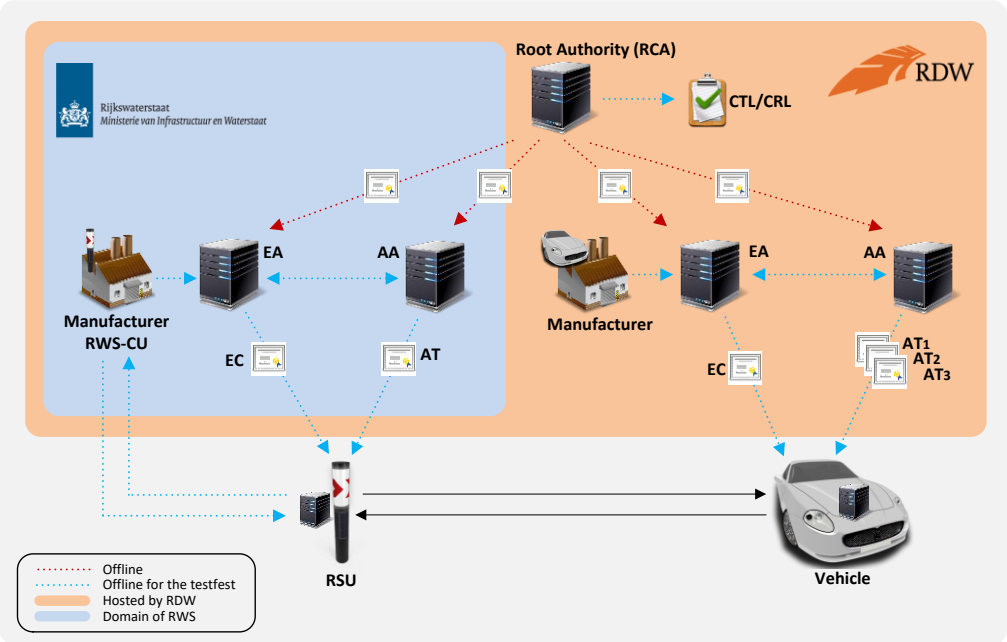

Figure 4: Dutch PKI architecture

Further technical reference documentation may be obtained from Dutch partners.

3.5. Belgian PKI

Further technical reference documentation may be obtained from Belgian partners.

3.6. British PKI

Further technical reference documentation may be obtained from UK partners.

3.7. Revocation and cryptoagility requirements for ITS stations

In the document InterCor_A2.1.c_004 [8], security requirements for C-ITS are reviewed. The scope of these requirements covers the revocation of trust of ITS stations and the ability to update or change of cryptographic algorithms, also called crypto-agility. The requirements set out in this document will only be applicable to C-ITS having the ability to revoke trust of

specific units or have crypto-agility. As these functions may not be present in the systems used in InterCor, then this document can be viewed as one for future systems and projects.

For revocation the document scope is to cover why revocation is needed, what requirements may be needed and how one could test whether the requirements have been achieved. The document also describes why revocation of ITS stations is difficult and therefore why it may not be implemented within InterCor.

For crypto-agility the scope is similar. The document briefly describes the need for crypto-agility, requirements for it within a C-ITS, and how those requirements might be tested.

3.8. PKI testing options

Within the InterCor project there is a requirement to test the PKI used. In the document InterCor_A2.1.c_005 [9], we set out a number of different tests that could be included in PKI/security TESTFEST, the rationale behind why the tests might be conducted, and their expected outcomes. This document describes a number of scenarios that could be tested, either by individual partners or by all partners, and what measures could be used to test these scenarios. The output from the PKI tests is expected to be a report detailing how it functions with respect to the pre-defined conditions chosen for both the system specification and the test conditions. Final PKI/security test scenarios are defined within the activity 2.2 to be considered during the InterCor TESTFESTs.

4. PKI System/Integration Guide

This chapter aims at giving all necessary implementation details about the PKI system for Member States. It presents the PKI system and describes the interactions on the basis of use cases. The chapter is composed of seven sections. The first section overviews the InterCor PKI system associated with use cases application. The second and third sections present CTL and CRL generation. Interoperability related operations. The certificate formats of CAs and InterCor_CTL Authority are also included.

4.1. InterCor PKI System Overview

4.1.1. InterCor Trust Model

The InterCor PKI model is composed of three main entities in each Member State PKI, as shown in Figure 1:

- **Root Certificate Authority (RCA):** is the root of trust for all certificates within the PKI hierarchy. It operates in an offline mode and is responsible for the management of EAs/LTCAs and AAs/PCAs (creation, security requirements authorizing the issuance of certificates to ITSSs).
- **Enrollment Authority(EA)/Long Term Certificate Authority (LTCA):** is a security management entity responsible for the issuance of EC/LTC and the validation of ATs/PCs as well as the management of the ITSSs (registration, status update, permissions…). It operates in an online mode.
- **Authorization Authority(AA)/Pseudonym Certificate Authority (PCA):** is a security management entity responsible for the delivery, the monitoring and the use of ATs/PCs. It operates in an online mode.

In order to assure the privacy and the security of communications between ITS Stations or ITSSs (vehicles, roadside units), the PKI is used to maintain trust between ITS Stations on one side and between ITS Stations and authorities on the other side.

Each InterCor Member StatePKI system manages the following elements:

- **EC/Long Term Certificate (LTC):** gives its holder (ITSSs) the right to request ATs/PCs.
- **AT/Pseudonym Certificate (PC):** gives its holder (ITSSs) the right to perform specific actions.
- **Certificate Revocation List (InterCor_CRL):** is a list digitally signed by a RCA that contains certificates identities that are no longer valid.

Common Trusted Service List (InterCor_CTL): It is a signed list which contains trusted RCAs, EAs/LTCAs and AAs/PCAs certificates and PKI service access points. This list is published and updated frequently. This list is stored in the InterCor repository managed by the French Transport Ministry.

Common InterCor_CRL: It is a signed list which contains the hashedID8 of the revoked CAs' certificates in the InterCor PKI domain. This list is stored in the InterCor Repository managed by the French Transport Ministry.

4.1.2. Certificates formats

The certificates formats for CAs, ATs and ECs used for the InterCor project are defined in ETSI TS 103 097 v1.2.1.

Each ITSS certificate is composed of several main fields: Version, Signer_Info, Subject_attributes, Validity_restrictions and Signature (64 bytes).

The assurance level field shall contain the assurance level of the sender or certificate authority. A certificate shall contain an assurance level that is equal to or lower than the assurance level of the certificate referenced by the Signer_info. If the assurance level is unknown for the certificate, then the default assurance level 0 shall be used. (cf 103 097 v1.2.1). In InterCor Project, we set the values of both assurance level and confidence level in ITSS-certificates to 0.

The formats of InterCor_CTL and InterCor_CRLs are defined in SCOOP@F Project (see deliverable 2.4.4.6). The CAs certificates duration is set to 5 years for the different EAs/LTCAs and the AAs/PCAs and to 8 years for the RCA. The EC/LTC duration is set to 3 years for all partners. The InterCor_CTL Authority certificate duration is set to 4 years for all partners.

4.1.3. Cryptographic operations

Cryptographic algorithms are used in InterCor PKI system. There are different types of algorithms defined in ETSI Standard TS 103 097 v1.2.1, some used for signing, others for encryption.

Here are the algorithms defined:

- ECDSA_nistP256_with_SHA256
- ECIES_nistP256_with_AES128_CCM

4.1.4. InterCor ITS Application ID (ITS-AID)

The ITS-AID format used in InterCor project is of type *IntX* (as described in ETSI TS 103 097 v1.2.1).

The ITS-AIDs chosen for the InterCor project are:

ITS-AID	Values
CAM	36
DENM	37
SPaT	137
MAP	138
IVI	139

The ITS-AIDs information can be found at the following URL:

http:/standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers.

4.1.5. Specific Service Permissions (SSPs)

The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions within the overall permissions indicated by the ITS-AID. For example, there may be an SSP value associated with the ITS-AID for CAM that indicates that the sender is entitled to send CAMs for a specific vehicle role.

SSPs are used in certificates, in certificate requests (get EC/LTC and get AT/PC) and during initialization phase.

SSPs for CAM message are defined using 3 bytes (as presented in ETSI EN 302 637-2 v1.3.2 section 6.2.2.2).

SSPs for DENM message are defined using 4 bytes (as presented in ETSI EN 302 637-3 v1.2.2, section 6.2.2.2).

The SSP format used in InterCor project is of type *opaque* (as described in ETSI TS 103 097 v1.2.1).

In the following section we give the SSPs adopted in InterCor project:

- the SSPs for CAM (see table 1),
- the SSPs for DENM (see table 2),
- the SSPs for SPaT (to add).
- Etc.

4.1.5.1. CAM SSPs

Table 1: CAM SSPs

CauseCodeType /Container	Bit Value				
		Road Operators			
			ITSS-Vg (Operator mode)	ITSS-Vu (User mode)	
CenDsrcTollingZone/ ProtectedCommunicationZonesRSU			0	0	
publicTransport / PublicTransportContainer			0	0	
specialTransport / SpecialTransportContainer			0	0	
dangerousGoods / DangerousGoodsContainer			0	0	
roadwork / RoadWorksContainerBasic			0	0	
rescue / RescueContainer			0	0	
emergency / EmergencyContainer			0	0	
safetyCar / SafetyCarContainer			0	0	
closedLanes / RoadworksContainerBasic			0	0	
requestForRightOfWay / EmergencyContainer: EmergencyPriority			0	0	
requestForFreeCrossingAtATrafficLight / EmergencyContainer: EmergencyPriority			0	0	
noPassing / SafetyCarContainer: TrafficRule			0	0	
noPassingForTrucks / SafetyCarContainer: TrafficRule			0	0	
speedLimit / SafetyCarContainer			0	0	
reserved for future usage			0	0	
reserved for future usage			0	0	

4.1.5.2. DENM SSPs

Table 2: DENM SSPs

CauseCodeType /Container	Bit Value				
		Road Operators			
		ITSS-R (RSU)	ITSS-V (Operator mode)	ITSS-V (User mode)	
trafficCondition(1)		0	0	0	
accident(2)		1	1	1	
roadworks(3)		1	1	0	
adverseWeatherCondition-Adhesion(6)		1	1	1	
hazardousLocation-SurfaceCondition(9)		1	1	1	
hazardousLocation-ObstacleOnTheRoad(10)		1	1	1	
hazardousLocation-AnimalOnTheRoad(11)		1	1	1	
humanPresenceOnTheRoad(12)		1	1	1	
wrongWayDriving(14)		0	0	0	
rescueAndRecoveryWorkInProgress(15)		1	1	0	
adverseWeatherCondition-ExtremeWeatherCondition(17)		1	1	0	
adverseWeatherCondition-Visibility(18)		1	1	1	
adverseWeatherCondition-Precipitation(19)		0	1	1	
slowVehicle(26)		1	1	0	
dangerousEndOfQueue(27)		1	1	1	
vehicleBreakdown(91)		0	0	0	
postCrash(92)		0	0	0	
humanProblem(93)		0	0	0	
stationaryVehicle(94),		1	1	1	
emergencyVehicleApproaching(95)		1	1	0	
hazardousLocation-DangerousCurve(96)		0	0	0	
collisionRisk(97),		0	0	0	
signalViolation(98)		0	0	0	
dangerousSituation(99)		1	1	1	

4.1.6. Secured Messages

Data Messages (CAM, DENM, SPaT, …) are signed following the guidelines of the standard ETSI 103 097 v1.2.1. Secured messages are built in Geonet layer and transmitted to the Security layer.

4.1.7. Verification of message signature

4.1.7.1. Description

The present section describes the general process of the message's signature verification by using InterCor_CTL and InterCor_CRL.

4.1.7.2. Pre-conditions

For each native PKI system,

- The RCA/AA certificates are provided to the ITSS during the initialization phase.
- The RCA/AA certificates, InterCor_CTL and InterCor_CRL are assumed to be valid.
- The common InterCor_CTL and InterCor-CRL are available in the InterCor repository.
- The ITSS shall verify the InterCor_CTL and the InterCor_CRL.

4.1.7.3. Verification steps

- **Step (1):** The ITSS receives a secured message and verifies the message signature with the associated AT certificate.
- **Step (2):** The ITSS verifies that the AT certificate is issued by an AA with a valid certificate (e.g.: presence of the right AIDs list, time start and end…). The AA certificate may be retrieved either from a V2X secured exchange or from the InterCor_CTL.
- **Step (3):** The ITSS verifies that the AA certificate is issued by RCA.
- **Step (4):** The ITSS checks that HashedID8 of AA certificate is not present in InterCor_CRL.

At every step of this procedure, if one verification fails, then the signed message must be considered as invalid and must be rejected by the ITSS.

4.1.7.4. Post-conditions

The ITSS has verified the integrity of the received message by validating the signature of the secured message as well as its authenticity by validating the certificate trust chain.

4.2. InterCor_CTL Generation

The InterCor trust model is based on a multiple root CA architecture, where the RCA certificates are integrated into a common list called InterCor_CTL. The InterCor_CTL is created, signed, updated under the responsibility of the French Transport Ministry.

This list contains the trusted RCA certificates. The certificate profile of InterCor_CTL authority is based on ETSI TS 103 097 v1.2.1. The InterCor_CTL format is based on certificate profile defined in [Deliverable 2.4.4.6 of SCOOP@F]. The process to add a RCA certificate in InterCor_CTL is done in 3 steps:

- **Step (1):** A root CA's Authorized representative transmits through an organizational process a signed application form and the RCA certificate to the InterCor_CTL Authority representative.
- **Step (2):** In positive case of verifications, the InterCor_CTL Authority generates and signs a new InterCor_CTL with the new RCA certificate added.
- **Step (3):** The InterCor_CTL Authority transmits to InterCor repository which makes the InterCor_CTL public to everyone.

4.3. InterCor_CRL Generation

The InterCor_CRL is created, signed, updated under the responsibility of the French Transport Ministry.

4.4. Pseudonym Management

Every partner is free to choose his own pseudonym management strategy.

4.5. PKI operations for interoperability

The execution of the following use cases is preconditioned by the creation of RCA, AA and EA authorities. The initialization is performed during a key ceremony. Each Member State should define its own procedures to set up its PKI system.

4.5.1. InterCor_CTL download

4.5.1.1. Description

In order to update its internal list of RCA certificates, the ITSS requests the InterCor_CTL from the InterCor repository once per month and when needed.

4.5.1.2. Pre-conditions

- The ITSS has InterCor repository access point.
- The ITSS has the InterCor_CTL Authority certificate.

4.5.1.3. Service flows

As shown in, Figure 5, the request/response cycle of the InterCor_CTL can be summed up in two steps:

- **Step (1):** The ITSS sends a Get InterCor_CTL to the InterCor repository. The request for InterCor_CTL is http://InterCor_access_point/getctl/HashedId8 with the HashedID8 of the InterCor_CTL AUTHORITY certificate signing the InterCor_CTL.
- **Step (2):** The InterCor repository returns the InterCor_CTL.

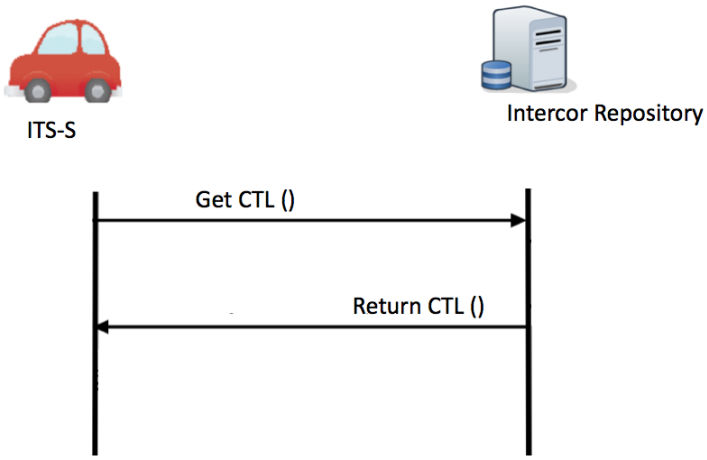

Figure 5: InterCor_CTL Download by ITSS

4.5.1.4. Post-conditions

The ITSS has downloaded the InterCor_CTL.

4.5.1.5. Potential requirements

- The ITSS must verify that the InterCor_CTL is signed by the InterCor_CTL Authority.
- The ITSS must consider the information present in the InterCor_CTL to have an up-to-date trust environment.

4.5.2. InterCor_CRL download

4.5.2.1. Description

An InterCor_CRL is requested by the ITSS from the InterCor repository.

4.5.2.2. Pre-conditions

- The ITSS has InterCor repository access point.
- The ITSS has InterCor_CTL Authority certificate.

4.5.2.3. Service flows

An ITSS sends a Get CRL request and receives a response from the InterCor repository. The request and response cycle are represented by two steps:

- **Step (1):** The ITSS sends the Get CRL request to InterCor repository. The request for InterCor_CRL is http://InterCor_access_point/getcrl/HashedId8ith the HashedID8 of the InterCor_CTL authority certificate signing the InterCor_CRL.
- **Step (2):** The InterCor repository returns the InterCor_CRL.

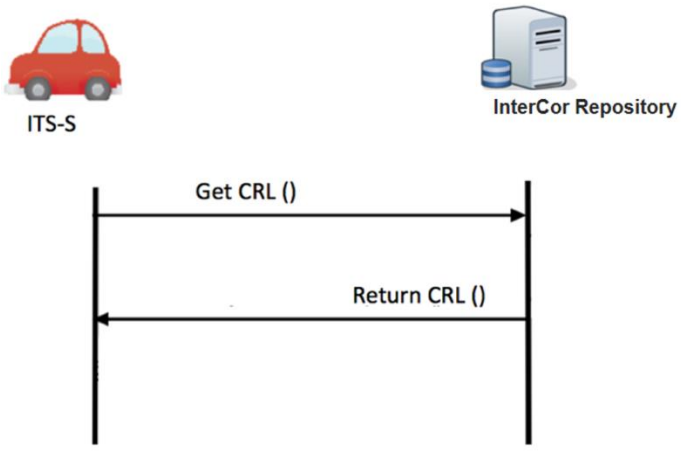

Figure 6: InterCor_CRL download by ITSS

4.5.2.4. Post-conditions

The ITSS has downloaded a InterCor_CRL.

4.5.2.5. Potential requirements

The ITSS must verify that the InterCor_CRL is signed by the InterCor_CTL Authority.

4.6. CA certificates details

The following tables illustrate the details of the certificates used in test and issued by the different certificates authorities (CAs). As shown in figure 1, one LTCA/EA is associated to the road operators.

Table 3: RCA Certificate for InterCor

Certificate data	Value
VERSION	2
SIGNER INFO	SELF
SUBJECT INFO	RCA
SUBJECT ATTRIBUTES	
Verification Key (0) Algorithm:	 Ecdsa_nistp256_with_sha256
Encryption Key (1)	N/A
Assurance Level (2) Assurance: Confidence:	 0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	N/A
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End Start: End:	Certificate issuance date 8 years after certificate issuance date. The French partner will keep the validity period of SCOOP@F PKI (20 years)
Geographic Region	NONE
SIGNATURE Algorithm:	 Ecdsa_nistp256_with_sha256

Table 4: EA certificate for InterCor

Certificate data	Value
VERSION	2
SIGNER INFO	HashedId8 of RCA certificate
SUBJECT INFO	EA
SUBJECT ATTRIBUTES	
Verification Key (0) Algorithm:	 ecdsa_nistp256_with_sha256
Encryption Key (1) Algorithm:	 ecies_nistp56
Assurance Level (2) Assurance: Confidence:	 0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	CA Basic Service (36) DEN Basic Service (37) SPaT (137) MAP (138) IVI (139)
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End Start: End:	 Certificate issuance date 5 years after certificate issuance date.
Geographic Region	NONE
SIGNATURE Algorithm:	 Ecdsa_nistp256_with_sha256

Table 5: AA Certificate for InterCor

Certificate data	Value
VERSION	2
SIGNER INFO	HashedId8 of RCA certificate
SUBJECT INFO	AA
SUBJECT ATTRIBUTES	
Verification Key (0) Algorithm:	 ecdsa_nistp256_with_sha256
Encryption Key (1) Algorithm:	 ecies_nistp56
Assurance Level (2) Assurance: Confidence:	 0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	CAM (36) DENM (37) SPaT (137) MAP (138) IVI (139)
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End Start: End:	 Certificate issuance date 5 years after certificate issuance date.
Geographic Region	NONE

Concerning InterCor_CTL and InterCor_CRL formats, description is provided in the deliverable [SCOOP_2.4.4.6] in the section 3.2.6 and 3.2.7.

4.7. Certificate of InterCor_CTL Authority

The following table illustrates the details of the certificate used by InterCor_CTL Authority to sign the InterCor_CTL and InterCor_CRL.

Table 6: Certificate details of InterCor_CTL Authority

Certificate data	Value
VERSION	2
SIGNER INFO	SELF
SUBJECT INFO	InterCor_CTL AUTHORITY
SUBJECT ATTRIBUTES	
Verification Key (0) **Algorithm:**	 Ecdsa_nistp256_with_sha256
Encryption Key (1)	N/A
Assurance Level (2) **Assurance:** **Confidence:**	 0 0
Reconstruction Value (3)	N/A
ITS AID List (32)	N/A
ITS AID SSP List (33)	N/A
VALIDITY RESTRICTIONS	
Time Start and End **Start:** **End:**	certificate issuance date 4 years after certificate issuance date
Geographic Region	NONE
SIGNATURE **Algorithm:**	 Ecdsa_nistp256_with_sha256

5. Communication protocols with PKI entities

Several communications can occur between ITSSs and PKI servers (AAs, EAs) in order to fulfil the following functions:

- AT/PC request and response,
- EC/LTC request and response,
- CTL/CRL request and response,
- CTL/CRL update and distribution.

This part has been cancelled from the expected 2.1c PKI specifications for several reasons:

- Due to the project timing constraints, none of the Member States have either the possibility or the need to specify these communication protocols and to test them within the scope of InterCoR.
- The incompatibility of the new version of ETSI TS 103 079 standard. The v1.3.1 version (released October 2017) is too early for implementation and will be validated for the first time in the ETSI Plugtest at the end of February 2019 which is close to the InterCor C-ITS services TESTFEST, scheduled in March 2019. Moreover, CTL/CRL formats and communication Protocol with PKI through ITS-G5 communication links have been recently defined in ETSI TS 102941 v1.2.1 and still need to be validated in terms of implementation.
- Member states would like to focus more on specifying security of hybrid communications and deeply evaluating PKI/security. In order to have interesting results by the end of the project, we think that we have just time to do both and specify the security tests for the C-ITS services TESTFEST in March 2019.

For the PKI/Security TESTFEST in Reims in April 2018 part of these required communication protocols were implemented according to the French SCOOP@F specifications (CTL/CRL). The majority of required PKI communications was done offline by the partners. This will be a feasible approach for the C-ITS services TESTFEST as well.

6. Certificate Policy (CP)

The scope of InterCor PKI specification work conducted in the InterCor 2.1c working group has concentrated on the harmonisation of partners PKIs implementations. The common trust model used is based on the Public Key Infrastructure (PKI) as recommended by the EC C-ITS Platform Certificate Policy and ETSI standardisation and also by similar initiatives in the world (USA Connected Vehicles). Indeed, Europe has already defined its certificate policy describing the European C-ITS Trust model based on Public Key Infrastructure.

In our 2.1c work, we followed the C-ITS Platform: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) DRAFT v1.0.1. February 2017 [4]. The certificate policy defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. In C-ITS platform CP, the PKI is composed at its highest level by root CAs “enabled” by the Trust List Manager (TLM), i.e. whose certificates are inserted in an European Certificate Trust List (ECTL), which is defined and published by the central entity TLM. The CPOC transmits the received root CA certificates to the TLM, which is responsible for collecting and signing the list of root CA certificates and sending them back to the CPOC, which make them public to everybody as described in the Certificate Policy.

We decided in InterCor not to use the TLM and CPOC entities. However, we use a common InterCor_CRL in addition to a common InterCor-CTL published in the InterCor repository managed by the French Transport Ministry. PKI French partner generates both common InterCor_CTL and InterCor_CRL data structures and defines the procedure to validate all the required management procedures related to these data structures.

Every InterCor partner has at least one Root Certificate Authority (RCA), one Enrolment Authority(EA)/Long Term Certificate Authority (LTCA) and one Authorization Authority(AA)/Pseudonym Certificate Authority (PCA). The certificates formats for CAs, ATs and ECs issued by these authorities and used for the InterCor project are defined in ETSI TS 103 097 v1.2.1. Concerning InterCor_CTL and InterCor_CRL formats, description is provided in the deliverable [SCOOP-2.4.4.6] in the section 3.2.6 and 3.2.7. In fact, the ETSI TS 102 941 version 1.1.13 given in [6] does not contain the PKIs requests and responses.

In terms of cryptoagility, the cryptographic algorithms used in InterCor PKI system are defined in ETSI Standard TS 103 097 v1.2.1, some are used for signing, others for encryption (ECDSA_nistP256_with_SHA256/ ECIES_nistP256_with_AES128_CCM). Some studies on cryptoagility and revocation were done in the context of 2.1c activity and we decided to remove those issues from our scope. We are compliant to the rest of C-ITS Platform CP recommendations and requirements.

7. Conclusions and future work

This document describes the v1.0 of the specifications of PKI and the common CP for InterCor. These specifications will be implemented in the participating countries, based on which European interoperability will be tested in PKI/Security TESTFEST. Actually, the first tests have been done in April 2018 at Reims (France). The second tests will occur during the C-ITS services TESTFEST in March 2019. Missing information in this document (SSPs and missing PKIs technical documentations) will be included in a re-issued version v2.0 in May 2019.

Collaboration with the InterCor sub-activity 2.1b will take place to specify the security of hybrid data communications for instance a security solution for InterCor hybrid interface (IF2) including authentication, authorization/access control and integrity based mechanisms.

A second collaboration with the InterCor sub-activity 4.2 will take place to define a list of evaluation objectives as well as a short list of KPIs (Key Performance Indicators) to be analysed during the C-ITS services TESTFEST in March 2019. These KPIs will include KPIs for PKI as well as KPIs for message security.

8. Bibliography

[1] Reference documentation List, InterCor_A2.1.c_001, May 2017, Internal Document.

[2] PKIs Trust models, InterCor_A2.1.c_002, May 2017, Internal Document.

[3] Gap Analysis, InterCor_A2.1.c_003, May 2017, Internal Document.

[4] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) DRAFT, v1.0.1, February 2017.

[5] ETSI TS 103 097 : ITS security: security header and certificate formats, v1.2.1, (2015-06)

[6] ETSI TS 102 941: ITS Security: Trust and Privacy Management, v1.1.1.

[7] SCOOP_2.4.4.6 PKI architecture and technical specifications (v2), release 2, 2017, http://www.scoop.developpement-durable.gouv.fr/en/technical-specifications-a22.html.

[8] Revocation and crypto-agility requirements for ITS stations, InterCor_A2.1.c_004, October 2017, Internal Document.

[9] PKI testing options, InterCor_A2.1.c_005, October 2017, Internal Document.

