



French C-ITS Deployment Coordination committee

Security System: Integration Guide for Migration of Pilot Validation PKI

2.4.4.8_M

Activity 2: Studies

Sub Activity 2.4 > Specifications

Version 0.60 (validated)

Publication Date: 26/03/2024



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

Information on the document

Document: 2.4.4.8_M Security System: Integration Guide for Migration of Pilot Validation PKI

Responsible, Entity: Rida Khatoun (Telecom Paris)

Publication history

Date	Version	Author(s)	Updates & changes	Diffusion
	0.1		<ul style="list-style-type: none">First Draft	COCSIC
	0.3	IDnomic	<ul style="list-style-type: none">Section 2.2	COCSIC
08/03/2020	0.4	Telecom Paris	<ul style="list-style-type: none">Integration of comments/corrections after the Migration security GT meeting of 25/02/2020Add sectionsAdd Annex1Add Annex2Delete section PKI validation platformDelete section web serviceAdd Annex 3Update referencesUpdate Acronyms	COCSIC
09/03/2020	0.01	A.Foulquié, Viveris AMO DIT	Formatting, adjusting version number as per project administration rules	COCSIC
17/03/2020	0.01	H. Labiod Telecom Paris	Integration of G. Richard, A. Foulquié and E. Petit corrections/comments	COCSIC
20/03/2020	0.1	A.Foulquié, Viveris AMO DIT	Document approved	COCSIC
10/08/2020	0.11	H. Labiod, Telecom Paris	Integration of retroaction in section 3.7.1. The retroaction concerns mainly the generation time field	COCSIC
03/09/2020	0.20	H. Labiod, Telecom Paris	Integration of corrections of A. Foulquié <ul style="list-style-type: none">Remove version number of 2.4.4.6, and 2.4.4.8 deliverables2.4.1_H replaced by 2.4.1_M	COCSIC
14/09/2020	0.21	G. Richard IDnomic	<ul style="list-style-type: none">Section 2.2 page 11 updatedAnnex 3 page 32 updated	COCSIC
14/10/2020	0.30	A.Foulquié, Viveris AMO DIT	<ul style="list-style-type: none">Link corrected page 11Document approved following COCSIC-Etudes meeting of september 23rd	COCSIC
02/07/2021	0.31	Jun Zhang Telecom Paris	<ul style="list-style-type: none">Section 2.2 page 11 updatedSection 2.4 page 13, Table 2 updated	COCSIC
07/09/2021	0.32	Jun Zhang Telecom Paris	<ul style="list-style-type: none">Section 3.1 page 14, provide more detail in canonical ID or UIDReplace ITSS by ITS-SReplace ETSI TS 103 097 V1.3.1 by 1.4.1Replace ETSI TS 102 094 V1.3.1 by 1.4.1Section 2.4, move the part of AT parameters from annex 3 to table 2, and separate the cases of Pilot Validation PKI and production PKI	COCSIC

			<ul style="list-style-type: none"> Section 2.4, add the sentence “It is suggested to use 2 days as the validity duration of AT, for personal data protection purposes.” 	
31/12/2021	0.34	Jun Zhang Telecom Paris	<ul style="list-style-type: none"> Combine the content of 2448 into 2448_M Put part of contents into exigences Update the service flow for V-ITS-S with cellular communication Update the security for Nfr-ITS-S and BI Add the AT policy for pedestrian 	COCSIC
January 2022	0.35	Antoine Foulquié, Viveris AMO DIT	<ul style="list-style-type: none"> Formatting Text correction 	
Octobre 2022	0.36	Rida Khatoun Telecom Paris	<ul style="list-style-type: none"> English correction and formatting Add section 4 "Secured Protocols" from 2.4.4.8 Add section 5 "MAC/IP/Geonetworking Address and Station ID change scheme" from 2.4.4.8 Add section 6 "PKI Validation platform" from 2.4.4.8 Add some recommendations (from tickets discussions) 	COCSIC
2022/11/07	0.37	Antoine Foulquié	<ul style="list-style-type: none"> Minor corrections 	
02/01/2023	0.38	Rida Khatoun Telecom Paris	<ul style="list-style-type: none"> Update Tables 2 and 3 Update of all images Formatting Add requirements Update requirements Removed section 4 Secured Protocols (outdated) 	
09/01/2023	0.39	Antoine Foulquié	<ul style="list-style-type: none"> Minor corrections Comments for COCSIC discussion 	
27/01/2023	0.40	Rida Khatoun	<ul style="list-style-type: none"> English correction Update section upon remarks on cocsic of 26/01/2023 Remove any ITS-S request through R-ITS-S 	
23/02/2023	0.40	Thiwiza BELLACHE (Viveris AMO DMR)	<ul style="list-style-type: none"> Version approved following COCSIC études of January 	COCSIC études
26/09/2023	0.41	Rida Khatoun	<ul style="list-style-type: none"> Retroaction 1592: Update of 2448M-STAND-001,2448M-CMGM-004,2448M-CMGM-005,2448M-CMGM-006,2448M-CMGM-007. Retroaction 1406: Update 2448M-CPKI-002 Retroaction 1608 : Update 2448M-PKIEH-009, Retroaction 1514: Update 2448M-ARHA-003 Retroaction 1575: Update 2448M-ARHA-004, 448M-CMMGM-008, 2448M-ARCM-003 Retroaction 1161: chapter 2 updated (in v0.40) Retroaction 1306: 2448M-SENF-003 updated (in v0.40) Retroaction 1219: 2448M-BI-001 updated (in version 0.40) 	
26/09/2023	0.50	Thiwiza BELLACHE	New version with validated retroactions (editorial) following CE of sept:	COCSIC Studies

			1161,1219,1306,1406,1408,1514,1592,1575. Minor corrections	
22/11/2023	0.50	Rida Khatoun	Minor corrections following the retroactions: 1673 Minor corrections	
26/03/2024	0.51	Rida Khatoun	Corrections following the retroactions: 1064, 1673, 1692 and 1710 Update of table 2 <ul style="list-style-type: none"> Add 2 requirements : 2448M-VALID-002 and 2448M-VALID-003 Add chapter IPv6 (Intégration du doc 2416 (IPv6 addressing over G5) : 2448M-IPv6-001, 2448M-IPv6-002	
26/03/2024	0.60	Thiwiza BELLACHE	Validated document following “retroaction CE meeting of 15/03/24”	CE

Quality rules

Reference to the version administration

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

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

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

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

As illustration:

0.03 > Work in progress version

0.10 > Del. Approved by SC Studies but not released

2.00 > Del. approved & released (in release 2)

2.05 > Del. Updated - in progress version

Requirements identification & traceability

In this document, the following verbal forms are used to indicate requirements: **Shall / Shall not**

Recommendations shall be indicated by the verbal forms: **Should / Should not**

Permissions shall be indicated by the verbal forms: **May / May not**

Possibility and capability shall be indicated by the verbal forms: **Can / Cannot**

Inevitability used to describe behaviour of systems beyond of the scope of this del. shall be indicated by: **Will / Will not**

Facts shall be indicated by the verbal forms: **Is / Is not**

In the table here below:

2.4.X.XX > is the number given to the deliverable (e.g. 2.4.4.8)

YYYY > for digit are given to identifying which component/entity the requirement is addressing (e.g. LTCA for long term certificate authority)

ZZZ > is the numeration of the requirement

ID	2.4.X.XX-YYYY-ZZZ
Component(s)	(e.g.) Vru-ITS-S, Vro-ITS-S, R-ITS-S, PKI
Requirement	(e.g.) An ITS station SHALL be able to request and get a Long-Term Certificate (LTC) from the SCOOP Public Key Infrastructure (PKI).
Acceptance	(e.g.) CA1: Vru-ITS-S sends a LTC request to the LTCA CA2: R-ITS-S relays the LTC request CA3: The LTCA verifies the request and sends a response CA4: The R-ITS-S relays the response CA5: The response is received by the Vru-ITS-S and is valid
Additional information	

Acronyms

AA	Authorization Authority
AID	Application Identifier (equivalent to PSID)
AT	Authorization Ticket
CA	Certification Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
CP	Certificate Policy
CRL	Certificate Revocation List
CTL	Certificate Trust List
CPOC	C-ITS Point of Contact
DC	Distribution Centre
EA	Enrollment Authority
EC	Enrollment Certificate
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECTL	European CTL
EU CCMS	European C-ITS Credential Management System
GN	Geo Networking
ITS-S	ITS Station
ITS-AID	ITS Applications ID
LTC	Long-Term Certificate
LTCA	Long-Term Certificate Authority
NAP-SER	National Application Server (smartphone application)
Nfr-ITS-S	National French ITS-S
PC	Pseudonym Certificate
PCA	Pseudonym Certificate Authority
PSID	Provider Service Identifier (equivalent to AID)
PP	Pre-Production
RCA	Root Certificate Authority
R-ITS-S	Roadside ITS Station (RSU in the French Terminology)
SSP	Specific service permissions
TLM	Trust List Manager
TSL	Trusted Service List
UID	Unique Identifier
V-ITS-S	Vehicle ITS-S
Vro-ITS-S	ITS-station for road operators vehicles in operator mode
Vru-ITS-S	ITS-station for road operators vehicles in user mode
ESP	Encapsulating Security Payload
IPsec	IP security
HA	Home agent

Table of Contents

Quality rules	5
Acronyms	6
Table of Contents	7
List of figures	9
List of requirements	10
1. Deliverable's purpose	12
2. Presentation	13
2.1 Security standards and security reference documents	13
2.2 Pilot migrated validation PKI System description	14
2.3 Communication with PKI servers	18
2.3.1 ITS-S Registration	19
2.3.2 EC request	20
2.3.3 AT Request	21
2.3.4 Road Operator Case	23
2.3.5 CRL download	24
2.3.6 CTL download	25
2.3.7 Message signature verification with CTL and CRL	27
2.4 EC and AT certificates' management	27
2.4.1 ATs storage in ITS-Ss	28
2.4.2 ATs change strategy	28
2.5 PKI requests errors handling	32
3. Security elements	32
3.1 Canonical ID or UID	32
3.2 ITS-AIDs & Psid	33
3.3 Service Permissions (SSPs) & App permissions	33
3.4 Certificates	34
3.5 Certificate profiles	35
3.6 Validity duration of certificates	35
3.7 Secured C-ITS messages	35
3.7.1 Secured data structure format	35

3.7.2	Security profile for C-ITS messages	36
3.8	Signature verification algorithm	37
4.	MAC/IP/Geonetworking Address and Station ID change scheme	37
4.1	MAC address and StationID	38
4.2	IPv6 Address	39
4.3	Geonetworking Address	39
5.	PKI Validation platform	39
5.1	Introduction	39
5.2	CA Hierarchy	39
5.3	CA certificates details	40
5.4	ITS Station profiles	40
5.5	Hosting	42
5.6	Access	43
6.	Security elements for the Nfr-ITS-S	43
7.	Security for hybrid communications	44
7.1	General requirement	44
7.2	Architecture with a Home Agent in case of using IPv6	45
7.3	Architecture with a Car Manufacturer Platform	46
7.4	Architecture supporting V2V communication through cellular network	48
7.5	Architecture for road operators	48
8.	Security elements for BI	51
9.	IPv6	51
10.	Bibliography	56
11.	Annexes	58
11.1	Annex 1: Association Table	58
11.2	Annex 2: List of actors	59
11.3	Annex 3: PKI main parameters	60

List of figures

Figure 1: European CCMS trust model	15
Figure 2: The pilot migrated validation PKI System Architecture (PP for Pre-Production)	16
Figure 3 – Trust model elements involved in the verification of a message received from a foreign C-ITS station	17
Figure 4 : EC Request and EC Response (R-ITS-S case and V-ITS-S case through cellular communication)	20
Figure 5 : AT Request and AT Response for an ITS-S through cellular communication.....	22
Figure 6 : ATs pool requests and responses (V-ITS-S case through R-ITS-S)	22
Figure 7 : AT Request/Response (Vru-ITS-S/Vro-ITS-S cases).....	24
Figure 8 : CRL Download by R-ITS-S and V-ITS-S through cellular communication	25
Figure 9 : : CTL Download by an ITS-S through cellular communication	26
Figure 10 : ATs storage in an ITS-S.....	28
Figure 11 : 2:Canonical ID (or UID).....	33
Figure 12 : Generation mechanism of StationID and MAC Address for a V-ITS-S	38
Figure 13 : CAs hierarchy overview	40
Figure 14 : Architecture with Home Agent (Uplink Communication).....	45
Figure 15 : Architecture with a PFcm (uplink communication).....	47
Figure 16 : V2V-communication using cellular technology	48
Figure 17 : GLOSA architectures ((a): with local traffic light controller, (b): with centralized traffic light controller)	49

List of requirements

Requirement	Page
2448M-STAND-001	12
2448M-STAND-002	12
2448M-VALID-001 (1)	16
2448M-VALID-002	17
2448M-VALID-003	17
2448M-PVPKI-001 (3)	17
2448M-PVPKI-002	17
2448M-CPKI-001 (2)	17
2448M-CPKI-002 (3)	17
2448M-REGI-001 (2)	18
2448M-ECREQ-001 (2)	19
2448M-ATREQ-001 (2)	22
2448M-CRLREQ-001 (2)	24
2448M-CTLREQ-001 (2)	25
2448M-CMGM-001 (2)	27
2448M-CMGM-002 (2)	28
2448M-CMGM-003 (2)	28
2448M-CMGM-004 (3)	29
2448M-CMGM-005 (3)	29
2448M-CMGM-006 (3)	29
2448M-CMGM-007 (1)	30
2448M-CMMGM-008 (2)	30
2448M-CMGM-009	30
2448M-PKIEH-009 (1)	31
2448M-CERT-001 (3)	33
2448M-CERT-002 (3)	33
2448M-FORMAT-001	34
2448M-FORMAT-002 (1)	34
2448M-SECM-001(2)	34
2448M-SECM-002 (2)	34
2448M-SECM-003 (2)	34
2448M-SECM-004 (2)	35
2448M-VERI-001	35
2448M-ASIDC-001	36
2448M-SENF-001	41
2448M-SENF-002 (2)	41
2448M-SENF-003	41
2448M-GENERAL-001	42
2448M-ARHA-001 (2)	43
2448M-ARHA-002 (2)	43
2448M-ARHA-003 (3)	44
2448M-ARHA-004 (2)	44
2448M-ARCM-001 (2)	45
2448M-ARCM-002 (2)	45
2448M-ARCM-003 (1)	45
2448M-V2VC-001 (2)	46
2448M-ARRO-002 (2)	46
2448M-BI-001 (1)	48
2448M-BI-002	48

2448M-IPv6-001	50
2448M-IPv6-002	51

1. Deliverable's purpose

This deliverable aims at giving all security details needed to migrate the current security system implemented in the different projects to a new release by applying a new security trust model according to the new versions of ETSI security standards.

Naming of entities in the trust model has changed; therefore to simplify reading we provide an association table (see Annex 1).

As of November 2022, the old security integration guide for scoop project, 2.4.4.8 is considered obsolete and will no longer be maintained; all relevant parts will be integrated into this deliverable 2.4.4.8_M. When there is no explicit mention, the description is valid both for validation and production environments.

2. Presentation

For information, in this deliverable, when the acronym V-ITS-S is used alone, it represents the ITS-S associated to all types of vehicles (V-ITS-S for user vehicles, Vru-ITS-S for operator in user mode, Vro-ITS-S for road operator vehicles). When we need to distinguish vehicles, we use the appropriate acronym explicitly. Also, the acronym ITS-S is used to represent V-ITS-S, R-ITS-S or Nfr-ITS-S.

2.1 Security standards and security reference documents

Id	2448M-STAND-001 (1)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	ITS stations shall comply to ETSI TS 103 097 [1] and ETSI TS 102 941 [2] standards
Additional information	

Id	2448M-STAND-002
Component(s)	PKI operators, stations operators
Requirements and configuration	PKI operators and stations operators shall comply to the Certificate Policy [3]
Additional information	

The main references documents are listed in the table 1.

cope	Reference Document
Trust Model	Certificate Policy Release v1.1 [3]
Certificate Data Structures	ETSI TS 103 097 V.1.4.1
Cryptographic Algorithms	ETSI TS 103 097 V.1.4.1 (NIST / Brainpool) Certificate Policy v1.1
TL and CRL Data Structures	ETSI TS 102 941 V1.4.1
Requests for communication with the PKI	ETSI TS 102 941 V1.4.1
Packet types for the different communication modes	ETSI EN 302 636-4-1 V1.3.1

Table 1: List of main security standards and reference documents

ETSI TC ITS defines security as a vertical layer adjacent to the access, networking and facilities layers. The corresponding security services are provided on a layer-by-layer basis through specific service access points (SAP). In this context, ETSI TS 103 097 specifies the main security components, including the security headers, certificate formats and security profiles, and reuses as much as possible the existing IEEE 1609.2 security standard [4]. The main security header is

the SecuredMessageStructure, which specifies how to encode a generic security message, which is itself encapsulated inside a GeoNetworking packet.

ETSI TS 103 097 specifies various type of certificates including:

- Authorization tickets.
- Enrolment credential.
- Root CA certificates.
- Subordinate certification authority certificates.
- Trust List Manager certificate.

ETSI TS 102 941 specifies the trust and privacy management for V2X communications. Based upon the security services defined in ETSI TS 102 731 [5] and the security architecture defined in ETSI TS 102 940 [6], it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [7]. It specifies trust and privacy management in the field of ITS-S Security Lifecycle

- Public Key Infrastructure (PKI)
- Generation, distribution and use of Trust information lists,

and specifies the security association and key management between ITS Stations.

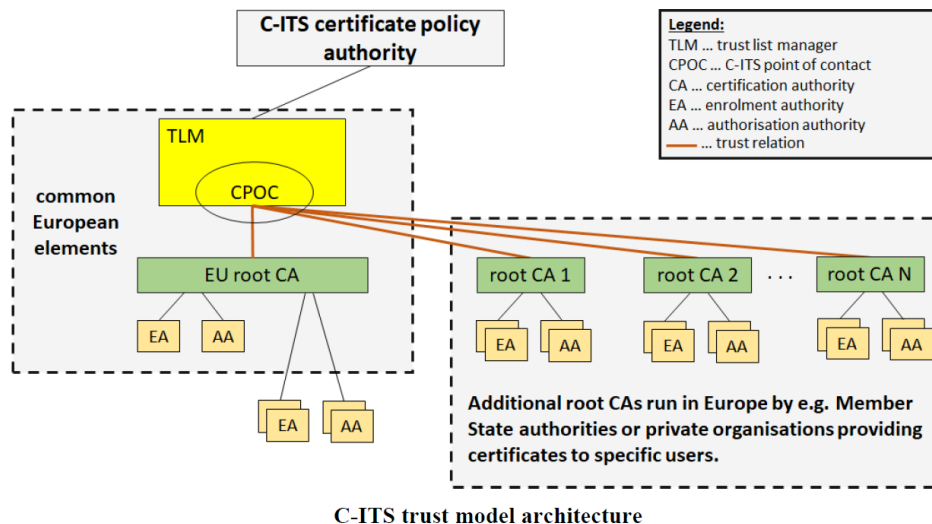
Certificate Policy (CP) and (Security Policy (SP) define the European C-ITS Trust model based on Public Key Infrastructure within the scope of the overall EU C-ITS Credential Management System (EU CCMS). It defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe.

2.2 Pilot migrated validation PKI System description

In order to assure the privacy and the security of communications between ITS-stations or ITS-Ss (V-ITS-S, R-ITS-S, Nfr-ITS-S), a public key infrastructure (PKI) is used to maintain trust between ITS-stations in one side and between ITS-stations and authorities in the other side.

Following the published version of the CP [3], the European PKI system manages the following elements:

- **Enrolment Certificate (EC):** gives its holder (ITS-Ss) the right to request ATs.
- **Authorization Ticket (AT):** gives its holder (ITS-Ss) the right to sign C-ITS messages.
- **Certificate Revocation List (CRL):** is a list digitally signed by a RCA that contains certificates authorities that are no longer valid.
- **Certificate Trust List (CTL):** is a signed list which contains trusted RCAs, EAs (Enrolment Authority) and AAs (Authorization Authority) certificates and PKI service access points.
- **European Certificate Trust List (ECTL):** is a list that contains all trusted RCAs within Europe. The ECTL is downloaded by C-ITS stations from the C-ITS Point of Contact (CPOC) to verify messages from other stations which are assigned to another root.
- **Trust List Manager (TLM) :** is the European entity that signs the ECTL. The purpose of the Trust List Manager (TLM) is to put trusted RCA certificates on a European Certificate Trust List (ECTL) and to sign this list with the TLM current valid private key.
- **C-ITS Point of Contact (CPOC):** is the website that hosts the ECTL and the TLM certificate (<https://cpoc.jrc.ec.europa.eu/>)



C-ITS trust model architecture

Figure 1: European CCMS trust model

Based on the specified European trust model architecture, we define a pilot migrated validation PKI core system composed of four main entities as shown 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 signature of EAs and AAs certificates. It contains the permissions that can be issued to Sub CAs (EAs & AAs).
- **Enrolment Authority (EA):** is a security management entity responsible for the issuance of EC and the validation of ATs requests as well as the management of the ITS-Ss (registration, status update, permissions...). It operates in an online mode.
- **Authorization Authority (AA):** is a security management entity responsible for the delivery, the monitoring and the use of ATs. It operates in an online mode.
- **Distribution Centre (DC):** provides the ITS-Ss with the updated trust information such as CTL and CRL necessary to assure that received message is coming from legitimate and authorized ITS-Ss or PKI certificates authority.

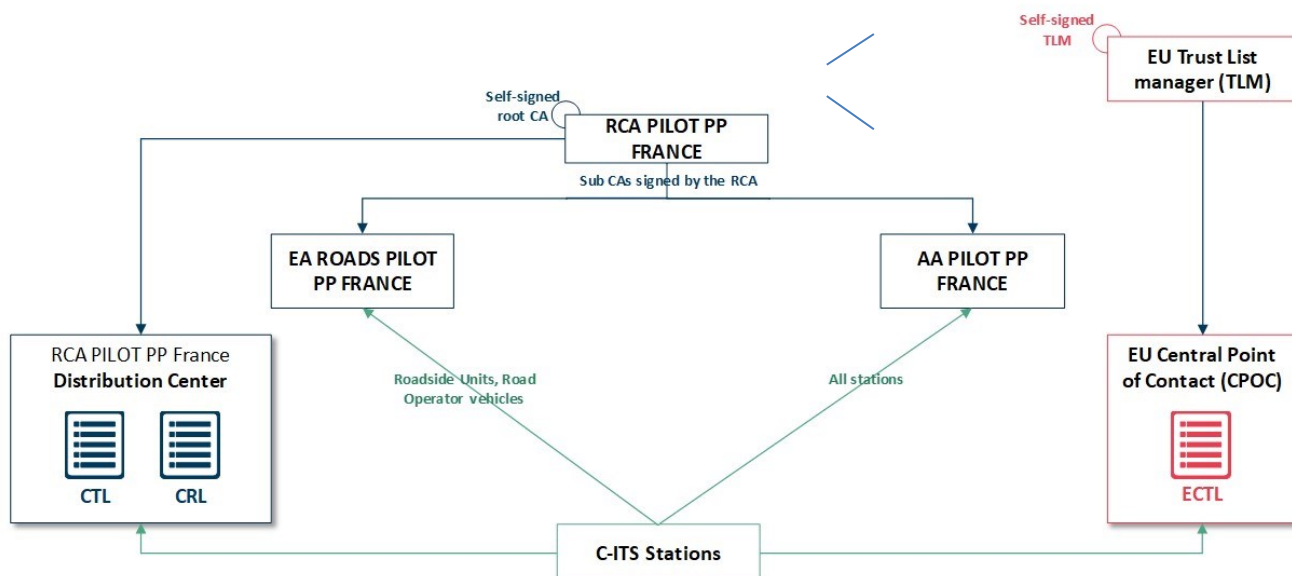


Figure 2: The pilot migrated validation PKI System Architecture (PP for Pre-Production)

As illustrated in Figure 2, there are different authorities:

- 1 RCA PILOT PP FRANCE
- 1 EA for ROADS PILOT PP FRANCE (for road operators)
- 1 AA: 1 AA SCOOP PILOT PP FRANCE

The RCA, EA and AA can have several valid certificates at the same time with the same name. The CRL for EA and AA certificates is defined in ETSI TS 102 941. The rules for verification of the Root CA certificate against the CTL are defined in ETSI TS 102 941.

Id	2448M-VALID-001(2)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	To verify the signature of a message signed by a foreign AT (ie. under a foreign root CA), a station shall validate the complete trust chain behind the AT that signed the received message [2]. This chain includes the certificates of all authorities involved in certificates signatures. An ITS-S must be able to automatically retrieve any of these certificates when an unknown ITS-S is encountered. The steps to validate a signature are described in the appendix of the document C-Roads_TF1_C-ITS_Security_Requirements_and_Specifications [12]
Additional information	

Id	2448M-VALID-002
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	for C-Roads tests, the level 0 (L0) of the EU Central Elements (TLM & ECTL) shall be used (see [21] section 2.4, and [22]).
Additional information	

According to the EU CCMS trust model (see Figure 3):

A foreign AA certificate can be obtained directly from the sending station or in the Distribution Center (DC) of the foreign RCA

- A foreign RCA certificate is available in the ECTL and in the Distribution Center (DC) of the foreign RCA
- ECTL is available on the CPOC website (<https://cpoc.jrc.ec.europa.eu/ECTL.html>)
- TLM certificate is also available on the CPOC website (<https://cpoc.jrc.ec.europa.eu/TLMCertificates.html>)
- The foreign CRL is available in the Distribution Center (DC) of the foreign RCA

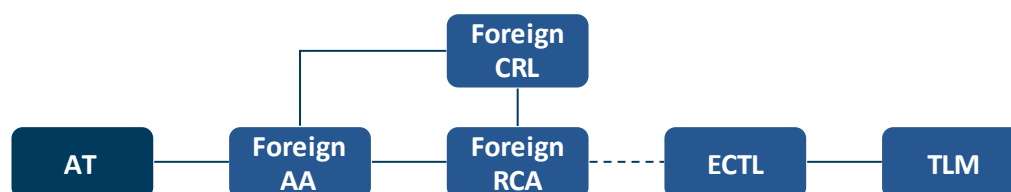


Figure 3 – Trust model elements involved in the verification of a message received from a foreign C-ITS station

URLs of foreign Distribution Centers shall be retrieved from the ECTL published by the European Commission on the CPOC (<https://cpoc.jrc.ec.europa.eu/>).

Id	2448M-VALID-003
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	URLs of foreign Distribution Centers shall be retrieved from the ECTL published by the European Commission on the CPOC website
Additional information	CPOC website : https://cpoc.jrc.ec.europa.eu/

Documentation of the CPOC protocol is available here:

https://cpoc.jrc.ec.europa.eu/data/documents/EU_CCMS_CPOC_Protocol_Release_1_2.pdf

CPOC protocol is applied for L0, L1 and L2.

Id	2448M-PVPMI-001 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	<p>Different cryptographic algorithms must be supported by C-ITS stations (as defined in the European CP [3]):</p> <ul style="list-style-type: none"> • ECDSA_nistP256_with_SHA256 (signing messages and signature verification) • ECDSA_brainpoolP256r1_with_SHA256 (signing messages and signature verification) • ECDSA_brainpoolP384r1_with_SHA384 (signature verification) • ECIES_nistP256_with_AES128_CCM (requests encryption) • ECIES_brainpoolP256r1_with_AES128_CCM (requests encryption)
Additional information	

Id	2448M-PVPMI-002
Component(s)	PMI servers
Requirements and configuration	Pilot validation PMIs as well as for production PMIs shall follow the main parameters listed in Annex 3.
Additional information	

2.3 Communication with PMI servers

The execution of the following use cases is preconditioned by the creation and the initialization of RCA and EAs for each of the car manufacturers as well as road operators. The RCA, EA and AA initialization (key generation) is performed during key ceremony.

Id	2448M-CPMI-001 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS, PMI servers
Requirements and configuration	Communication protocol with PMI is based on http connection as defined in the section 2.3.1 to 2.3.7, and section 4.5.2 in [23].
Additional information	

Id	2448M-CPMI-002 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S, PMI servers

Requirements configuration and	Authorization tickets should be downloaded manually or using a cellular technology for validation, and only by cellular technology for production, according to European CP [3] and SP [24].
Additional information	For validation case, the Nfr-ITS-S should download the AT by wire networks.

2.3.1 ITS-S Registration

2.3.1.1 Description

The registration procedure consists of registering an ITS-S in the PKI and it is manually performed by the manufacturer using a web browser.

2.3.1.2 Pre-conditions

The manufacturer has the right of access to PKI. A list of profiles to be assigned to the ITS-Ss is provided on the HMI by the operator.

2.3.1.3 ITS-S registration

The registration request is done by an IHM on the following link:
<https://0.fr-op-roads.io/c-its-pki.eu/>

2.3.1.4 Post-conditions

The ITS-S is registered in an internal database of EA and activated.

2.3.1.5 Potential requirements

- The canonical ID of the ITS-S must be unique per EA.
- The ITS-Ss canonical IDs respect the format defined in the section 3.1.
- The technical key pair (TPK: technical public key, TSK: technical secret key) is generated. TSK and TPK are generated in the HSM based on the algorithm ECDSA NIST P-256.
- Certificates for CAs and their access points are manually installed inside the ITS-S during the initialization phase (see section 6).

Id	2448M-REGI-001 (2)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S,-S, EA
Requirements configuration and	The canonical ID of the ITS-S must be unique per EA, respect the format defined in the section 3.1 and adopted by all road operators as well as the car manufacturers
Additional information	

2.3.1.6 Extensions

A manufacturer might proceed to the registration of multiple ITS-Ss via a .csv file with the following elements included: canonical IDs and technical public keys. A common profile for the whole list is selected from the list provided in the HMI.

2.3.2 EC request

2.3.2.1 Description

This action consists of requesting an EC from the EA and it is performed by the ITS-Ss (V-ITS-S or R-ITS-S) following the registration phase. The EC duration is to be fixed by the manufacturers and road operators.

2.3.2.2 Pre-conditions

- The ITS-S is already registered in the EA internal database and activated.
- The ITS-S has its verification key pair.
- The ITS-S has the EA's access point link and certificate.

2.3.2.3 Flow diagram

When an ITS-S needs a new EC, it starts by sending an EC request to the EA which sends back a response. Figure 4 describes the request/response cycle represented by three steps:

- **Step (1):** The ITS-S sends a EC request to the EA.
- **Step (2):** The EA verifies the request. If it is NOT correct, it sends an HTTP status code 400. Else, it processes the request and sends the EC response.
- **Step (3):** The ITS-S extracts the Enrollment Certificate (EC) from the EC response.

An ITS-S such as Vro-ITS-S, Vru-ITS-S and R-ITS-S communicates with EA by cellular technology .

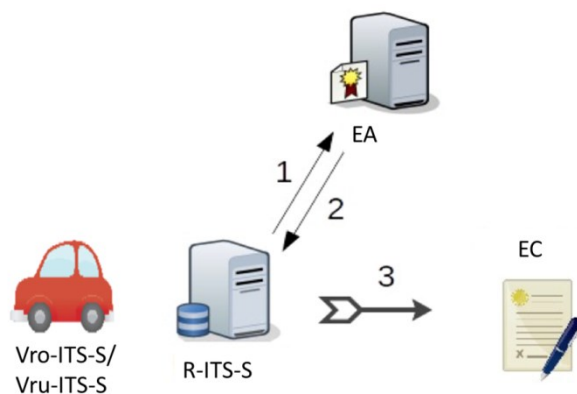


Figure 4 : EC Request and EC Response (R-ITS-S case and V-ITS-S case through cellular communication)

2.3.2.4 Post-conditions

- The ITS-S has its new EC whose format is described in the ETSI 103097 standard.
 - Returned EC's validity duration is compliant to values filled in the EC request (optional beginning date and ending date);
 - For validation, if dates are not filled in the EC request, returned default validity duration is a value defined in the profile.

2.3.2.5 Potential requirements

- The ITS-S has to renew its EC before the expiration of the previous one. A renew request must be signed by the previous EC.
- The EC verification key pair must be generated in the HSM based on the algorithm ECDSA NIST P-256.
- The signature of the EC request has to be verified.

Id	2448M-ECREQ-001 (2)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	Each ITS-S has to renew its EC before the expiration of the previous one. The key pair must be generated in the HSM based on the algorithm ECDSA NIST P-256. A renew request must be signed by the previous EC.
Additional information	For information, a technical key is used during the first request for an EC. Before the expiration of the EC, an ITS-S requests a new EC and sign the request by the last valid EC. If the EC is no longer valid, the technical key must be used as in the initialization phase.

2.3.3 AT Request

2.3.3.1 Description

This action consists of requesting an AT from the AA. It is performed by R-ITS-Ss and Vro-ITS-S/Vru-ITS-Ss in order to have the required reserve for the coming period (fixed to six months for validation, and three months for production).

2.3.3.2 Pre-conditions

- The AT lifetime is already defined in the ITS-S profile during the registration phase.
- The ITS-S has a valid EC.
- The ITS-S has EA and AA access points and certificates.
- The ITS-S has already generated the needed ATs verification key pairs.
- The ITS-S knows the SSPs of ITS-AIDs to be used.

2.3.3.3 Flow diagram

a) Acquiring of an AT

When an ITS-S needs a new AT, it has to send an AT request to the AA, which sends back an AT

response. As illustrated in Figure 5, this request/response cycle contains five steps:

- **Step (1):** The ITS-S sends the AT request (with a starting date) to the AA.
- **Step (2):** The AA verifies the AT request. If it is NOT correct, it sends a HTTP status code 400. Else, it processes the request and sends the validation AT request to the EA.
- **Step (3):** The EA sends the validation AT response to the AA.
- **Step (4):** The AA sends the AT response to the ITS-S.
- **Step (5):** The ITS-S extracts the Authorization Ticket (AT) from the AT response.

The following process is applied in the case of acquiring an AT for V-ITS-S, Vro-ITS-S, Vru-ITS-S and R-ITS-S. Cellular technology is used to send the request.

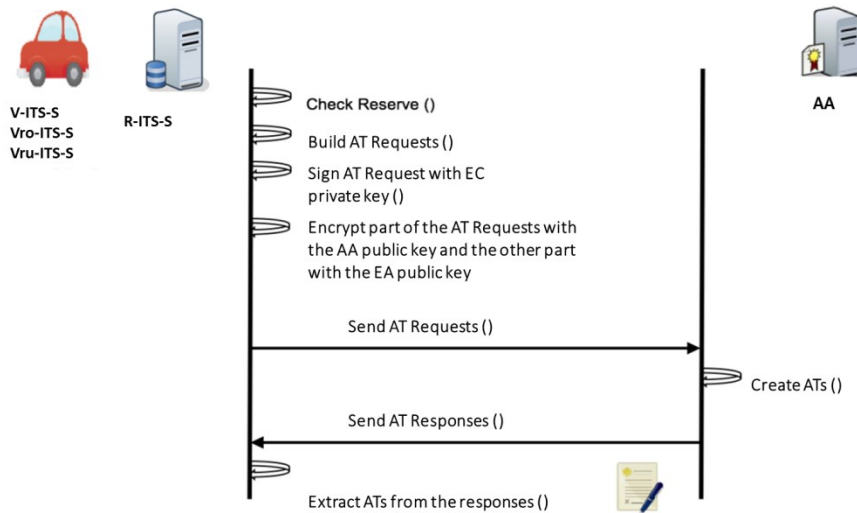


Figure 5 : AT Request and AT Response for an ITS-S through cellular communication

b) Request for a pool of ATs

To upload a pool of n ($n > 1$) ATs, an ITS-S sends n requests and receives n responses following the same steps described in section 2.3.3.3. Figure 6 illustrates the case of manufacturer vehicles through R-ITS-S.

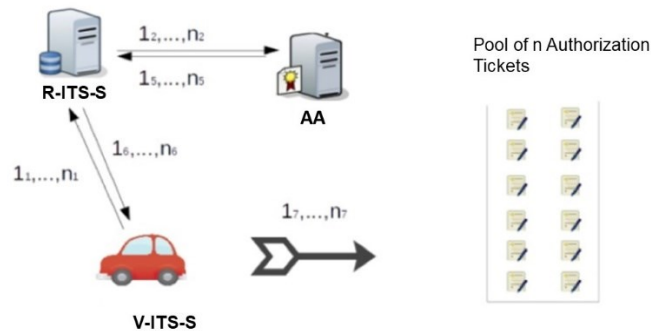


Figure 6 : ATs pool requests and responses (V-ITS-S case through R-ITS-S)

2.3.3.4 Post-conditions

- The ITS-S has its new AT.

2.3.3.5 Potential requirements

- The signature of the AT request has to be verified.

Id	2448M-ATREQ-001 (2)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	Each ITS-S has to request AT from the AA. The ATs verification key pair must be generated in the HSM of the ITS-S based on the algorithm ECDSA NIST P-256.
Additional information	

2.3.4 Road Operator Case

In road operator networks, to support their specific use cases, we define one EC and two associated ATs, the first one for classical usage or user mode and the second for operator usage or operator mode. These two ATs are distinguished by their supported SSPs related respectively to each of the two modes. Two pools of ATs are filled: a first one for user mode and a second one for operator mode. When a V-ITS-S (in mode user/operator) needs a new AT, it has to send AT requests and receive AT responses from the AA. This request/response cycle goes through five steps (see Figure 7):

- **Step 1:** The V-ITS-S (in mode user/operator) sends 2 AT requests to obtain 2 ATs (AT1 user with VerificationKey1 vs. AT2 road operator with VerificationKey2).
- **Step 2:** The AA verifies each of the request. If one is NOT correct, it sends a HTTP status code 400. Else, it processes the requests and sends the AT validation requests to the EA.
- **Step 3:** The EA sends the AT validation responses.
- **Step 4:** The AA sends the AT validation responses to the V-ITS-S.
- **Step 5:** The V-ITS-S (in mode user/operator) extracts the Authorization Ticket (AT) from the AT validation responses (AT1 user and AT2 road operator).

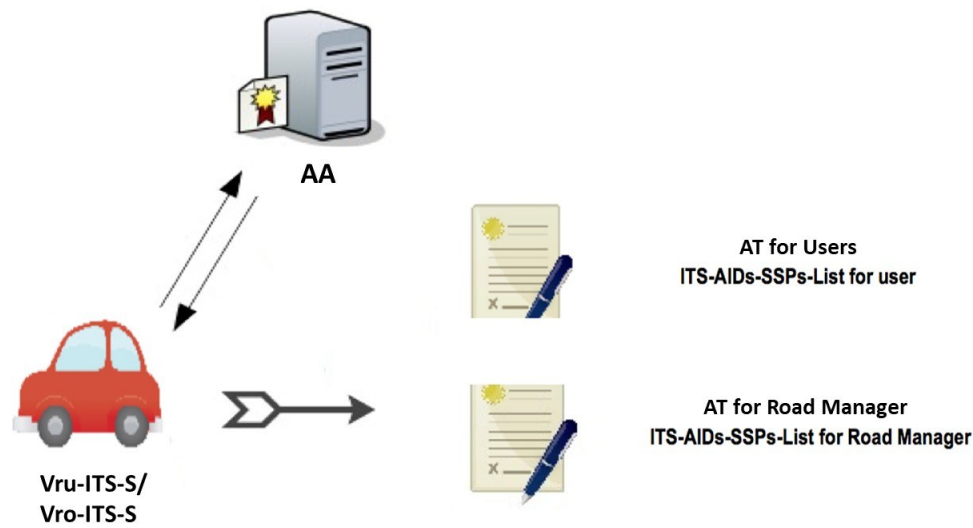


Figure 7 : AT Request/Response (Vru-ITS-S/Vro-ITS-S cases)

2.3.5 CRL download

2.3.5.1 Description

A CRL is requested by a ITS-Ss from the DC.

2.3.5.2 Pre-condition

- The ITS-S has the DC access point link.
- The DC contains the CRL correspondent to the RCA.
- The ITS-S has RCA certificate.

2.3.5.3 Flow diagram

An ITS-S sends a Get CRL request and receives a response from the DC. Figure 8 illustrates the procedure to get a CRL from the DC.

- **Step (1):** The ITS-S sends the Get CRL request to DC. The request is :
"http://dc_access_point/getcrl/HashedId8 "GET
http://dc_access_point/getcrl/HashedId8 " with the HashedID8 of the RCA
certificate signing the CRL.
- **Step (2):** The DC sends the response.
- **Step (3):** The ITS-S extracts the CRL from the response.

Figure 9 illustrates the case of CRL requests sent by an ITS-S through cellular technology.

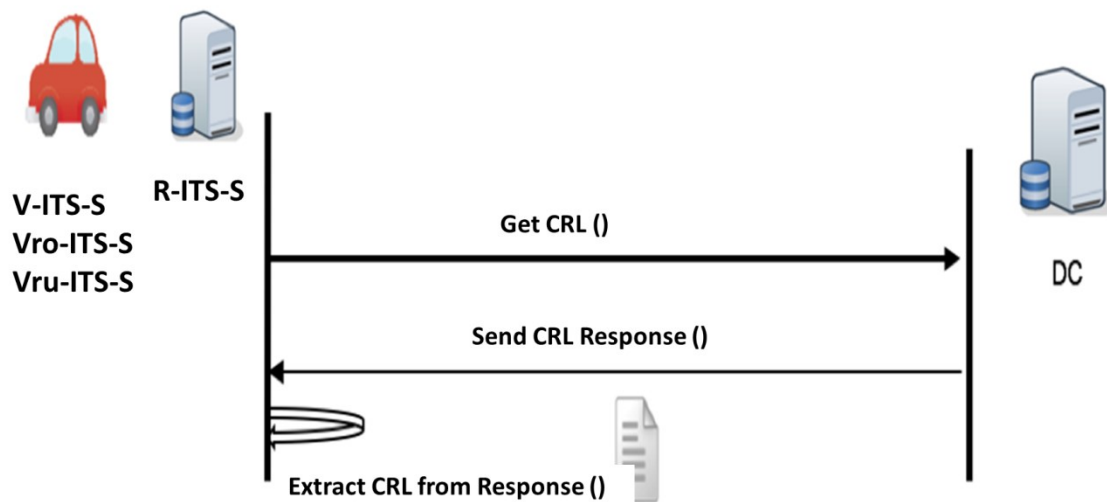


Figure 8 : CRL Download by R-ITS-S and V-ITS-S through cellular communication

2.3.5.4 Post-conditions

- The ITS-S has downloaded a CRL.

2.3.5.5 Potential requirements

- The ITS-S must verify that the CRL is signed by the RCA.

Id	2448M-CRLREQ-001 (2)
Component(s)	V-ITS-S, Vro-ITS-S or Vru-ITS and DC
Requirements and configuration	Each V-ITS-S, Vro-ITS-S or Vru-ITS-S has to download a CRL from the DC once per month in validation process and every week in production mode. A signature verification is mandatory before using the CRL.
Additional information	If the EC is expired, after requiring a new one, the ITS-S can download the most recent CRL

2.3.6 CTL download

2.3.6.1 Description

In order to update its internal list of trusted services (EA, AA, DC), an ITS-S needs a CTL.

2.3.6.2 Pre-conditions

- The ITS-S has DC access point link.
- The DC contains the CTL correspondent to the RCA.
- The ITS-S has an RCA certificate.

2.3.6.3 Service flows

As shown in Figure 9, the request/response cycle of the CTL can be summed up in three steps:

- **Step (1):** The ITS-S sends a Get CTL request to the DC. The request is : "GET http://dc_access_point/getctl/HashedId8/ctlSequence" with the HashedID8 of the RCA certificate signing the CTL.
- **Step (2):** The DC sends the CTL response.
- **Step (3):** The ITS-S extracts the CTL from the response.

An ITS-S sends CTL requests through cellular communication as illustrated in Figure 9.

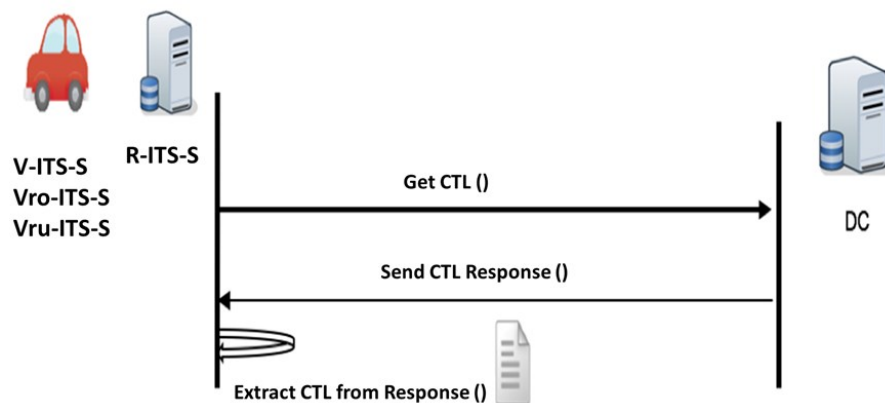


Figure 9 : : CTL Download by an ITS-S through cellular communication

2.3.6.4 Post-conditions

- The ITS-S has downloaded a CTL.

2.3.6.5 Potential requirements

- The ITS-S must verify that the CTL is signed by the RCA.

Id	2448M-CTLREQ-001 (2)
Component(s)	V-ITS-S, Vro-ITS-S or Vru-ITS-S and DC

Requirements configuration	and	Each V-ITS-S, Vro-ITS-S or Vru-ITS-S has download a CTL from the DC once per month for validation mode, and once per week for production.mode. A signature verification is mandatory before using the CTL.
Additional information		If the EC is expired, after requiring a new one, the ITS-S can download the most recent CTL

2.3.7 Message signature verification with CTL and CRL

2.3.7.1 Description

The present section describes the general process of the message's signature verification using CTL and CRL. It is recommended to verify the signature of a received message before forwarding it at the geonetworking level according to ETSI EN 302 636-4-1 V1.4.1 [20] section 10.3.3.

2.3.7.2 Pre-conditions

- The RCA certificate is provided to the ITS-S during the initialization phase.
- The RCA certificate, CTL and CRL are assumed to be valid.
- The CTL and CRL are available in the DC.
- The ITS-S shall verify that the CTL and the CRL are signed by RCA.
- For optimization reasons, the trust chain can be stored in a cache memory.

2.3.7.3 Procedure

- **Step (1):** The ITS-S receives a secured message and verifies the message signature with the associated AT certificate.
- **Step (2):** The ITS-S checks that HashID8 of AA certificate is not present in CRL.
- **Step (3):** The ITS-S verifies that the AA certificate is issued by C-Roads@F and InDiD RCA in case of French station
- **Step (4):** The ITS-S 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 CTL.

At every step of this procedure, if one of the verifications fails, then the signed message must be considered as invalid and must be rejected by the ITS-S. To identify its associated EA, the ITS-S can check the field "SubjectInfo.subject_name" of the EAs' certificates present in the CTL.

2.3.7.4 Post-conditions

The ITS-S verifies 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.

2.4 EC and AT certificates' management

This section deals with the main operational processes occurring in the PKI such as the ATs storage and change strategy. In order to protect the privacy of vehicle drivers, ITS-Ss have to change its ATs regularly.

2.4.1 ATs storage in ITS-Ss

An ITS-S (except Nfr-ITS-S) needs a reserve of ATs to be able to change frequently its pseudonym in respect to privacy requirements. The provisioned ATs are stored in a pool for a specific duration called TS (Time Slot) corresponding to their common validity period as shown in Figure 10

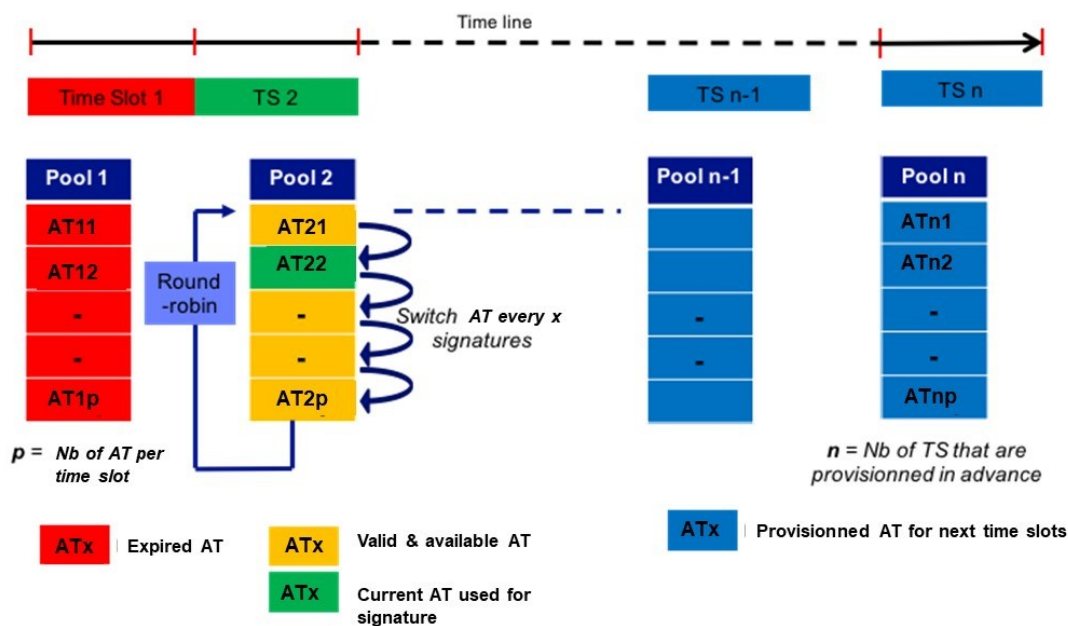


Figure 10 : ATs storage in an ITS-S

For example, the communication between ITS-Ss and a AA can be broken seldom the ITS stations should create multiple asymmetric key pairs locally, in advance and send them to the AA in order to retrieve corresponding ATs. Therefore, when a communication is established between the AA and the ITS-S, this latter must pre-load the required ATs for near future. We aim at the target that the ITS-S always obtained the required number of ATs within the fixed preloading period.

2.4.2 ATs change strategy

In order to protect the privacy of the road users, a regular change of AT (except Nfr-ITS-S) is required.

Id	2448M-CMGM-001 (2)
Component(s)	V-ITS-S, R-ITS-S

Requirements configuration and	For V-ITS-S and R-ITS-S, AT change should follow the following mechanism: Round Robin is the default strategy but it is not mandatory.
Additional information	Other strategies (like Random or randomized Round Robin) are accepted since there is no interoperability issue. The AT change Round Robin strategy is illustrated in Figure 10. The ITS-S selects a new AT from its pool based on a Round-Robin algorithm and so on until the expiration of period of validity of the ATs pool which is a Time Slot (TS) in our case.

Id	2448M-CMGM-002 (2)
Component(s)	Nfr-ITS-S
Requirements configuration and	Nfr-ITS-S shall not change its AT.
Additional information	Nfr-ITS-S can only change its AT if the latest is expired.

Id	2448M-CMGM-003 (2)
Component	V-ITS-S
Requirements configuration and	Applications shall be able to block the authorization ticket AT change if the ITS-S is stationary. In other cases, applications shall only be able to block it for at most pSecChangeBlockingMaxTime (See requirement RS_SEC_032 in [21]).
Additional information	Exception for all cases: • Validity of the authorization ticket expired • Collision of "Certificate digest" / "hashedId8.

Parameters for AT change and refill are provided in Table 2, in which the validity duration of certificate for validation will be referred to 2.5.4.7_M [11], and that for production will be referred to 2.5.4.15_M [15]

It is suggested to use 2 days as the validity duration of AT, for personal data protection purposes.

- For Pilot Validation PKI

Parameters	V-ITS-S or pedestrian	R-ITS-S	Nfr-ITS-S
Pseudonym max validity duration	1 week	1 week	1 week
Number of parallel Pseudonyms (issued to be valid in the same period)	10	10	1
Pseudonym max preloading period	6 months	6 months	3 months
Pseudonym change method (default method)	Round-Robin	Round-Robin	NA

Maximal pseudonym change	40000 signatures At each auto starter	6 Millions signatures	NA
AT duration overlapping	Recommended value: 1 hour	value: 24 hours	NA
pSecChangeBlockingMaxTime.	If supported, recommended value :5 mn		NA

- For Production PKI

Parameters	V-ITS-S or pedestrian	R-ITS-S	Nfr-ITS-S
Pseudonym max validity duration	1 week	1 week	1 week
Number of parallel Pseudonyms (issued to be valid in the same period)	100	2	1
Pseudonym max preloading period	3 months	3 months	3 months
Pseudonym change method (default method)	Round-Robin	Round-Robin	NA
Maximal pseudonym change	40000 signatures At each auto starter	6Millions signatures	NA
AT duration overlapping	Recommended value: 1 hour	value: 24 hours	NA
pSecChangeBlockingMaxTime.	recommended value :5 mn		NA

Table 2: ATs parameters.

Id	2448M-CMGM-004 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S
Requirements and configuration	A pool shall be used only if it is full. AT change follows a Round Robin strategy.
Additional information	

Id	2448M-CMGM-005 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S

Requirements and configuration	Preloaded ATs are valid for a period. This period should be configurable.
Additional information	

Id	2448M-CMGM-006 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S
Requirements and configuration	AT duration overlapping could be supported. Each partner can choose the value of this parameter.
Additional information	

Id	2448M-CMGM-007 (1)
Component	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S
Requirements and configuration	When all ATs within the pool expire, data transmission should be stopped.
Additional information	

Id	2448M-CMMGM-008 (2)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements and configuration	Addresses (MAC, IP/Geonet) and ATs change must not occur during communication sessions in particular for PKI requests, logs upload and DENM transmission. The path history must also be reset when the pseudonym changes.
Additional information	For the other messages (CAM, IVI, MAP, SPaT, POI, ETA) this requirement is not applied. If the change is done during the generation of DENM and CAM, there will be one for the DENM that does not change and one for the CAM that is the new AT.

Id	2448M-CMGM-009
Component(s)	Vro-ITS-S (Road operator)

Requirements configuration and	Road operator vehicles must renew their ATs after one hour (max).
Additional information	According to the requirements of the CNIL, an AT duration is one hour.

2.5 PKI requests errors handling

A C-ITS station shall not flood the PKI servers with continuous PKI requests (AT requests, EC requests, CRL requests and CTL requests).

To avoid PKI overload, all C-ITS stations shall implement a retry pattern with exponential back-off, regardless of the type of error received.

The retry pattern shall limit the amount of requests to a maximum of:

1 request every 1 second during the 3 minutes following the first error received
Then 1 request every 5 minutes during 1 hour
Then 1 request every 1 hour during 1 day
2 requests per day after

Id	2448M-PKIEH-009 (1)
Component(s)	PKI servers, V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS-S
Requirements configuration and	The retry pattern shall limit the amount of requests to a maximum of: 1 request every 1 second during the 3 minutes following the first error received Then 1 request every 5 minutes during 1 hour Then 1 request every 1 hour during 1 day 2 requests per day after
Additional information	

3. Security elements

This section is dedicated to the main elements involved in security functions as well as in security procedures and mechanisms. Security Data structures in the present document are defined using Abstract Syntax Notation 1 (ASN.1) and shall be encoded using the Canonical Octet Encoding Rules (COER) as defined in Recommendation ITU-T X.696 [9].

3.1 Canonical ID or UID

During initialization phase, the ITS-S station uses a unique identifier called Canonical ID (or UID (Unique Identifier)). Actor type and Actor are two fields composing the UID. The list of Actor types

and Actors participating in the projects are given in Annex 2. The format of the canonical ID (or UID) is described by Figure 11. It is composed of the following parts:

- Country Code (CC) – 2 bytes: it is a two-letter short code to define a country name based on the ISO 3166 standard, recommended as the general purpose code.
- Actor type (AT) – 2 bytes: it represents the different types of actors participating in the project.
- Actors (AC)- 4 bytes: it defines the name of each actor.
- Serial Number (SN) – 8 bytes: it is the serial number of the V2X on-board unit.

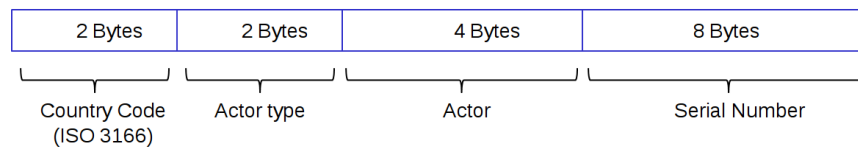


Figure 11 : Canonical ID (or UID)

In INDID project, the following codes are defined:

- CC= 'FR'
- AT= {'01': Road Operator, '02': Car manufacturer, '03': SNCF, '04': Transdev}
- AC is listed in Annex 2.

The UID format described in this section is adopted by all road operators and recommended to be used by the car manufacturers (i.e. Renault and PSA).

3.2 ITS-AIDs & Psid

In the deliverable 2.4.1.2_M Master, the ITS-AIDs (Application ID) for the different used messages (CAM, DENM,) are defined. The ITS-AID format is of type Integer (IntX as described in ETSI TS 103 097). Repository for Application IDs:

- Standardized ITS-AID values are listed in ETSI TS 102 965 v1.4.1.
- ETSI TS 102 965 V2.1.1 (2021-11) "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration," November 2018. _Psid is defined (see section 3.4) to replace ITS-AID but both fields are of type Integer and are equivalent.

3.3 Service Permissions (SSPs) & App permissions

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 and get AA) and during initialization phase. SSPs values can be found in Deliverable 2.4.1.2_M Master [10].

To be able to deliver ATs with required permissions (SSP), Certificate Authorities are also created with permissions (APP permissions and Cert Issue Permissions). These specific permissions are defined in 2.5.4.7_M[11].

3.4 Certificates

The certificates formats for CAs, Authorization Ticket (AT)s, ECs, TLM certificates used are defined in ETSI TS 103 097. Each ITS-S certificate is composed of several main fields and shall be of type ETSITS 103 097Certificate:

- Version: 3
- Type: the certificate's type is set to explicit
- Certificate issuer: self for the root CA certificate and sha256AndDigest or sha384AndDigest for the subordinate CA certificate AT and EC,
- To be signed content: contain several information about the issued certificate:
 - Certificate Id: the name of the authority issuing the certificate,
 - CRACId: set to 0x000000,
 - CRL Series: set to 0,
 - ValidityPeriod: containing the duration from the issuing time, generally in years,
 - Region (optional): not used,
 - Assurance level (optional): 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,
 - appPermissions: indicates permissions (Psid and SSP) of the Certificate Authority
 - certIssuePermissions (optional): indicates permissions (Psid and SSP) that the Certificate Authority is allowed to sign (in sub certificates),
 - certRequestPermissions (optional): not used,
 - canRequestRollover (optional): not used,
 - encryptionKey: encryption key of the CA,
 - verifyKeyIndicator: signature key indicator of the CA.
- Signature (NIST or Brain pool with 256 Bit = maximum 64 bytes): the certificate signature as proof of authentication.

Id	2448M-CERT-001 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS
Requirements and configuration	The certificates for ITS-Ss follow the structure defined in ETSI 103097
Additional information	

Id	2448M-CERT-002 (3)
Component(s)	V-ITS-S, Vro-ITS-S, Vru-ITS-S, R-ITS-S, Nfr-ITS
Requirements and configuration	The values of both assurance level and confidence level in ITS-S certificates shall be set to 0.
Additional information	

3.5 Certificate profiles

Depending on its use, each certificate includes specific information which could be different depending on the certificate profile. Regarding certificates authorities, there is a profile specific to each authority according to ETSI TS 103097. All details are provided in the deliverable 2.5.4.7_M [11].

3.6 Validity duration of certificates

According to the CP recommendations, the values of the validity duration of the used certificates are given in the deliverable 2.5.4.7_M [11].

3.7 Secured C-ITS messages

C-ITS messages are signed using authorization tickets ATs before being sent and exchanged between ITS-S. The signature will be computed with the private key associated to the verification public key included in the AT. Secured C-ITS messages are built in the Geonetwork layer and transmitted to the Security layer according to ETSI EN 302 636-4-1 v1.3.1.(clause 9.4).

3.7.1 Secured data structure format

The ETSI TS 103097 standard defines the security headers of the Secured Message structure.

Id	2448M-FORMAT-001
Component(s)	secure data structure
Requirements and configuration	A secure data structure shall be of type ETSI103 097 Data as defined in annex A in TS 103 097
Additional information	

Id	2448M-FORMAT-002 (2)
----	----------------------

Component(s)	secure data structure
Requirements and configuration	The option signedData, corresponding to the type SignedData as defined in ETSI TS 103 097 V2.1.1 section 5.2, shall be used to transfer a data structure with a signature. ECDSA signature shall be used as defined in IEEE Std 1609.2 [4] clauses 6.3.29, 6.3.29a and 5.3.1.
Additional information	All details are given in ETSI TS 103 097 section 5.2. More particularly, the generation time shall be used.

3.7.2 Security profile for C-ITS messages

Id	2448M-SECM-001(2)
Component(s)	ITS-S
Requirements and configuration	Messages are signed following the guidelines of the standard ETSI TS 103 097.
Additional information	

Id	2448M-SECM-002 (2)
Component(s)	ITS-S
Requirements and configuration	CAM is signed following the security profile for CAMs defined in TS 103 097 § 7.1.1"
Additional information	Two types of certificates are used: a hashed certificate or a complete certificate which is generally transmitted every second.

Id	2448M-SECM-003 (2)
Component(s)	ITS-S
Requirements and configuration	DENM is signed following the security profile for DENMs defined in TS 103 097 § 7.1.2.
Additional information	Complete certificates are used for signing DENMs.

Id	2448M-SECM-004 (2)
----	--------------------

Component(s)	ITS-S
Requirements and configuration	For IVI, MAP, SPaT, POI and ETA messages, see TS 103 097 § 7.1.3 to have more details on signature. Generic security is used with a Payload element of type signed only
Additional information	Complete certificates are used for signing IVI, MAP, SPaT, POI and ETA messages.

3.8 Signature verification algorithm

The receiver ITS-S checks the signature of the Secured Message. If the signature is valid the receiver ITS-S will process the C-ITS message, in all other cases, the receiver station will discard the message.

Id	2448M-VERI-001
Component(s)	ITS-S
Requirements and configuration	The verification algorithm shall follow the algorithm defined in C-roads TF1 deliverable [12], see annex B.
Additional information	

NIST and Brainpool curves can be used in signature and encryption algorithms. Different key sizes can also be used. During ASN.1 decoding of each received C-ITS message, we can know explicitly which kind of signature algorithm has been used. We can simply, during signature verification, decode the COER received packet part and extract the signature part which is a CHOICE structure composed of `ecdsaNistP256Signature`, `ecdsaBrainpoolP256r1Signature` or `ecdsaBrainpoolP384r1Signature`. In fact, the received C-ITS message follows `EtsiTs103097Data` structure derived from `leee16092Data` structure. We have `EtsiTs103097Data->content->signedData->signature`, and signature is encoded into one of the cited alternatives as defined in TS 103097.

4. MAC/IP/Geonetworking Address and Station ID change scheme

Each time the AT changes, the four following types of fields will change.

- Station ID,
- MAC address,
- IP address,
- Geonetworking address.

Id	2448M-ASIDC-001
----	-----------------

Component(s)	V-ITS-S
Requirements and configuration	Each time the AT changes, the four following types of fields will change. <ul style="list-style-type: none"> • Station ID, • MAC address, • IP address, • Geonetworking address
Additional information	

4.1 MAC address and StationID

The Figure 12 shows how to change Station ID and MAC address of ITS-Ss (V-ITS-Ss or R-ITS-Ss) based on the new value of the AT.

- **Station ID:** is set taking the first four bytes of HMAC-SHA256 [FIPS 198-1: The Keyed-Hash Message Authentication Code (HMAC)] computed using a nonce of 32 bytes and the new requested AT.
- **MAC Address:** is set taking the last six bytes of HMAC-SHA256 computed using a nonce of 32 bytes and the new requested AT. If the MAC address is used for unicast, the least significant bit of the first octet (Individual/Group(I/G) bit) must be set to 0 (bit number 8). If the MAC address is used for multicast/broadcast, the least significant bit of the first octet must be set to 1 (bit number 8). Note: Since the MAC address is changed from the Burned-In-Address (BIA) to an address that is locally setup, the 7th bit (the Universally or Locally(U/L) bit) must be set to 1.

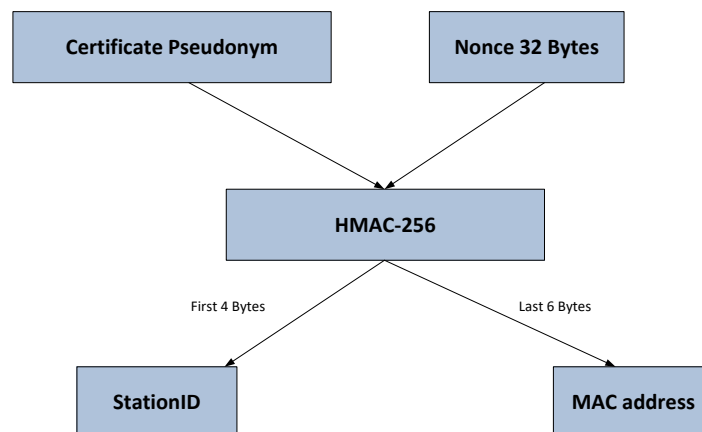


Figure 12 : Generation mechanism of StationID and MAC Address for a V-ITS-S

After MAC address and stationID generation, a collision avoidance control must be done. If the station generating the pair of MAC address and Station ID receives a message containing the same MAC address or/and StationID sent from another ITS-S, a new generation, using the same AT with a new Nonce, must be done (StationID, MAC Address, IP Address and GN Address should be re-

generated). The same derivations should be executed again. If two MAC addresses (associated to two access network interfaces) are needed, we follow the same derivation method using two distinct nonces without changing the AT. If all the AT pools expire, we generate a random MAC address to request new ATs.

4.2 IPv6 Address

For the IPv6 addressing, the interface ID (64 bits) is defined based on EUI-64 as defined in IETF RFC 4291, Appendix A. In fact, we follow two steps:

- Add FFFE after the first three bytes of the new MAC address generated (as explained in section 5.1).
- Invert the "u" bit (universal/local bit in IEEE EUI-64 terminology), which is the 7th bit.

Recall that IPv6 address of the R-ITS-S is sent to V-ITS-Ss through RA (router advertisement) messages. In this case there is no need to set this address statically in V-ITS-Ss.

4.3 Geonetworking Address

For the Geonetworking address, as defined in ETSI TS 102 636-4-1, the MID field should be changed whenever the AT changes. In fact, the MID representing the LL-ADDR (5th field, from Octet 2 to Octet 7) must be updated using the new generated MAC address (as described in section 5.1).

5. PKI Validation platform

5.1 Introduction

A validation platform is set in order to perform the integration and validation tests. These tests will be executed assuming that the AID/SSP pairs, assurance levels and ATs' validity periods to be adopted are predefined

5.2 CA Hierarchy

This part describes the Certification Authorities (CAs) hierarchy created for the French PKI validation platform. It describes the contents of the CAs certificates and the content of the Certificates Revocation List (CRL) and Certificate Trust List (CTL) issued by the RCA. The key pairs and certificates are generated during a key ceremony. The following chart in Figure 13 shows the certificates hierarchy of the PKI demo platform

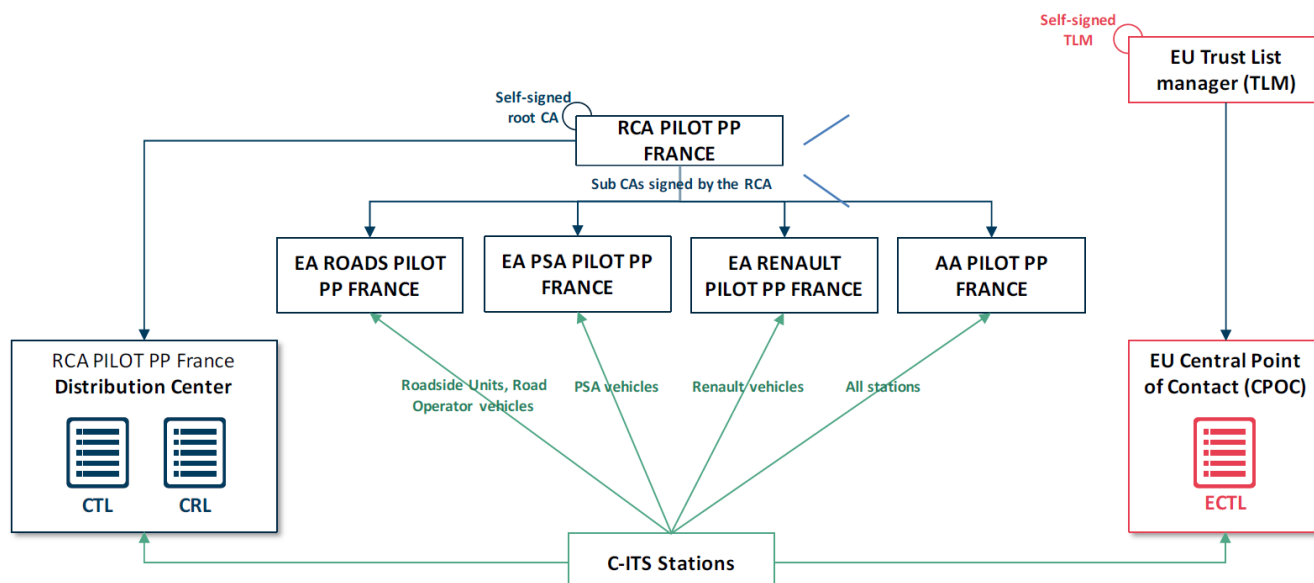


Figure 13 : CAs hierarchy overview

5.3 CA certificates details

Concerning the formats of different certificates authorities(Cas), a description is provided in the deliverable 2.5.4.7_M [11] for the validation, and deliverable 2.5.4.15_M [25] for the production. As for CTL and CRL formats, a description is provided in the deliverable 2.4.4.6 in the section 3.2.6 and 3.2.7.

5.4 ITS Station profiles

Profiles are defined to facilitate management of ITS Stations. Indeed, a profile is associated to an ITS-S during its registration process. This profile is mainly defined by the ITS-AID/SSP pairs as defined in sections 3.2 and 3.3 and it is represented in our platform by the following attributes illustrated in table 3. It is noteworthy that these AID/SSP pairs are defined in the AT.

Profile attributes		Format
Name	The profile is a unique identifier for each profile.	Text
ITS-AID/SSP pairs	The AID defines the scope of the applicability of the certificate while the SSP defines the permissions of the ITS-S.	Decimal/Hexadecimal
Assurance Level	The assurance level of the ITS-S described in [2.4.4.4] .	Decimal (between 0 and 7)
Confidence Level	The confidence level of the ITS-S described in [2.4.4.4].	Decimal (between 0 and 3)

Profile attributes		Format
Validity Period/Unit	It determines the validity period of the issued ATs and can be expressed in terms of seconds, minutes, hours or days.	Decimal
EC validity period	This value is the maximum limit for the validity period of EC certificates.	Decimal (in Seconds, Minutes, Hours, Days, Years)
AT validity period	This value is the maximum duration for the validity period of AT certificates.	Decimal (in Seconds, Minutes, Hours, Days, Years)
AT preloading period	This value is the validity period duration in which AT certificates can be requested from the date of request.	Decimal (in Seconds, Minutes, Hours, Days, Years)
Validity privacy policy	Encryption of EC signature in AT requests	Possible values are with or without encryption
Group	Name of the group that will use the profile.	Text

Table 3: Profile attributes.

Since the difference of the ITS-Ss types deployed in French C-ITS test, different profiles shall be defined for each one. Once profiles are defined, it is possible to start the registration of ITS-Ss. The ITS-Ss are represented by the following attributes illustrated in table 4.

ITS attributes		Format
Canonical ID	The canonical identity is a unique identifier for each ITS-S.	Text
Technical public key	A pair of technical key is generated by the ITS-S during bootstrap. The technical private key will be used to sign EC request. The technical public key is transmitted to the EA during the registering of the ITS-S to enable it to verify the signature of EC request received.	Hexadecimal SubjectPublicKeyInfo (X.509)
Profile	A profile should be associated to an ITS-S. It can be selected from a list provided in the HMI.	Text
Status	<p>Status must be selected during the registering of an ITS-S. Several statuses were for ITS Stations:</p> <ul style="list-style-type: none"> • Registered: An ITS-S is registered in internal database of EA. • Activated: ITS-S is activated once registered with the LTCA to be allowed to obtain authorization tickets. • Suspended: An ITS-S could be suspended for different reasons. This state doesn't allow ITS-S to request ECs. • Deactivated: In case of end life or following a compromise, ITS-S is deactivated. <p>It is recommended to choose the status "registered" although it is possible to choose another status.</p>	Text

Table 4: ITS-S attributes

The profiles creation and the ITS-Ss registration are performed via HMI. Standard default profiles are defined in 2.5.4.6_M specification [26].

5.5 Hosting

PKI Validation platform is hosted on IDnomic tenant in Orange cloud.

5.6 Access

Each component of the PKI has an access point: values are defined in 2.5.4.6_M specification [26].

6. Security elements for the Nfr-ITS-S

Specification of the National French ITS station (Nfr-ITS-S) is provided in deliverable 2.4.2.4_M[13]. For security concerns, the National French ITS-S may exchange with PKI servers to manage certificates, CRL and CTL. It may communicate with PKI servers to request its AT to be used to sign C-ITS messages or use a pre-installed certificate.

Id	2448M-SENF-001
Component(s)	Nfr-ITS-S
Requirements and configuration	The national French ITS-S is enrolled in the C-ITS trust domain as all other ITS-Ss, perform verification of messages and sign outgoing C-ITS messages.
Additional information	

Id	2448M-SENF-002 (2)
Component(s)	Nfr-ITS-S
Requirements and configuration	The communication between the Nfr-ITS-S and any V-ITS-S shall be secured by an IPSEC tunnel when IPv6 is used by the V-ITS-S
Additional information	

Id	2448M-SENF-003
Component(s)	Vro-ITS-S
Requirements and configuration	It is recommended to use TLS1.3 on Vro-ITS-S. No need to use an X509 certificate on the client Vro-ITS-S. However, the Nfr-ITS-S server must use an X509 certificate to be authenticated by the clients.
Additional information	

7. Security for hybrid communications

As described in deliverables 2.4.1_M [15], hybrid communication approach is used by combining ETSI ITS-G5 and 4G (LTE) communication technologies. Therefore, the V-ITS-S is able to communicate using simultaneously these two links when they are available. Security mechanisms needed to secure data transmission through the hybrid architecture defined in the deliverable 2.4.1_M are described below. Hybrid communication (ITS-G5 and LTE) is provided to carry C-ITS messages from different senders to different receivers. The communication architecture that supports the data messages transmission is complex and can be mostly divided in two sub-architectures:

- a sub-architecture with a Home Agent
- a sub-architecture with a Relay platform (named a car manufacturer platform).

Mobility management is then supported or not. An important part of the burden is the mobility management signalling and the re-encapsulation (tunnelling) of the IP packets in the case of architectures providing seamless mobility.

To securely deploy C-ITS use cases within the considered projects, we will provide:

- end-to-end data security fulfilling security requirements in terms of integrity, confidentiality, authentication and privacy.
- IP mobility signaling security in respect of authentication, integrity and privacy.
- end-to-end PKI interaction security in terms of integrity, confidentiality, authentication and privacy.

We assume that all exchanged C-ITS messages (CAM, DENM, ..) are secured and trusted following the agreed ETSI security standard (see details in section 3) and all PKI requests are secured following the agreed ETSI security standard (see section 2). In the following sections, we define a security solution to be applied for these two kinds of architectures. Security requirements related to the different architectures are defined below.

7.1 General requirement

Id	2448M-GENERAL-001
Component(s)	ITS-S
Requirement	IPsec with VPN or TLS with a X509 certificate should be used to secure transport of C-ITS messages.
Additional information	The C-ITS message between V-ITS-S and Nfr-ITS-S can be standard C-ITS message, or a proxy can be inserted between V-ITS and Nfr-ITS-S, while the connection between V-ITS-S and the proxy is protected by secured web socket, and the connection between the proxy and Nfr-ITS-S is simply web socket.

7.2 Architecture with a Home Agent in case of using IPv6

This architecture makes it possible to have a seamless connection switching between IP/802.11p and cellular access networks. It involves a Home Agent in charge of masking the mobility of the vehicle to the network. Figure 14 illustrates this architecture where C-ITS messages (CAM and DENM messages) are sent to the National Central ITS-S Nfr-ITS-S. These messages are then translated into Datex II messages and transmitted to the relevant Platform. For information, the home agent is added to the architecture only when IPv6 is used on the Vru-ITS-S otherwise the



TLS1.3 is used.

Figure 14 : Architecture with Home Agent (Uplink Communication)

The interfaces cited below are defined in 2.4.1_M [15]

Id	2448M-ARHA-001 (2)
Component(s)	Vru-ITS-S, Home Agent, interfaces 1,2
Requirement	<ul style="list-style-type: none"> ✓ IPsec (Transport Mode) shall be used to secure signaling messages (See section 6.1 RFC 4877) only when IPv6 is used on the Vru-ITS-S otherwise see ARHA-002 (2) ✓ IPsec configuration shall use IKE (with pre-shared keys) and ESP. ✓ For IPsec Group/IKE_SA_INIT exchange, the following algorithms shall be supported: <ul style="list-style-type: none"> ➤ Confidentiality: ENCR_AES_CBC with 128-bit key length; ➤ Pseudo-random function: PRF_HMAC_SHA2_256; ➤ Integrity: AUTH_HMAC_SHA256_128; ➤ Diffie-Hellman group 19 (256-bit random ECP group) ;
Additional information	It is recommended to use IKEv2, see Recommendation R8 [16].

Id	2448M-ARHA-004 (3)
Component(s)	Vru-ITS-S, interfaces 1,2
Requirement	✓ A Web socket shall be used to send DENM or CAM messages signed in GeoNet Layer following the ETSI TS 103 097.
Additional information	<ul style="list-style-type: none"> ✓ It is recommended to use WebSocket over an encrypted TLS 1.3 with X509 certificate. It is recommended to use mutual authentication¹. ✓ For TLS version 1.3 use, see cipher suites recommended by ANSSI[17], section A page 45 (tables A.1 and A.2) and annex C for the list of ANSSI recommendations for TLS use. ✓ For X509, see section 3.1 [18] for attributes configuration

Id	2448M-ARHA-003 (3)
Component(s)	Nfr-ITS-S, PFro , Interface 11, Interface 4, Interface 5
Requirement	The communication between Nfr-ITS-S and the PFro is secured through TLS1.3. A X509 certificate shall be used to protect transport of DatexII messages. Mutual authentication shall be used.
Additional information	

Id	2448M-ARHA-004 (2)
Component(s)	Interface 1, Interface 2, Interface 4, Interface 5, Interface 11
Requirement	For downlink communications, C-ITS messages can be sent from the PFro to the V-ITS-S following the same path through the Nfr-ITS-S and R-ITS-S
Additional information	

7.3 Architecture with a Car Manufacturer Platform

To illustrate our defined security solution, we consider the architecture described in **Figure 15** where C-ITS messages (DENM messages) are sent to the Car Manufacturer Platform which forwards them to the National Central ITS-S Nfr-ITS-S. DENM messages are then translated into Datex II messages and transmitted to the local Platform PFro.

¹ Mutual authentication: Mutual authentication or two-way authentication refers to two parties authenticating each other.

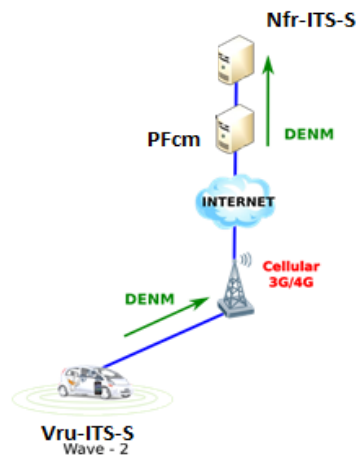


Figure 15 : Architecture with a PFcm (uplink communication)

Id	2448M-ARCM-001 (2)
Component(s)	Vru-ITS-S, Car Manufacturer Platform, interface 3
Requirements	DENM messages shall be signed in Geonet Layer following the ETSI TS 103 097. Signed DENM messages are transmitted to the Car Manufacturer Platform
Additional information	
Id	2448M-ARCM-002 (2)
Component(s)	Car Manufacturer Platform, Nfr-ITS-S, interface 4
Requirement	AMQP protocol shall be used. TLSv1.3 with a X509 certificate shall be used to protect transport of signed DENM messages and authenticate the Nfr-ITS-S
Additional information	

Id	2448M-ARCM-003 (1)
Component(s)	Interface-3, Interface 4
Requirement	For downlink communications, TLSv1.3 with a X509 certificate shall be used to protect transport of signed DENM messages and authenticate the Nfr-ITS-S.
Additional information	

7.4 Architecture supporting V2V communication through cellular network

The security solution for V2V communication shall be a combination of the proposed solutions presented in previous sections. Figure 16 illustrates the V2V communication using cellular technology.

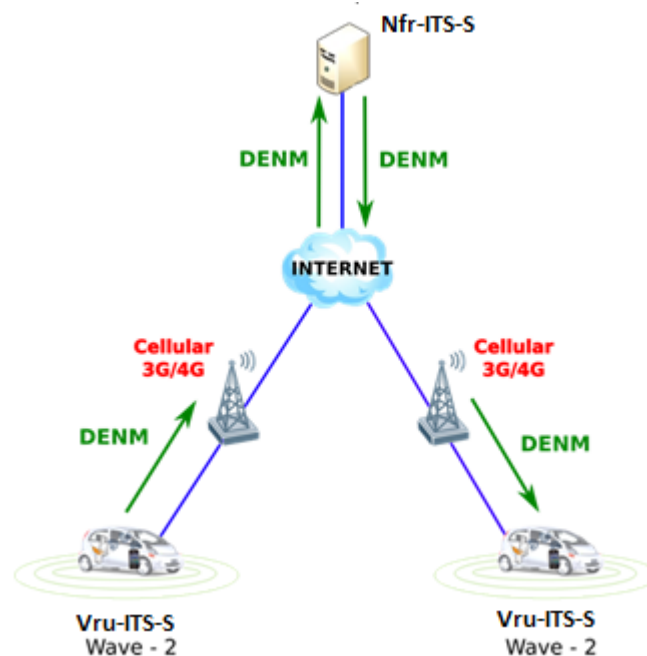


Figure 16 : V2V-communication using cellular technology

Id	2448M-V2VC-001 (2)
Component(s)	V-ITS-S, Nfr-ITS-S, Home Agent, PfcM
Requirement	The security solution for V2V communication with a cellular technology combination of the proposed solutions presented in sections 7.2 and 7.3 . The requirements shall be also supported.
Additional information	

7.5 Architecture for road operators

As described in 2.4.1_M [15] and 2.4.1.5 [18] deliverables, road operators can use two architectures: one architecture based on using a direct link between Vro-ITS-Ss and the Nfr-ITS-S or using a home agent. IPsec with VPN (using IPv4 or IPv6) or TLS with a X509 certificate shall be used to protect transport of C-ITS messages. The management of X509 certificates handled in the defined TLS connections is supported by the security policy of each road operator.

The security solution to support uplink communication is given below, and downlink communication is similar to the case of uplink communication

Id	2448M-ARRO-002 (2)
Component(s)	Vro-ITS-S, Home Agent, interfaces 6,7
Requirement	<ul style="list-style-type: none"> ✓ IPsec (Transport Mode) shall be used to secure signaling messages (See section 6.1 RFC 4877) ✓ IPsec configuration shall use IKE-2 (with pre-shared keys) and ESP for phase 1. ✓ IPsec configuration shall use IKE-2 (with X509 certificates) and ESP for phase 2. ✓ For IPsec Group/IKE_SA_INIT exchange, the following algorithms shall be supported: <ul style="list-style-type: none"> ➤ Confidentiality: ENCR_AES_CBC with 128-bit key length; ➤ Pseudo-random function: PRF_HMAC_SHA2_256; ➤ Integrity: AUTH_HMAC_SHA256_128; ➤ Diffie-Hellman group 19 (256-bit random ECP group) ;
Additional information	It is recommended to use IKEv2, see recommendation R8 [16]

7.6 GLOSA architecture

For GLOSA architecture using SPATEM/MAPEM messages (see Figure 17), TLS with a X509 certificate shall be used to protect transport of C-ITS messages between R-ITS-S and Nfr-ITS-S stations. Data transmission between Nfr-ITS-S and V-ITS-S shall be secured using IPsec with VPN or TLS with a X509 certificate.

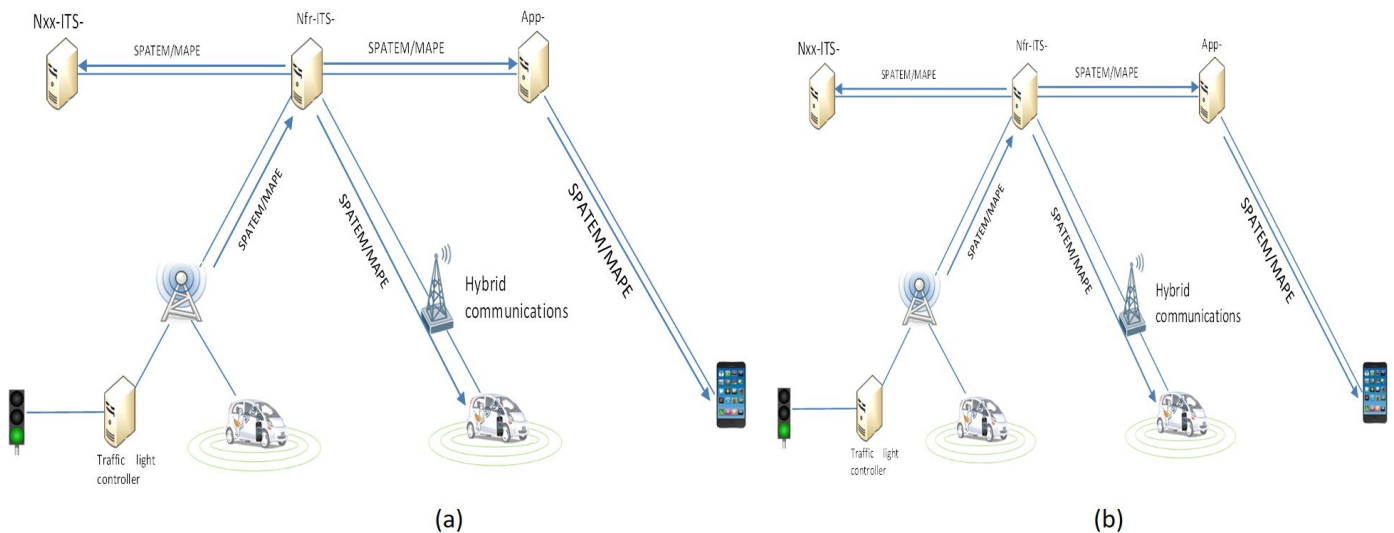


Figure 17 : GLOSA architectures ((a): with local traffic light controller, (b): with centralized traffic light controller)

7.7 Smartphone application

Security details for the smartphone application with its ecosystem are given in Deliverable 2.4.5.1.

7.8 P2V use case

Security details for the device P2V application are given in Deliverable 2.4.1.5_H.

8. Security elements for BI

The interface called Basic Interface is an IP-based interface between back-office systems, to support the exchange of the information between back-entities required to support the services via hybrid communications. The specification of this interface for hybrid communication is given in C-Roads deliverable [14]. The back-office is represented by the National French ITS Station. AMQP protocol is used as a communication protocol. In order to support end-to-end security for the deployed services, the security objectives for each data path transmission should be clearly defined including:

- Path 1: the path from sending vehicle to our National French Nfr-ITS-S.
- Path 2: the path along BI between our home National French Nfr-ITS-S and foreign Serving back_end entity.
- Path 3: the path from foreign Serving back-end entity to the Receiving vehicle in our home network.

The following tables provide security details to secure data transfer between our National French Nfr-ITS-S and foreign back-entities.

Id	2448M-BI-001 (1)
Component(s)	Nfr-ITS-S
Requirement	For validation, Nfr-ITS-S shall be configured to follow the tables in 8.
Additional information	

Id	2448M-BI-002
Component(s)	ITS-S
Requirement	The SecuredMessage structure of a data signed message is put into the AMQPv1.0 Message body
Additional information	

9. IPv6

A V-ITS-S can communicate directly with each other and with R-ITS-S using IPv6. In order to communicate with other stations using IPv6 protocol, an ITSS-V needs an IPv6 address, which can be obtained manually or automatically via:

- Statefull configuration via a DHCPv6 server
- Stateless auto configuration.

Auto-configuration of addresses with local scope (link-local addresses) [27] is done on every interface of ITS stations:

- Generating a link-local address,
- Performing duplicate address detection

On an ITSS-V, auto-configuration of addresses of global scope can be done on each interface by:

- Determining the prefix(es) for the link
- Generating one or more global addresses via stateless auto-configuration,
- Attempting duplicated address detection.

In IP networks, a host generates link local addresses when a communication interface is enabled. They are only used for communicating with stations (hosts and routers) attached to the same local link.

Stateless Address Auto-configuration (SLAAC) allows nodes to auto-configure their interfaces using a local interface identifier and the prefixes advertised by the routers. Thus, this auto-configuration is made for each router (prefix advertised). SLAAC is based on Neighbor Discovery Protocol (NDP) [2]. Address duplication procedure is used to ensure that all configured addresses (auto-configured or obtained via DHCPv6) are likely to be unique on a given link.

To allow the use of IPv6, V-ITS-Ss are configured to discover the global prefix announced by the infrastructure (R-ITS-S) and to identify the default router they need to configure their IPv6 communication interfaces.

The routers are implemented inside the R-ITS-S. A Router can generate a link-local address and perform Duplicate Address Detection on all addresses prior to assigning them to one of its interface.

Neighbor Discovery (NDP) is the protocol used by the V-ITS-S to configure its local link address and the global unicast IPv6 address. V-ITS-Ss have to build a global unicast IPv6 address to access to the Internet when the service is provided by the infrastructure (R-ITS-S).

A Router Solicitation message is sent by the host (V-ITS-S) when an interface is enabled to request routers for a Router Advertisement instead of waiting for an unsolicited one. Each ITSS-R shall send a Router Advertisement each 2 seconds.

Id	2448M-IPv6-001
Component(s)	ITSS-R

Requirement	Each ITSS-R shall send a Router Advertisement each 2 seconds.
Additional information	

A Router Advertisement message is periodically sent by routers (R-ITSS-S) to:

- Advertise their presence
- Indicate the parameters of the link and Internet
- Give information to configure the address.

A Neighbor Solicitation message is send by a node (V-ITSS-S or R-ITSS-S) to:

- Determine the link layer address of a neighbor,
- Verify that a neighbor is reachable,
- Detect duplicate addresses.

A Neighbor Advertisement message is sent as a response to Neighbor Solicitation message.

As general requirements, all the ITS Stations shall implement and support the requirements set by the "IPv6 Node Requirements" [29], which includes NDP and SLAAC. All the ITS Stations must also comply with the RFC 4861 [28].

Id	2448M-IPv6-002
Component(s)	ITS-S
Requirement	all the ITS Stations shall implement and support the requirements set by the "IPv6 Node Requirements" [29]. All the ITS Stations must also comply with the RFC 4861 [28].
Additional information	

SENDING BI messages

	CAM	DENM	IVI	SPAT
--	-----	------	-----	------

	(incl. SRM)	(incl. RWW)		(GLOSA)/ MAP
Message type in scope?	yes	yes	yes	no
Security properties				
1. SIGN on Geonet layer: Whose certificate/signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	Yes (A Web socket shall be used to send signed DENM or CAM to the French National ITS station.) ○ Vehicle	yes ○ Vehicle ○ Nfr-ITS-S	○ R-ITS-S ○ Nfr-ITS-S	
2. SIGN on Facility layer: Whose certificate/signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	no	no	no	
3. NO message signature	no	no	no	

RECEIVING BI messages

	CAM (incl. SRM)	DENM (incl. RWW)	IVI	SPAT (GLOSA)/ MAP
Message type in scope?	yes	yes	yes	no
Security properties				
11. SIGNED on Geonet layer: Certificate validation? Which certificate/signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	yes (accept message) yes (validate certificate) ○ Vehicle ○ R-ITS-S ○ Nfr-ITS-S	yes (accept message) yes (validate certificate) ○ Vehicle ○ R-ITS-S ○ Nfr-ITS-S	yes (accept message) yes (validate certificate) ○ R-ITS-S ○ Nfr-ITS-S	
12. SIGNED on Facility layer: Certificate validation? Which certificate/signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	no (accept message) no (validate certificate)	no (accept message) no (validate certificate)	no (accept message) no (validate certificate)	
13. NO message signature	no	no	no	
Comments/ Specifications:				

Securing BI connection

	CAM (incl. SRM)	DENM (incl. RWW)	IVI	SPAT
--	--------------------	---------------------	-----	------

				(GLOSA)/ MAP
Protocol AMQP v1.0	yes	yes	yes	no
14. Authorization/service access control - Supported ? - Which mechanism ?	yes Defined in [1] and [2]	yes Defined in [1] and [2]	yes Defined in [1] and [2]	
15. Authentication - Server-to-server mutual authentication - Transport-layer security (TLS 1.3 (RFC 2546) with X509 certificates - SASL [RFC4422] Simple Authentication and Security Layer	yes yes no	yes yes no	yes yes no	
16. Data message integrity	yes	yes	yes	
Comments/ Specifications:				

10. Bibliography

- [1]. ETSI TS 103097 V1.4.1, ITS Security-Security header and certificate formats, 10/2020.
- [2]. ETSI TS 102941 V1.4.1: ITS Security - Trust and Privacy Management, 01/2021.
- [3]. "EU CP, Certificate Policy," [Online]. Available: https://transport.ec.europa.eu/system/files/2018-05/c-its_certificate_policy-v1.1.pdf
- [4]. IEEE Std 1609.2™-2016, "IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages – Amendment 1" 01/2016.
- [5]. ETSI TS 102731 V1.1.1, Security; Security Services and Architecture, 10/2010.
- [6]. ETSI 102940 V1.3.1, ITS communications security architecture and security management, 04/2018.
- [7]. ETSI EN 302665 V1.1.1, Communications Architecture, 09/2010.
- [8]. Certificate Policy (ANNEX 3 to the Commission Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems) – March 2019 Draft available at https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-2592333_en#isc-2018-08207
- [9]. Recommendation ITU-T X.696 | ISO/IEC 8825-7, Information technology - ASN.1 encoding rules: Specification of Octet Encoding Rules (OER)
- [10]. 2.4.1.2_M Master , Common technical specifications for use cases – Master document.
- [11]. 2.5.4.7_M, Pilot valisation PKI- Naming Document.
- [12]. C-Roads_TF1_C-ITS_Security_Requirements_and_Specifications_2.0.5
- [13]. 2.4.2.4_H, LTE/ITS-G5 hybrid architecture – French National Central ITS Station specifications.
- [14]. C-Roads TF4 deliverable, Specification for interoperability of backend hybrid C-ITS communication, version 1.6.1, 12/02/2020.
- [15]. 2.4.1_M, Functional and technical hybrid architecture- common specifications.
- [16]. IKEv2 R8, Agence nationale de la sécurité des systèmes d'information , Note technique: Recommandations de sécurité relatives à IPsec pour la protection des flux réseau, https://www.ssi.gouv.fr/uploads/2012/09/NT_IPsec.pdf.
- [17]. TLS 1.2/1.3, ANSSI, Recommandations de sécurité relatives à TLS, <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls>.
- [18]. X509, ANSSI, Recommandations de sécurité relatives à TLS, <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls>.
- [19]. IPsec R16, Agence nationale de la sécurité des systèmes d'information, Technica Report Recommendations for securing networks with IPsec, https://www.ssi.gouv.fr/uploads/2015/09/NT_IPsec_EN.pdf
- [20]. ETSI EN 302 636-4-1 V1.4.1, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality, 01/2020
- [21]. C-Roads: C-ITS Security Requirements & Specifications, v1.8.0.sc, 1.Dec 2020
- [22]. C-ITS Point of Contact (CPOC) Protocol, Annex: EU CCMS Levels & Requirements, Draft v8.0, July 2021,

https://collab.algoe.fr/DATAS/modFile/6329/6149/6155/6177/10157/15046/63140_1625644267.docx

- [23]. 2.4.1.1_M_Master_V2X, Master technical specifications for V2X use cases
- [24]. "EU SP, Security Policy," [Online]. Available:
https://collab.algoe.fr/ViewerJS/#../DATAS/modFile/6329/6149/6155/6176/8576/8579/8843/30417_1558440746.pdf.
- [25]. 2.5.4.15_M, Production L1 PKI - Naming Document
- [26]. 2.5.4.6_M, Pilot Validation PKI: Configuration Manual
- [27]. Rajiv Asati and Hemant Singh and Wes Beebee and Carlos Pignataro and Eli Dart and Wesley George. Enhanced Duplicate Address Detection. RFC 7527, 2015.
- [28]. Narten, T., et al. "Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (draft standard). Internet Engineering Task Force, 2020-01-21
- [29]. Tim Chown and John A. Loughney and Timothy Winters. IPv6 Node Requirements (RFC 8504), Internet Engineering Task Force, Jan 2019.

11. Annexes

11.1 Annex 1: Association Table

Previous acronym	New acronym
LTC	EC
PC	AT
LTCA	EA
PCA	AA
TSL	CTL

11.2 Annex 2: List of actors

Full name of the actor	Actor code (AC)	Actor type (AT)
DIR Ile de France	DRIF	01
DIR Atlantique	DIRA	01
DIR Ouest	DIRO	01
Département de l'Isère	LD38	01
Conseil Départemental des Côtes d'Armor	CD22	01
Conseil Départemental d'Ile est Vilaine	CD35	01
Saint Briec Agglomération	StBA	01
Région Bretagne	RBZH	01
SANEF	SANF	01
RENAULT	RENA	02
PSA	PSA	02
DIR Nord	DIRN	01
DIR Est	DIRE	01
DIR Centre-Est	DRCE	01
DIR Sud-Ouest	DRSO	01
DIR Centre-Ouest	DRCO	01
DIR Méditerranée	DRMD	01
DIR Nord-Ouest	DRNO	01
DIR Massif Central	DRMC	01
APRR	APRR	01
VINCI Autoroutes	VINC	01
AREA	APRR	01
Autoroutes du Sud de la France (ASF)	VASF	01
Cofiroute	VCOF	01
Escota	VESC	01
Syndicat Mixte des Transports en Commun de la Région Grenobloise (SMTc)	SMTc	01
Grenoble Alpes Métropole (METRO)	GAME	01
Metropole Aix Marseille Provence (MAMP)	MAMP	01
Bordeaux Metropole	BDMe	01
Eurométropole de Strasbourg (EMS)	EMS	01
Transdev	TDG	04
SNCF	SNCF	03

11.3 Annex 3: PKI main parameters

Parameters	For Pilot Validation PKI	For Production PKI
Home RCA-CRL update frequency	CRL is only modified and published if it has been modified or if it has expired.	<=3 months
Home RCA-CTL update frequency	CRL is only modified and published if it has been modified or if it has expired.	
ECTL update frequency for ITS-S		<=3 months
CRL update frequency for ITS-S	1 month	1 week
CTL update frequency for ITS-S	1 month	1 week
EC max validity duration	5 years	3 years
EA certificate validity duration	5 years	5 years
AA certificate validity duration	5 years	5 years
RCA certificate validity duration	5 years	5 years
Home RCA-CRL validity duration	5 years	4 months
Home RCA-CTL validity duration	5 years	5 years
TLM certificate validity duration	4 years	4 years