



French C-ITS Deployment Coordination committee

SCOOP@F Security Integration Guide

Deliverable 2.4.4.8_H

Activity 2: Studies

Sub Activity 2.4 > Specifications

Version 4.00

Publication Date: 14/11/2019



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

The contents of this publication are the sole responsibility of the SCOOP@F project consortium, C-ROADS France project consortium and InterCor project consortium (French beneficiaries only) and do not necessarily reflect the opinion of the European Union.

Information on the document

Document: SCOOP@F Security Integration Guide

Date of publication: 14/11/2019

Responsible Entity: Houda LABIOD, Telecom Paris

Participants: IDNomic, IMT-Atlantique

Status: Version 4.00 – Release 4

Publication history

Date	Version	Author(s)	Updates & changes	Diffusion
14/11/2019	4.00	Telecom Paris	Consolidated version for release 4	Release 4

Input documents

Reference	Title	Version & Date	Origin
2.4.4.8	SCOOP Security System: Integration Guide	Version 7.0 16/10/2017	SCOOP@F release 2 wave 1
2.4.2.4_H	LTE/ITS-G5 hybrid architecture – French National Central ITS Station specifications	Version 0.18 16/11/2018	SCOOP@F wave 2
2.4.4.11_H	Hybrid end-to-end security: Specifications	Version 0.12 06/08/2018	SCOOP@F wave 2
2.4.1_H	Functional and technical hybrid architecture- common specifications	Version 0.30 20/12/2108	SCOOP@F wave 2
2.4.1.2_H Master	Common technical specifications for use cases – Master document	Version 1.0 17/12/2018	SCOOP@F wave 2
InterCor M4	Milestone 4- Common set of upgraded specifications for hybrid communications – Specifications for IF2 for hybrid communications	Version 2.1 Final Draft	InterCor

Table of Contents

Information on the document.....	2
Input documents.....	2
Table of Contents.....	3
List of Figures.....	4
1. Deliverable's purpose	6
2. Presentation.....	7
2.1 SCOOP@F PKI System description	7
3. Security elements	9
3.1 ITS-AIDs.....	9
3.2 Specific Service Permissions (SSPs).....	9
3.3 Certificates	9
3.4 Secured Messages.....	9
3.5 Requirements.....	10
4. Security elements for the Nfr-ITS-S	11
5. Security for hybrid communications	12
5.2 Architecture with a Car Manufacturer Platform	13
5.3 Architecture for road operators	14
6. Security elements for IF2	15
7. PKI Validation platform.....	17
8. Bibliography	18

List of Figures

Figure 1: PKI System Architecture	8
Figure 2 : Structure of CAM secured message	10

GLOSSARY

Term/abbreviation	Definition
C-ITS	Cooperative Intelligent Transport Systems
CA	Certificate Authority
CP	Certificate Policy
CRL	Certificate Revocation List
DC	Distribution Centre
ITS-AID	ITS Applications ID
ITS-S	ITS Station
LTC	Long-Term Certificate
LTCA	Long-Term Certificate Authority
Nfr-ITS-S	National French ITS-S
PC	Pseudonym Certificate
PCA	Pseudonym Certificate Authority
RCA	Root Certificate Authority
SSP	Specific service permissions
TSL	Trusted Service List

1. Deliverable's purpose

This deliverable aims at giving all necessary details about the security system used to secure data messages transmission using hybrid communications for SCOOP@F wave 2, InterCor and C-Roads projects.

2. Presentation

For simplicity, in this deliverable, when the acronym V-ITS-S is used alone, it represents the ITS-S associated to all kinds of SCOOP vehicles (V-ITS-S for manufacturer vehicles, V-ITS-S and V-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 when it represents both V-ITS-S and R-ITS-S.

2.1 SCOOP@F 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), the presence of a trusted third-party as a certificate authority is required. To do so, 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.

SCOOP@F PKI system manages the following elements:

- **Long Term Certificate (LTC):** gives its holder (ITS-Ss) the right to request PCs.
- **Pseudonym Certificate (PC):** gives its holder (ITS-Ss) the right to perform specific actions.
- **Certificate Revocation List (CRL):** is a list digitally signed by a CA that contains certificates identities that are no longer valid.
- **Trusted Service List (TSL):** is a signed list which contains trusted RCAs, LTCAs and PCAs certificates and PKI service access points. This list is updated frequently.

The SCOOP@F PKI core system consists of four main entities 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 LTCAs and PCAs (creation, security requirements authorizing the issuance of certificates to ITS-Ss).
- **Long Term Certificate Authority (LTCA):** is a security management entity responsible for the issuance of LTC and the validation of PCs as well as the management of the ITS-Ss (registration, status update, permissions...). It operates in an online mode.
- **Pseudonym Certificate Authority (PCA):** is a security management entity responsible for the delivery, the monitoring and the use of PCs. It operates in an online mode.
- **Distribution Centre (DC):** provides the ITS-Ss with the updated trust information such as TSL and CRL necessary to assure that received information is coming from legitimate and authorized ITS-Ss or PKI certification authority.

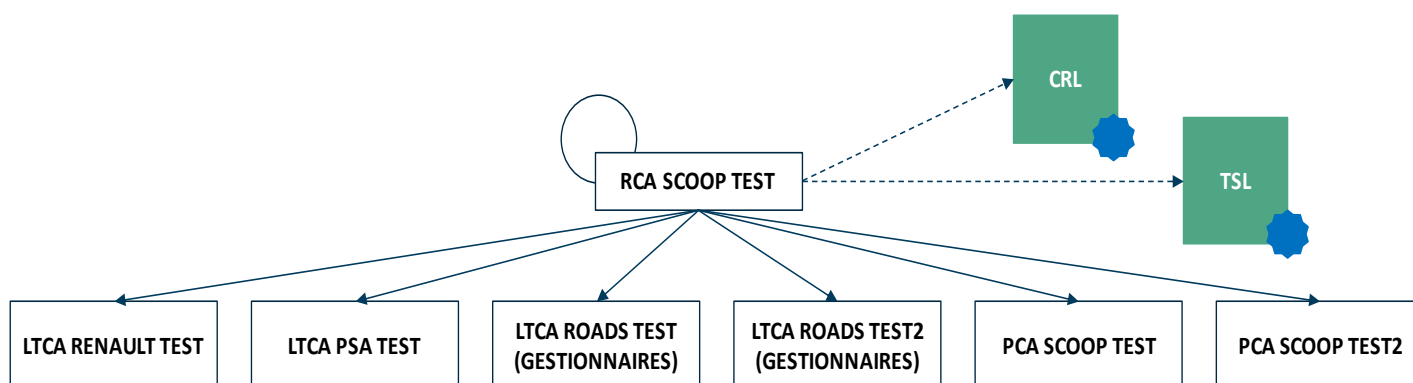


Figure 1: PKI System Architecture

We have the following CAs:

- 1 RCA SCOOP TEST
- 4 LTCAs: 1 LTCA Renault TEST, 1 LTCA PSA TEST and 2 LTCAs for Road Operators
- 2 PCAs: 1 PCA SCOOP TEST and 1 PCA SCOOP TEST2

Different cryptographic algorithms are used. Among, the Elliptic Curve Digital Signature Algorithm (ECDSA) which is used for the signature of messages (CAM, DENM, CAM-I, SPaT, MAP, IVI, POI and ETA) with keys of size 32/64 bytes (with or without compression). Besides, encryption algorithms include:

- Elliptic Curve Integrated Encryption Scheme (ECIES) [ref IEEE Std 1363a™-2004] with keys of size 32 bytes with compression and 64 bytes without compression.
- Advanced Encryption Standard (AES) with CCM (CBC+CTR) mode with keys of size 16 bytes.

• Communication with PKI servers

Similarly to the approach used for SCOOP@F wave 1 project, the communication protocol with PKI remains the same based on http connection as defined in the SCOOP@F wave 1 deliverables 2.4.4.6 [1] and 2.4.4.8 [2].

3. Security elements

This section is dedicated to the main elements involved in security functions as well as in security procedures and mechanisms.

3.1 ITS-AIDs

In the deliverable 2.4.1.2_H Master, the ITS-AIDs (Application ID) for the different used messages (CAM, DENM, CAM-I, SPaT, MAP, IVI, POI, ETA) are defined.

The ITS-AID format is of type IntX (as described in ETSI TS 103 097 v1.2.1). Some ITS-AID values can be found at URL in ETSI TS 102 965 V1.4.1.

3.2 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 LTC and get PC) and during initialization phase.

SSPs values can be found in Deliverable 2.4.1.2_H Master [3].

3.3 Certificates

The certificates for ITS-S stations follow the structure defined in ETSI 103097 v1.2.1 .

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

The field 'Subject_attributes' contains the following subfields: assuranceLevel, confidenceLevel, its_aid_ssp_list, serviceSpecificPermissions.

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).

We set the values of both assurance level and confidence level in V-ITS-S/R and Nfr-ITS-S certificates to 0.

Pseudonym change strategy for V-ITS-S and R-ITS-S is the same as defined in SCOOP@F wave 1 and is available in deliverable 2.4.4.8 [2]. For Nfr-ITS-S, there is no need to change the pseudonym certificate.

3.4 Secured Messages

All messages 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.

The figure 16 illustrates the structure of a CAM secured message. The signature is applied on header field, payload field and on specific subfields of the trailer field. The payload of the secured message on the figure shows, for simplification, only the CAM data payload but it should contain the Geonet layer headers (GN Common Header, Extended Header), the BTP layer header, and the content of the CAM message.

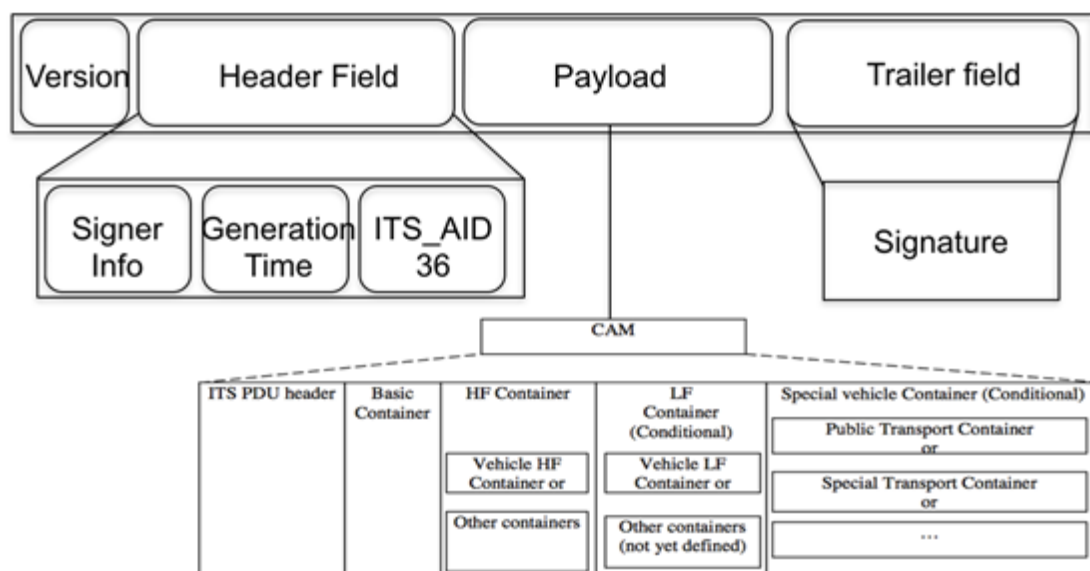


Figure 2 : Structure of CAM secured message

CAM is signed using a complete certificate every second otherwise a hashed certificate is included. For more details, see TS 103 097 v1.2.1 § 7.1". The complete certificate is maintained only for one second.

Similar approach is used to generate secured message for DENM but only complete certificates are used for signature. The same procedure is applied for IVI, MAP, SPaT, POI and ETA messages.

3.5 Requirements

Addresses (MAC, IP/Geonet) and pseudonym certificates change must not occur during communication sessions in particular for PKI requests, logs upload and DENM.

The path history must also be reset when the pseudonym changes.

4. 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_H[4].

For security concerns, the National French ITS-S may exchange with PKI servers to manage certificates, CRL and TSL. The national French ITS-S is enrolled in the ITS trust domain as all other ITS-Ss, perform verification of messages and sign outgoing ITS messages. It may communicate with PKI servers to request its pseudonym certificate to be used to sign ITS messages or use a pre-installed certificate.

The Nfr-ITS-S is also involved in communication through IF2 [5, see section 5]. The Nfr-ITS-S has several certificates:

- A certificate which follows the structure defined in ETSI 103097 v1.2.1. This certificate is used to sign the used ITS messages.
- X509 certificates shall be used:
 - to protect data transmission between V-ITS-S and the national French ITS-S.
 - to protect transmission of Datex II messages between the Nfr-ITS-S and the local platform.
 - to secure the IF2 connections involved in each communication with the foreign countries (Netherlands, United Kingdom, Belgium, Spain, Portugal, Austria).

5. Security for hybrid communications

As described in deliverables 2.4.1_H [6] and 2.4.4.11_H [7], 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_H are described.

The 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 and a sub-architecture with a Relay platform (named a car manufacturer platform). We define a security solution to be applied for these two architectures.

5.1 Architecture with a Home Agent

Id	24411H-ARHA-001
Component(s)	Vru-ITS-S, Home Agent
Requirements and configuration	<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 (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) ❑ For IPSec, follow recommendations R16 [8]
Additional information	It is recommended to use IKEv2, see recommendation R8 [9].

Id	24411H-ARHA-002
Component(s)	Vru-ITS-S, Nfr-ITS-S
Requirements and configuration	<ul style="list-style-type: none"> ✓ A Web socket shall be used to send DENM or CAM signed in GeoNet Layer following the ETSI TS 103 097 v1.2.1. ✓ TLS with X509 certificate shall be used to protect data transmission. Mutual authentication shall be used. ✓ TLS version 1.2 ✓ Cipher suites recommended by ANSSI for TLS 1.2 [10], see section A page 45 (tables A.1 and A.2)

	<ul style="list-style-type: none"> ✓ Annex C for the list of ANSSI recommendations for TLS use. ✓ X509, see section 3.1 [11] for attributes configuration
Additional information	

Id	24411H-ARHA-003
Component(s)	Nfr-ITS-S, PFro
Requirements and configuration	<ul style="list-style-type: none"> ➤ TLS with a X509 certificate shall be used to protect transport of Datex II messages. Mutual authentication shall be used.
Additional information	

5.2 Architecture with a Car Manufacturer Platform

To illustrate our defined security solution, we consider the architecture described in deliverable 2.4.1_H [6] where data messages (DENM messages) are sent to the Car Manufacturer Platform PFcm which forwards them to the Nfr-ITS-S. DENM messages are then translated into Datex II messages and transmitted to the Local Platform.

Id	24411H-ARCMP-002
Component(s)	Vru-ITS-S, PFcm
Requirements and configuration	DENM messages shall be signed in Geonet Layer following the ETSI TS 103 097 v1.2.1. Signed DENM messages shall be transmitted to the Car Manufacturer's Platform
Additional information	

Id	24411H-ARCMP-002
Component(s)	PFcm, Nfr-ITS-S
Requirement	<ul style="list-style-type: none"> ➤ AMQP protocol shall be used. ➤ TLS with a X509 certificate shall be used to protect transport of signed DENM messages.
Additional information	

Id	24411H-ARCMP-003
Component(s)	Nfr-ITS-S, PFro
Requirement	<ul style="list-style-type: none"> ➤ TLS with a X509 certificate shall be used to protect transport of Datex II messages.
Additional information	

5.3 Architecture for road operators

To complete when a validated version of deliverable 2.4.1_H is available.

The management of X509 certificates handled in the defined TLS connections is supported by the security policy of each road operator.

6. Security elements for IF2

The second interface (called IF2) is an interface between back-office systems, to support the exchange of the information between back-offices required to support the services via cellular communications. The specification of this interface for hybrid communication is given in InterCor M4 deliverable [5]. In InterCoR only ETSI TS 103 079 v1.2.1 will be used.

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 InterCor services, we have to define clearly the security objectives for each data path transmission including:

- Path 1: the path from sending vehicle in to our National French ITS-S.
- Path 2: the path along IF2 between our home National French ITS-S and foreign Back_office.
- Path 3: the path from foreign Back-Office to the Receiving vehicle in our home network.

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

SENDING IF2 messages

	CAM (incl. SRM)	DENM (incl. RWW)	IVI	SPAT (GLOSA)/ MAP
Message type in scope?	y	y	y	n
<i>Security properties</i>				
1. SIGN on Geonet layer: Whose certificate/ signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	y o Vehicle	y o Vehicle o Nfr-ITS-S	o R-ITS-S o Nfr-ITS-S	
2. SIGN on Facility layer: Whose certificat/ signature? ❖ Vehicle ❖ R-ITS-S ❖ Nfr-ITS-S	n	n	n	
3. NO message signature	N	N	n	
Comments/ Specifications:	<p>A Web socket shall be used to send signed DENM or CAM to the French National ITS station. The SecuredMessage structure of a data signed message is put into the AMQP Message body.</p> <p>TLS with a X509 certificate shall be used to protect data transmission.</p> <p>IPsec (Transport Mode) shall be used to secure signaling messages.</p> <p>IPsec configuration shall use IKE (with pre-</p>			

	shared keys) and ESP.			
--	-----------------------	--	--	--

RECEIVING IF2 messages

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

Securing IF2 connection

	CAM (incl. SRM)	DENM (incl. RWW)	IVI	SPAT (GLOSA)/ MAP
Protocol AMQP ?	y	y	y	n
14. Authorization/service access control - Supported? - Which mechanism?	y Defined	y Defined	y Defined	
15. Authentication - Server-to-server mutual authentication - Transport-layer security (TLS (RFC 2546) with X509 certificates - SASL [RFC4422] Simple Authentication and Security Layer	y y n	y y n	y y n	
16. Data message integrity	y	y	y	
Comments/ Specifications:				

7. PKI Validation platform

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 PCs' validity periods to be adopted are predefined.

All the details related to the PKI validation platform are available in deliverable 2.5.4.7_H.

8. Bibliography

- [1] 2.4.4.6, PKI architecture and technical specifications, Release 2, May 2017.
- [2] 2.4.4.8, SCOOP Security System: Integration Guide,SCOOP@F release 2 wave 1, 16/10/2017.
- [3] 2.4.1.2_H Master, Common technical specifications for use cases – Master document, version 1.0, 17/12/2018.
- [4] 2.4.2.4_H, LTE/ITS-G5 hybrid architecture – French National Central ITS Station specifications, version 0.18, 16/11/2018.
- [5] InterCor M4, Milestone 4- Common set of upgraded specifications for hybrid communications – Specifications for IF2 for hybrid communications, version 2.1, Final Draft.
- [6] 2.4.1_H, Functional and technical hybrid architecture- common specifications, version 0.30 20/12/2108.
- [7] 2.4.4.11_H, Hybrid end-to-end security: Specifications, version 0.12, 06/08/2018.
- [8] 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
- [9] 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.
- [10] TLS 1.2, ANSSI, Recommandations de sécurité relatives à TLS, <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls>.
- [11] X509, ANSSI, Recommandations de sécurité relatives à TLS, <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls>.