



French C-ITS Deployment Coordination committee

Hybrid end-to-end security: Specification

Deliverable 2.4.4.11_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: Hybrid end-to-end security: Specification

Date of publication: 14/11/2019

Responsible, Entity: Houda LABIOD – Telecom Paris

Status: Version 4.00 – Released

Distribution

Date	Version	Author(s)	Updates & changes	Diffusion
14/11/2019	V4.00	TPT	<ul style="list-style-type: none">Consolidated version for release 4 wave 2	Release

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 & abbreviations

BTP	Basic Transport Protocol
C2C-CC	Car2Car communications Consortium
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
DCC	Decentralised Congestion Control
DENM	Decentralized Environmental Notification Message
DP	DCC profile
DPID	DCC profile identifier
DSRC	Dedicated Short Range Communications
GBC	Geo Broadcast
GN	Geo Networking
GPS	Global Positioning System
HST	Header Sub-Type
HT	Header Type
ITS	Intelligent Transport Systems
IVI	Infrastructure to Vehicle Information
IVIM	Infrastructure to Vehicle Information Message
LT	Lifetime
MAP	Geometric information for the intersection
MAPEM	MAP (topology) Extended Message
MHP	Maximum Hop limit
NH	Next Hop
R-ITS-S	Roadside ITS Station (RSU in the French Terminology)
RSP	Wi-Fi ITS-G5 Roadside System Profile (short also Roadside System Profile)
RWW	Roadworks Warning
s	Seconds
SCF	Store Carry Forward
SHB	Single-Hop Broadcast
SPAT	Signal Phase and Timing
SPATEM	Signal Phase and Timing Extended Message
TC	Traffic class
TCC	Traffic Control Centre
ITS-G5	<p>ITS-G5 is a European standard for ad-hoc short-range communication of vehicles among each other (V2V) and with Road ITS Stations (V2I). ITS-G5 refers to the approved amendment of the IEEE 802.11 (standard IEEE 802.11p). This technology (possibly others) uses the 5.9 GHz frequency band to support safety- and non-safety ITS applications.</p> <p>In this document ITS-G5 stands for IEEE802.11p/ETSI ITS-G5.</p>
N/A	Not Applicable
TBC	To Be Checked, with MS or associated partner

Table of Contents

Scope 7

1.	Introduction	8
2.	SCOOP@F2 Global Hybrid Architecture.....	8
2.1	Architecture with a Home Agent.....	9
2.2	Architecture with a Relay Platform	11
3.	SCOOP@F2 PKI Model.....	13
4.	Bibliography	14

List of figures

Figure 1: SCOOP@F2 Global Hybrid Architecture	8
Figure 2: Architecture with a Home Agent (Uplink Communication)	9
Figure 3: Architecture with a Relay (uplink communication)	11
Figure 4: SCOOP@F2 validation PKI Architecture Model	13

Scope

This deliverable gives all necessary details about the security mechanisms used to secure data messages transmission using hybrid communications (ITS-G5 and LTE) for SCOOP@F2, InterCor and C-Roads projects.

1. Introduction

In SCOOP@F2, as described in the deliverable 2.4.1_H, we use the hybrid communication approach by combining ETSI ITS-G5 and 4G (LTE) communication technologies. Therefore, the ITSS-V is able to communicate using simultaneously these two links when they are available.

This deliverable identifies the security mechanisms needed to secure data transmission through the hybrid architecture defined in the deliverable 2.4.1_H. IP and end-to-end security specification is provided.

An important part of the burden is the mobility management signaling and the re-encapsulation (tunneling) of the IP packets. These messages need to be protected to avoid an attacker to tamper and divert the packets while the ITSS-V visits foreign networks. The main security objectives ensured via these specifications are: confidentiality, integrity and authentication.

Therefore, this deliverable studies security mechanisms for:

- Data link technologies (ITS-G5 and LTE),
- Mobility management signaling,
- and end-to-end data traffic transmission.

The deliverable is composed of three sections. In the Section 2, we review briefly the global hybrid communication architecture. Then, we give the security specification details for two sub-architectures derived for the main global one.

In section 3, we address the PKI model as well as security communication with the PKI.

2. SCOOP@F2 Global Hybrid Architecture

As defined in the deliverable 2.4.1_H, the SCOOP@F2 architecture consists of several components as shown in Figure 1 (ITSS-V, ITSS-R, eNoedB, National C-ITSS, Local C-ITSS, Home Agent, PKI servers, etc.).

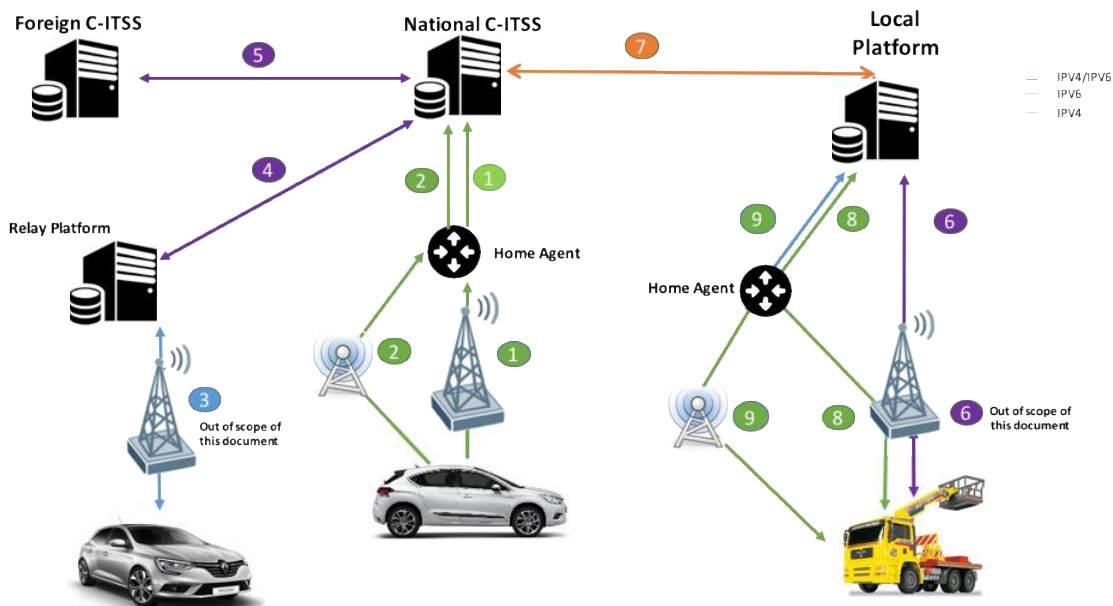


Figure 1: SCOOP@F2 Global Hybrid Architecture

Hybrid communication (ITS-G5 and LTE) is provided to carry data messages from different senders to different receivers. 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. In this deliverable, we will present the security solution to be applied for these two architectures.

The main security objectives ensured via our specifications are: Confidentiality, Integrity and Authentication.

To securely deploy SCOOP@F2 use cases, we will provide:

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

2.1 Architecture with a Home Agent

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.

To illustrate our defined security solution, we consider the architecture described in figure 2 where data messages (CAM and DENM messages) are sent to the National Central ITSS. These messages are then translated into Datex II messages and transmitted to the Local Platform.

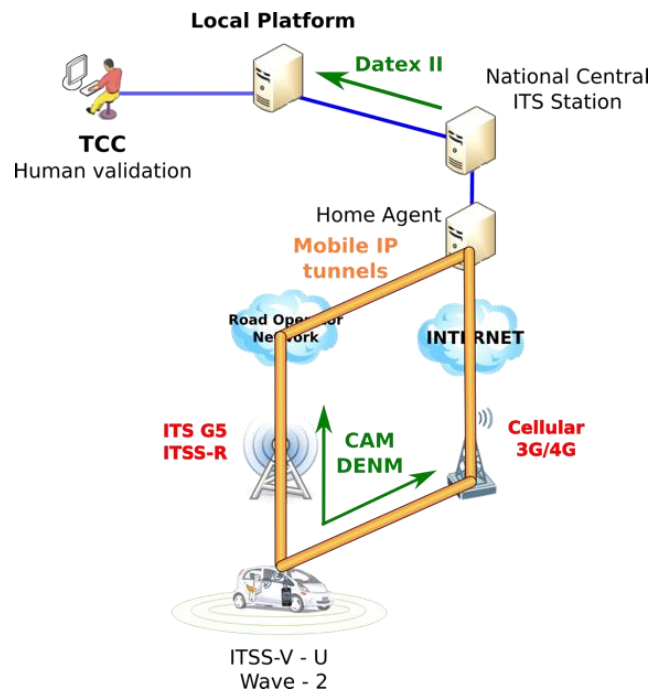


Figure 2: Architecture with a Home Agent (Uplink Communication)

Id	24411H-ARCH-001
Component(s)	Vru-ITS-S, HA
Requirement	<p>IPsec (Transport Mode) shall be used to secure signaling messages (See section 6.1 RFC 4877)</p> <p>IPsec configuration shall use IKE (with pre-shared keys) and ESP.</p> <p>For IPsec Group/IKE_SA_INIT exchange, the following algorithms shall be supported:</p> <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) ;
Acceptance	
Additional information	It is recommended to use IKEv2.

Id	24411H-ARCH-002
Component(s)	Vru-ITS-S, Nfr-ITS-S
Requirement	<p>A Web socket shall be used to send DENM or CAM messages signed in GeoNet Layer following the ETSI TS 103 097 v1.2.1.</p> <p>TLS with X509 certificate shall be used to protect data transmission</p>
Acceptance	
Additional information	

Id	24411H-ARCH-003
Component(s)	Nfr-ITS-S, PFro
Requirement	TLS with a X509 certificate shall be used to protect transport of DatexII messages.
Acceptance	
Additional information	

For downlink communications, Datex II can be sent from the local platform to the ITSS-V following the same path through the National central ITSS. The same security mechanisms as used for the uplink communications are applied. IVI and DENM messages are signed by the National central ITSS and sent to the ITSS-V.

2.2 Architecture with a Relay Platform

To illustrate our defined security solution, we consider the architecture described in figure 3 where data messages (DENM messages) are sent to the Relay Platform which forwards them to the National Central ITSS. DENM messages are then translated into Datex II messages and transmitted to the Local Platform.

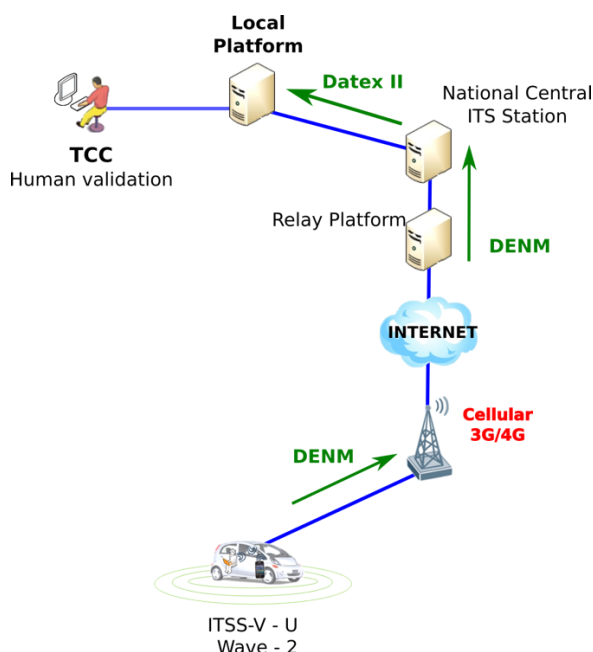


Figure 3: Architecture with a Relay (uplink communication)

Id	24411H-ARCH-007
Component(s)	Vru-ITS-S, PFcm
Requirement	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 Relay Platform
Acceptance	
Additional information	

Id	24411H-ARCH-008
Component(s)	PFcm, Nfr-ITS-S
Requirement	AMQP protocol shall be used. TLS with a X509 certificate shall be used to protect transport of signed DENM messages.
Acceptance	
Additional information	

Id	24411H-ARCH-009
Component(s)	National Central ITS Station, Local Platform
Requirement	TLS with a X509 certificate shall be used to protect transport of DatexII messages.
Acceptance	
Additional information	

For downlink communications, IVI and DENM messages can be sent from the local platform to the ITS following the same path through the National central ITSS and a Relay Platform. The same security mechanism as used for the uplink communications are applied. IVI and DENM messages are signed by the National central ITSS and sent to the Relay Platform which forwards them to the ITSS-V.

3. SCOOP@F2 PKI Model

SCOOP@F2 considers new C-ITS messages. The validation PKI architecture will be updated by:

- ✓ Adding a new PCA' supporting new ITS-AIDs for new messages (SPaT, MAP, IVI, POI). In fact we will keep SCOOP@F1 PCA and we will add a new PCA.
- ✓ Adding a new LTCA' for Road operators supporting new ITS-AIDs Application Object Identifier) for new messages (SPaT, MAP, IVI, POI). In fact we will keep SCOOP@F1 LTCA and we will add a new LTCA for Road Operators.
- ✓ The new certificates of new authorities will be added to the new SCOOP@F2 TSL.

All indicated modifications concern only the SCOOP@F2 validation PKI. The update of validation PKI implies the new registration of only Road operators ITSSs and the update of SCOOP@F2 TSL for all ITSSs.

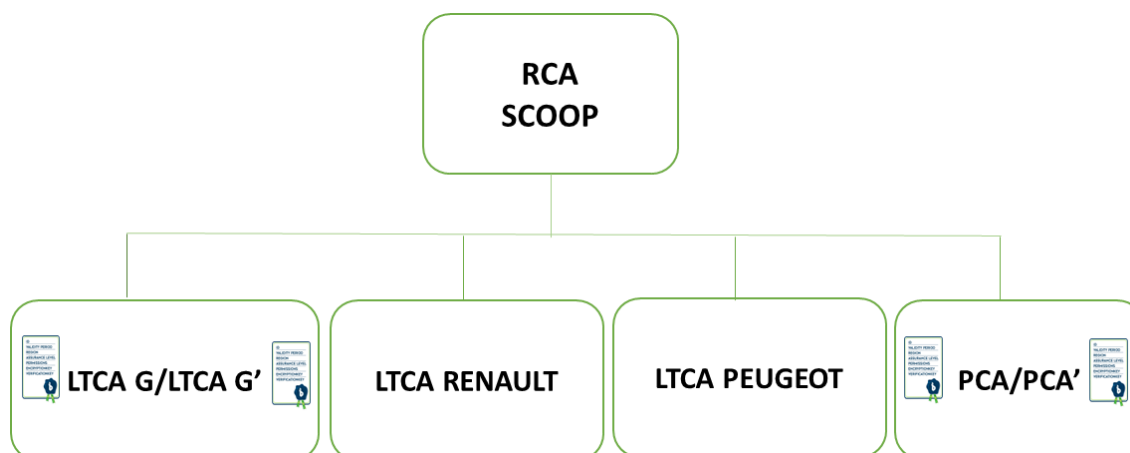


Figure 4: SCOOP@F2 validation PKI Architecture Model

• Communication with PKI servers

Similarly to the approach used for SCOOP@F1 project, communication protocol with PKI remains the same based on http connection as defined in the SCOOP@F1 deliverables 2446 and 2448.

4. Bibliography

- [1] Perkins, Charles, David Johnson, and Jari Arkko. *Mobility support in IPv6* RFC 6275. 2011.
- [2] Wakikawa, R., et al. Multiple care-of addresses registration, RFC 5648 (2009).
- [3] Tsirtsis, G., et al. "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support RFC 6089.(2011).
- [4] Devarapalli, Vijay, et al. *Network mobility (NEMO) basic support protocol*. RFC 3963. 2004.
- [5] Soliman, Hesham. "Mobile IPv6 support for dual stack hosts and routers." RFC 5555 2009.
- [6] Devarapalli, Vijay, and Francis Dupont. "Mobile IPv6 operation with IKEv2 and the revised IPsec architecture." RFC 4877 2007.
- [7] Deliverable 2.4.1.6 v 2.0: IPv6 Addressing over G5,
- [8] ANSSI, Recommendations for Securing networks with IPsec, DAT-NT-003-EN/ANSSI/SDE/NP
- [9] Conta, A. (1998). Generic packet tunneling in IPv6 specification. RFC 2473. 1998
- [10] McGrew, David, and Paul Hoffman. "Cryptographic algorithm implementation requirements and usage guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)." (2014).
- [11] Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296, 2014.
- [12] Internet Key Exchange Protocol Version 1 (IKEv1), RFC 2409, 1998.