Securing messages in C-ITS: a proof of concept

Jun Zhang, Houda Labiod, Ghassen Chaabane
INFRES
Télécom Paris, IP PARIS
Palaiseau, France
{jun.zhang,houda.labiod,ghassen.chaabane}@telecom-paris.fr

Clément Ruffin, André-Perpey
NeoGLS
Martillac, France
{clement.ruffin,andre.perpey}@neogls.com

Abstract—**Today's vehicles and traffic infrastructures are becoming more and more connected, using technologies to enable users to utilize transport networks more safely and efficiently. Cooperative Intelligent Transport Systems (C-ITS) describe a domain where smart vehicles and infrastructures can inter-act and share data directly with each other. The need for a way to establish trust and preserve the integrity of the system is evident. In this paper, we present a proof-of-concept of securing messages between communicating entities in C-ITS based on the European ETSI TS 103 097 standards in the c-roads project.**

Index Terms—**C-ITS, security, PKI**

I. Secured C-ITS architecture

The c-roads project [1] aims to deploy C-ITS in European countries to improve traffic safety and efficiency. As shown in Fig. 1, the secured PKI(Public key infrastructure)-based C-ITS in the c-roads project contains 4 main entities:

- Root CA (RCA): it defines common policies to all subordinate CAs. It delivers certificates for Long-Term CAs (LTCAs) and Pseudonym CAs (PCAs). It Periodically produces a revocation list of LTCA and PCA certificates and defines a list of trusted services to introduce new RCAs, PCAs. The Root CA is required when a new LTCA or PCA shall be created, or when the lifetime of LTCA or PCA certificate expires.
- Long term certificate authority (LTCA): The LTCA issues for each vehicle a long-term certificate (LTC) called also enrollment certificate (EC). LTCs are used to identify and authenticate vehicles with the PKI system. They should not be used for external communications of vehicles.
- Pseudonym CA (PCA): The PCA issues for each vehicle one or more pseudonymous certificates (PCs) called also Authorization tickets (AT). Pseudonymous certificates are used for all external communications of vehicles and must be renewed frequently for reasons of protection of users' privacy.
- Distribution center (DC): Distribution Center provides ITS-S the updated trust information necessary for performing the validation process to control that received information is coming from a legitimate and authorized ITS-S or PKI certification authority.

The European standard ETSI TS 103 097 specifies the secure data structure including header and certificate formats for Intelligent Transport Systems, including security profiles for Cooperative Awareness Messages (CAMs), Decentralized Environmental Notification Messages (DENMs), and general messages, and certificates like Root CA certificates, Trust List Manager certificates, Enrollment credentials, Authorization tickets, Subordinate certification authority certificates like enrolment and authorization authorities certificates. The implementation of ETSI TS 103 097 V1.2.1 [2] is already available in commercial products from companies such as NeoGLS. Nevertheless, the implementation of last version of ETSI TS 103 097, V1.3.1 [3] has not been widely tested yet.

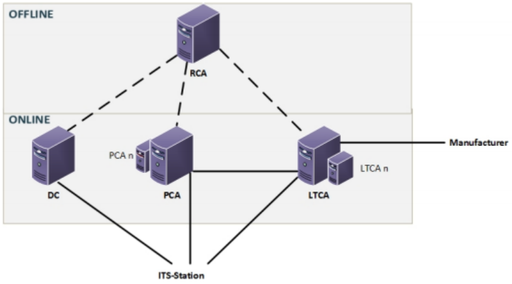


Fig. 1. High level PKI architecture for C-ITS

II. Proof-of-concept of ETSI TS 103 097 V1.2.1

We verify the message securing mechanism according to ETSI TS 103 097 V1.2.1 [2] by the testbed composed by two OBUs (on borad units), and one RSU (Road side unit) from NoeGLS, as shown in Fig. 2.

The devices have build-in sim cards, so that they can always access to the Internet. With the interface as shown in Fig. 3, we can enable/disable PKI, and select the LTCA, PCA and DC for the device, and enable/disable security options.

We test the security mechanism between two communicating devices (OBU vs RSU, or OBU vs. OBU), according to the scenarios specified in Table I. The objective of tests is to see whether a valid message will be rejected falsely, or an invalid message will be received falsely. If any case above case happens, it indicates the failure of the implementation of ETSI TS 103 097 V1.2.1.

Annex to ISBN 978-3-903176-28-7© 2020 IFIP.

This work is supported by the EU project C-Roads (Connected Roads) co-financed by the connecting Europe facility of the European Union.

The result of the testing shows that, when the securing mechanism is enabled at the receiver side, only the signed message from the sender that uses the same PKI server can be received; otherwise, the receiver accepts all the incoming messages. This reflects that the implementation of ETSI TS 103 097 V1.2.1 in NeoGLS works well.

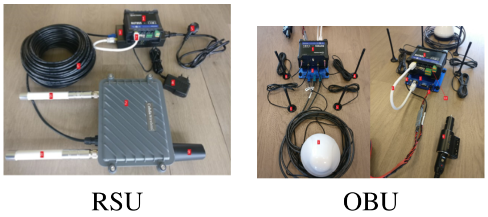
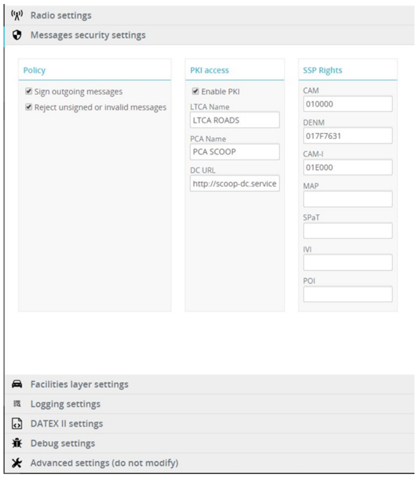

RSU OBU

Fig. 2. C-ITS equipments from NeoGLS


Radio settings

Messages security settings

Policy

☑ Sign outgoing messages

☑ Reject unsigned or invalid messages

PKI access

☑ Enable PKI

LTCA Name: LTCA ROADS

PCA Name: PCA SCOOP

DC URL: http://scoop-dc.service

SSP Rights

CAM: 010000

DENM: 017F7631

CAM-I: 01E000

MAP:

SPaT:

IVI:

POI:

Facilities layer settings

Logging settings

DATEX II settings

Debug settings

Advanced settings (do not modify)

Fig. 3. Web Interface

Scenarios	***Sign outgoing messages at the sender***	***Reject unsigned or invalid messages at the receiver***	***Received***
Same PKI server at both sides	√	√	√
	√	x	√
	x	√	
	x	x	√
Different PKI servers at both sides	√	√	

TABLE I
TESTING OF MESSAGE SIGNATURE AND VERIFICATION MECHANISM BASED ON ETSI TS 103 097.

III. PROOF-OF-CONCEPT OF ETSI TS 103 097 V1.3.1

The structures of certificates according to ETSI TS 103 097 V1.3.1 [3] are totally different from that in V1.2.1. Its implementation is not widely tested, and is not available in the current NeoGLS devices (OBUs and RSUs). To verify its functionality, we test its proof-of-concept by a hybrid platform composed by computers and OBUs, as shown in Fig. 4.

Two computers are connected with two OBUs by the Wi-Fi connection and the ssh connections are established between computers and OBUs. Then we stop the default application of the two OBUs and configure the radio, channel, transmission power so as to ensure that the two OBUs can listen to each other on the ITS-G5 channel [5].

For each message to be transmitted, it is signed (by ECDSA), encrypted (by ECIES), and then encapsulated inside a GeoNetworking packet, which is the payload in a BTP (Basic Transport Protocol) packet. The MAC layer frame is aggregated by adding the MAC layer header, LLC (logic link control) layer header, GeoNetworking header [4], BTP (Basic Transport Protocol) header [6], the payload of a BTP packet, and the checksum.

Then we configure the OBU_2 into the reception mode, and we transmit the framework from OBU_1 by sending the frame transmission command to OBU_1. Notice that, the destination of the MAC frame is known according to the MAC layer header.

When the MAC layer frame is received at the OBU_2, it is shown in the screen of the computer as the receiver. Then we de-aggregate the frame and extract the payload in the BTP packet, and pass the payload to the verification program written by java. The corresponding certificates, including RCA certification, AA certification, Authorization certificate, Enrollment certificate, and receiver's private key are pre-loaded into the program. The decrypted message is shown in the program, when there is no verification error, or an error is displayed in case of verification error.

We have executed the same tests as summarized in Table I for V1.3.1 and obtained the same result as V1.2.1, which validate the functionality of ETSI TS 103 097 V1.3.1.

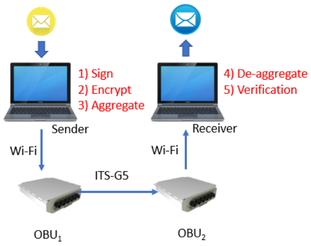


Fig. 4. Working flow of the proof-of-concept for ETSI TS 103 09 V1.3.1

IV. CONCLUSION

The ETSI TS 103 097 V1.3.1 standard introduces new formats for the certificates for securing C-ITS. But its implementation has not been widely tested so far. In this paper, we implemented the proof-of-concept for securing messages in C-ITS by ETSI TS 103 097 with both versions V.1.2.1 and V1.3.1, and verify their functionalities.

REFERENCES

[1] c-roads project, https://www.c-roads.eu/
[2] ETSI TS 103 097 V1.2.1 (2015-06)
[3] ETSI TS 103 097 V1.3.1 (2017-10)
[4] ETSI EN 302 636-4-1 v1.3.1, 2017-08
[5] ETSI EN 302 663 V1.3.1 (2020-01)
[6] ETSI EN 302 636-5-1 V2.2.1. ETSI ITS, 2019.