On the performance evaluation of vehicular PKI protocol for V2X communications security

Farah Haidar, Arnaud Kaiser, Brigitte Lonc

On the performance evaluation of vehicular PKI protocol for V2X communications security

Farah HAIDAR
IRT SystemX
8 avenue de la Vauve,
91120, Palaiseau, France
Email: farah.haidar@irt-systemx.fr

Arnaud KAISER
IRT SystemX
8 avenue de la Vauve,
91120, Palaiseau, France
Email: arnaud.kaiser@irt-systemx.fr

Brigitte LONC
Renault
Alliance System Engineering Department
Guyancourt, France
Email: brigitte.lonc@renault.com

***Abstract*—Cooperative Intelligent Transportation Systems (C-ITS) is an ongoing technology that will change our driving experience in the near future. In such systems, vehicles and Road-Side Units (RSU) cooperate by broadcasting V2X messages over the vehicular network (802.11p). Safety applications use these data to detect dangerous situations on time and avoid them.**

The security of V2X communications is based on the use of a vehicular Public Key Infrastructure (PKI) that delivers digital certificates to vehicles and RSU. Vehicles frequently change their certificate in order to make tracking more difficult and thus preserve drivers privacy.

In this paper, we evaluate the performance of our PKI regarding the reloading of certificates by comparing two communication profiles (with and without V2X security). We developed a Proof-of-Concept (PoC) with real implementation of the PKI protocol and the embedded system. The obtained results show that the end-to-end latency between a requesting vehicle and the PKI is non-negligible. We then discuss and propose optimizations that can be done to improve the performance of the system.

***Keywords*—Public Key Infrastructure, Security, Performance evaluation, Authorization Tickets.**

I. Introduction

C-ITS have gained much attention in the recent years due to the large number of applications that can improve future driving experience. The driver receives information about traffic efficiency, emergency warning, and many others to help him make good decisions [1]. This information is exchanged between ITS-Stations(ITS-S) using V2X messages.

The kind of information exchanged and processed by vehicles can be critical and directly linked to the driver's privacy. A vehicle indeed periodically broadcasts Cooperative Awareness Messages (CAM) [2] that contain its geographical position, speed and heading to the neighboring vehicles. Safety applications use this information to compute potential critical situations and prevent them.

In order to be usable by a maximum number of ITS-S, V2X messages are not encrypted. That is, a malicious person can take advantage of the opportunity to disrupt the system by, for instance, broadcasting false messages. In order to cope with such security issues and guarantee a satisfying level of security, researchers and companies rely on the use of a vehicular PKI. Basically speaking, ITS-S authenticate themselves to the PKI and get digital certificates in return. They sign their V2X messages with these certificates to guarantee authenticity and integrity.

However, V2X messages also include several identifiers (such as MAC address, GeoNetworking address, StationID, certificate, etc.) that enable linkage of messages originated by a same ITS-S. Consequently, it becomes easy for a malicious person to track a vehicle just by eavesdropping its CAM. The tracker can then find the real driver's identity, postal address, work place, etc. leading to severe privacy violation. The countermeasure adopted by the community relies on the use of short term certificates (called Authorization Tickets – AT). Vehicles get a pool of AT from the PKI. They use one of them to sign their V2X messages during an arbitrary period (e.g. for 10 minutes or for 10 km) and then use another one. Each time a vehicle changes its AT, it also changes all of its identifiers. As a result, vehicles frequently change their identity, making tracking much more difficult.

In this paper, we aim at evaluating the performance of our PKI protocol regarding the reloading of AT. We compare two communication profiles that can be used by a vehicle to request new AT to the PKI in terms of network overhead and end-to-end latency. Our measurements are made on a real testbed deployment. Results show that for both profiles the network packets size as well as the latency are non negligible. We then discuss and propose solutions to improve these performance.

This paper is organized as follows. Section II presents the related works. Our PKI and its protocol are described in section III. Section IV describes the ITS-S architecture as well as the communication profiles. In section V we detail the use case and the experimentation setup. We discuss the obtained results in section VI and conclude this work in section VII.

II. Related works

Despite the large literature on vehicular networks, there are very few papers that focus on the performance evaluation of PKI protocols.

PRESERVE is an European project that contributed to the security and privacy aspects of vehicular networks. They proposed a V2X security system based on a PKI and evaluate its performance. More precisely, they calculated the processing latencies of the different entities of the system. Results from this study can be found in PRESERVE public deliverable D5.3

[3]. The main difference with our work is that they considered cellular network instead of 802.11p to communicate between the vehicle and their PKI.

Authors of [4] present SEROSA, a service-oriented security and privacy-preserving architecture for vehicular networks. SEROSA also relies on the use of a PKI. They evalute its performance in terms of time spent at each system component. However unlike us, the evalution is done by simulation rather than a on PoC.

III. Public Key Infrastructure

PKI is the trusted third-party that guarantees security and privacy for C-ITS. It delivers two kinds of certificates: long term (called Enrolment Credentials – EC) and short term (AT). EC are used by ITS-S for authentication within the PKI in order to request AT. AT are then used to sign V2X messages.

That is, an ITS-S typically has one EC and many AT. As mentioned previously, ITS-S frequently change of AT to help against tracking of vehicles.

A. ISE PKI architecture

ISE stands for *ITS SEcurity*, a 3 years French research project that focus on security and privacy aspects of C-ITS. In this project we developed and implemented a PKI fully compliant with the European Telecommunications Standards Institute (ETSI) current standards. Our PKI has been used during the last ETSI Plugtests 2016 in Livorno. We also provide our PKI to SCOOP@F, a French deployment project that aims at deploying more than 3000 equipped vehicles within 2000 km of equipped roads. We are also currently proposing our PKI protocol at ETSI for standardization.

Figure 1 depicts ISE PKI architecture that consists of the following entities:

- **Root Certificate Authority (RCA)**: RCA is the root of trust for all certificates within the PKI hierarchy. It delivers certificates to the Enrolment Authority (EA) and the Authorization Authority (AA) to authorize them to issue certificates to ITS-S.
- **Enrolment Authority (EA)**: EA issues one EC per ITS-S. EC are considered as a proof of identity, thus used to identify and authenticate ITS-S within the PKI.
- **Authorization Authority (AA)**: AA issues AT to ITS-S that are used in V2X communications.
- **Distribution Center (DC)**: provides to ITS-S up-to-date trust information necessary to validate that received information come from a legitimate and authorized ITS-S/PKI authority.
- **Operator**: registers ITS-S and updates necessary information in the EA.
- **ITS-S**: end-entity of the system that requests certificates to the PKI and communicates with other end-entities.

In this architecture, the separation of the EA and the AA in two distinct entities guarantees ITS-S privacy: EA knows the real identity of the ITS-S but does not know its AT, whereas AA knows the ITS-S AT but not its real identity.

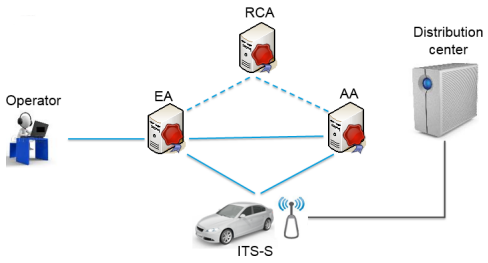

Fig. 1. ISE PKI architecture

B. ISE PKI protocols

The deployment of a new ITS-S follows the steps below:

1) **ITS-S registration**: the operator registers the new ITS-S to the EA. This operation is usually done using a secured web interface.
2) **EC request**: the registered ITS-S sends a request to the EA in order to get its EC. This operation can be done either directly by the operator or by the end user that purchased the ITS-S. As EC are long term certificates, an ITS-S usually requests only one EC in its lifecycle.
3) **AT request**: when needed the ITS-S sends AT requests to the AA in order to get new AT. Before providing AT, the AA forwards the request to the EA. The EA verifies that the requesting ITS-S is legitimate and authorized to request AT. Depending on the response from the EA, the AA delivers or not new AT to the requesting ITS-S.

About communication, note that all exchanges with the PKI are done using HTTP.

IV. ITS-S architecture

A. ETSI architecture

Figure 2 depicts the ETSI ITS-S communication reference architecture as defined in [5] with a zoom in the Networking and Transport layer. The architecture consists of four horizontal layers (the communication stack) and two cross layers used for management and security purposes. Each layer provides the following functionnalities:

- **Access Technologies**: manages the access technologies that are available in the ITS-S (802.11p, cellular, etc).
- **Networking and Transport**: provides data transport between source and destination ITS-S. As detailed in figure 2 ETSI considers the following communication profiles to achieve this task:
  - BTP [6] over GeoNet [7]
  - TCP/UDP over IPv6
  - TCP/UDP over IPv6 over GeoNet [8]
- **Facilities**: provides support to ITS applications by sharing generic functions and data such as: generic HMI support, data presentation (e.g. ASN.1), environment information (time, location, etc.), addressing mode and channel selection at lower layers, etc.
- **Applications**: runs the ITS applications.

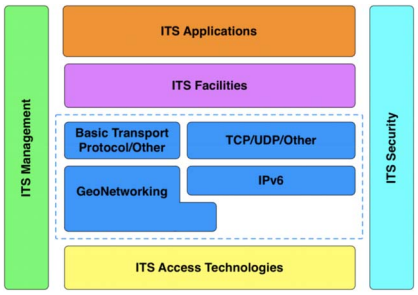

Fig. 2. ETSI ITS-S reference architecture

- **Management**: manages the communication stack depending on ITS applications requirements.
- **Security**: secures communications between ITS-S by providing security services (cryptographic computation, secured memory, etc.)

B. Communication profiles for PKI requests

In this paper we evaluate the performance of the PKI protocol according to ETSI communication profiles. More precisely, we compare the performance of the two following profiles regarding AT requests:

- **TIG** (**T**CP/**I**Pv6/**G**5): the AT request is created and encapsulated in HTTP, TCP and IPv6. The request is then directly sent over the G5 network (802.11p).
- **TI3G** (**T**CP/**I**Pv6/**G**N6ASL/**G**N/**G**5): the AT request is created and encapsulated in HTTP, TCP and IPv6. It then goes through the GN6ASL (GeoNetworking to IPv6 Adaptation Sub-Layer) [8] and GN layers. Finally, the request is then sent over the G5 network.

Figure 3 details the path followed by data when the ITS-S sends an AT request to the PKI. (1) The *Cert Reload* application requests the creation of an AT request to the Security layer. (2) The Security layer generates the request, adds the HTTP header and sends it to the Networking and Transport layer. (3) The request is encapsulated into TCP and IPv6 headers. (4) According to the selected profile (TIG or TI3G), the request is either directly sent to the Access layer or (5) sent to the GN6ASL for encapsulation in a GN packet. (6) The GN packet is then sent to the Security layer for signature. (7) The Security signs the GN packet and returns it. (8) The signed GN packet is sent to the Access layer. (9) Finally, the 802.11p frame is sent over the G5 network. The AT response coming from the PKI follows the same steps in reverse order.

Note that TI3G profile provides security over the G5 network (AT request is signed) which is not the case with TIG profile.

V. Experimentation

A. Use case description

The use case is depicted on the left part of figure 4. A vehicle is within range of a RSU that provides Internet access. The vehicles is low on AT and needs to refill its pool. It thus

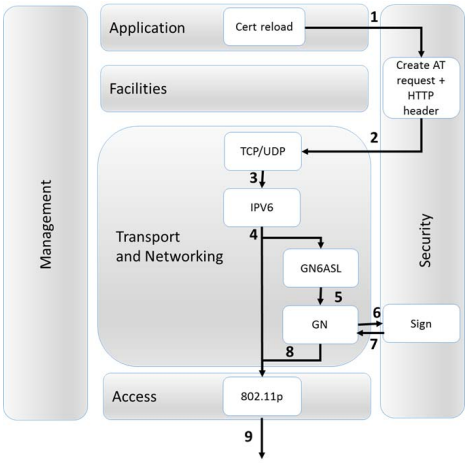

Fig. 3. Data path within the ITS-S architecure when sending an AT request

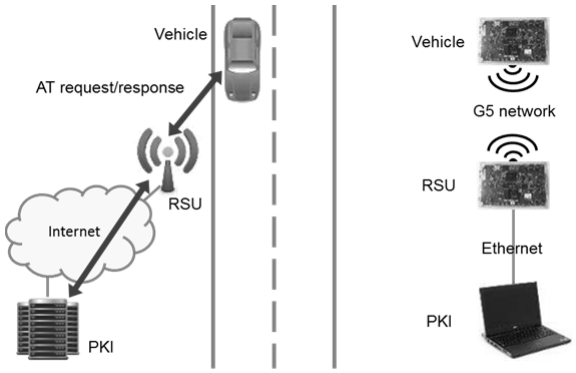

Fig. 4. Use case picture (left) and testbed deployment (right)

uses the RSU as gateway forwarder to reach the PKI (located somewhere on the Internet) and requests new AT.

Note that the service advertisement (i.e. how the RSU advertises the vehicle that it provides Internet connectivity) as well as the vehicle IPv6 autoconfiguration are not considered in this paper.

B. Testbed deployment

The testbed deployment for our experimentation is depicted on the right part of figure 4. We deploy two boards: one is the On-Board Unit (OBU) within the vehicle, the other is the RSU. We deploy the PKI on a laptop. Table I summarizes the testbed specifications.

The OBU and the RSU are connected via the G5 network at 1-hop distance. As the PKI can be located anywhere on the Internet, it is difficult to estimate the connectivity between the RSU and the PKI. Therefore in our experiments we decided to lower at maximum the impact of the network latency between the RSU and the PKI. To this end, we connect them directly using a Gigabit Ethernet cable.

Before starting our experiments, we registered both OBU and RSU to the PKI and get their respective EC by executing

Equipment	V2X Board	Laptop
Vendor	Renesas	Dell
Type	R-Car E2 Hideyoshi board	Latitude 3330
Architecture	ARMv7a	x86
OS	Linux Poky (Yocto project)	Linux Ubuntu 14.04 LTS
Connectivity	802.11p, GNSS, Ethernet	Ethernet
V2X software	ETSI V2X communication and security stacks	ISE PKI

TABLE I
SPECIFICATIONS OF THE TESTBED EQUIPMENT

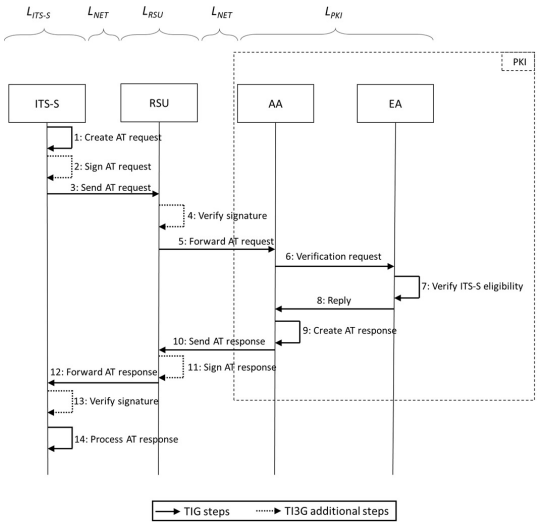

Fig. 5. AT request/response using TIG or TI3G profile

steps 1) and 2) of section III-B.

For cryptographic operations, we use the well-known OpenSSL library.

C. Messages exchanges

Figure 5 depicts the messages exchanged when the ITS-S requests AT using TIG or TI3G profile. The difference between both profiles is the computation and verification of GN packet signatures at both OBU and RSU.

At the top of figure 5 we show the measured latencies:

- L_{ITS-S}: latency in the ITS-S. It consists of the creation of the request and the processing of the response. With the TI3G profile, it also includes the signature computation of the request and the signature verification of the response.
- L_{NET}: latency of both G5 and Ethernet networks.
- L_{RSU}: latency in the RSU. It consists of the forwarding of both the request and the response between the two networks. With the TI3G profile, it also includes the signature verification of the request as well as the signature computation of the response.
- L_{PKI}: latency of the PKI. It consists of the verification of the request, its eligibility and the creation of the response.

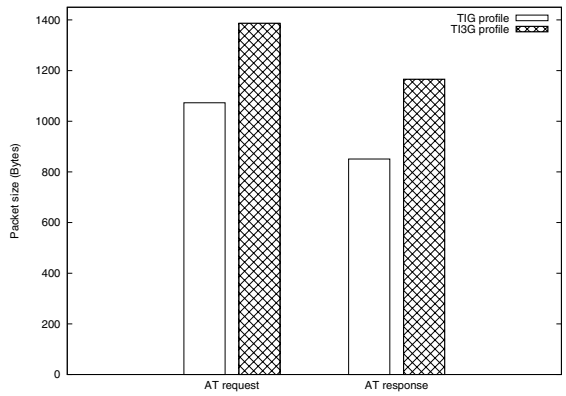

Fig. 6. AT request/response median packet size on the G5 network

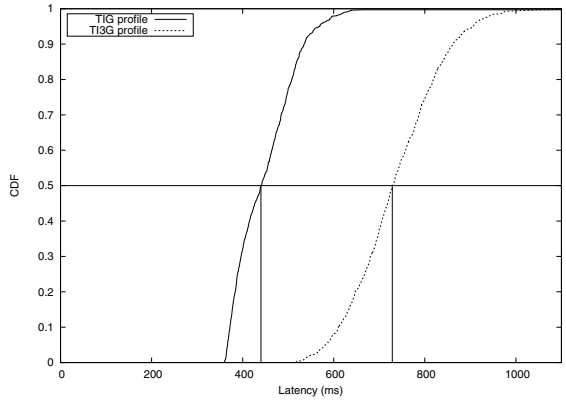

Fig. 7. AT request/response round-trip latency

VI. RESULTS AND ANALYSIS

We conduct our experiments as follow: for each profile, the ITS-S sends one AT request to the PKI via the RSU. Once the AT response is received, the ITS-S sends another request, and so on until reaching 1000 requests/responses.

A. Packets size

Figure 6 shows the median packet size of an AT request and response on the G5 network for both profiles. As we can observe, the packet size for the TI3G profile is larger than the size for the TIG profile. This difference is due to the overhead generated by the Geonetworking protocol and the Security stack: the Geonet header + the Security header + the signature.

B. Latency

Figure 7 depicts the cumulative distribution function (CDF) of the AT request/response round-trip latency for both profiles. We plot the horizontal line at 0.5 to show the median latencies: 440.051 ms for TIG profile and 728.657 ms for TI3G. The difference is explained by two reasons: 1) TI3G requires aditionnal security operations (message signature/verification) and 2) TI3G packets size are larger, thus requires more time to be sent over the G5 network.

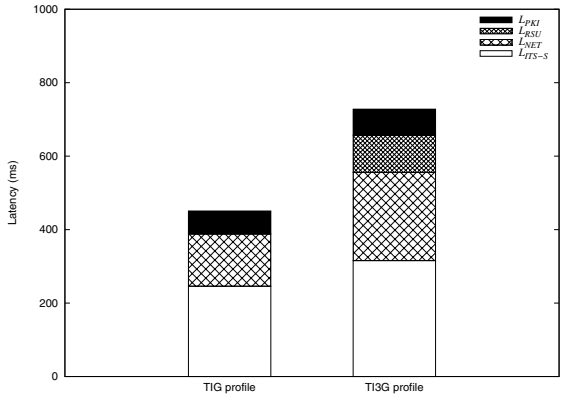

Fig. 8. AT request/response detailed latency

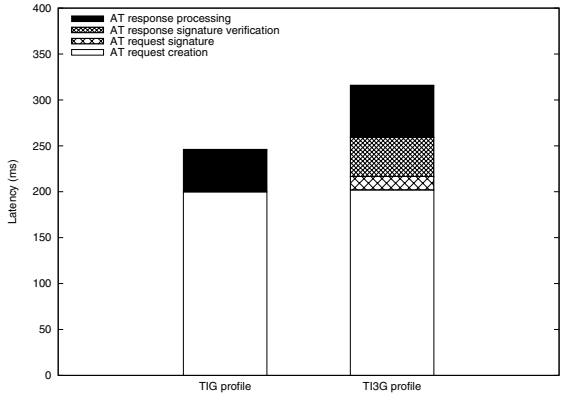

Fig. 9. AT request/response detailed L_{ITS-S}

Let us have a look at the round-trip latency in more details (remember it consists of L_{ITS-S} + L_{NET} + L_{RSU} + L_{PKI}). Figure 8 shows the distribution of each of these latencies (the median values are represented). With TI3G profile, we observe an increase of L_{ITS-S} and L_{RSU} that are due to signature/verification operations (note that L_{RSU} is negligble with TIG profile as the RSU just forwards the packets) as well as an increase of L_{NET} that is due to the extra time required to send the larger packets over the network. L_{PKI} is not affected by the use of one or the other profile, thus remains of the same order. We also observe that L_{ITS-S} has the highest impact on the round-trip latency. Let us have a deeper look at this latency.

Figure 9 details L_{ITS-S}. We clearly observe that the AT request creation costs the most time. This is because it consists of 7 cryptographic operations: 3 generation of keys, 1 HMAC, 1 signature and 2 encryptions.

C. Discussion

The obtained results show that requesting an AT to the PKI requires about half a second, and even more in the case of a secured G5 communication (TI3G). Remember that our experiments are run in optimal conditions: the latency between the RSU and the PKI is negligible (direct connexion in Ethernet) and the G5 network is not loaded (only OBU and RSU are broadcasting V2X messages). Therefore, the round-trip latency in a real situation will be even higher.

Results also show that a lot of time is spent in cryptographic operations. This is quite interesting because optimizing such operations is feasible compared to trying to lower network latencies. For instance, integrating specific Hardware Security Modules (HSM) dedicated to cryptographic acceleration in ITS-S will lead to lower the round-trip latency.

VII. Conclusion and future works

In this paper we evaluate the performance of our PKI protocol on a testbed with real implementations. We compare two communication profiles: with and without the V2X security. Results in terms of overhead and round-trip latency show that skipping security provides better performance but still requires at least half a second, which is non negligible in highly mobile networks.

Latency results also show that a large amount of time is elapsed in the ITS-S when processing cryptographic operations. Therefore, optimizing this kind of operations with a HSM will help reducing the overall latency.

Future works include a performance evaluation and comparison with the integration of a HSM, experimentations in a real situation while driving, as well as evaluating the protocol under a congested G5 network (high density of vehicles). Integrating the service advertisement procedure as well as evaluating the latency between RSU and PKI are also of interest to improve our study.

Acknowledgments

This research work has been carried out in the framework of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program *Investissements d'avenir*.

References

[1] ETSI, "TR 102 638 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," June 2009.

[2] ——, "EN 302 637-2 V1.3.2 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," November 2014.

[3] "Deliverable 5.3 - Deployment Issues Report v3," in *PRESERVE project*, https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D5.3-Deployment_Issues_Report_V3.pdf, December 2013.

[4] S. Gisdakis, M. Lagana, T. Giannetsos, P. Papadimitratos, "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications," in *Vehicular Networking Conference (VNC)*, December 2013.

[5] ETSI, "EN 302 665 V1.1.1 - Intelligent Transport Systems (ITS); Communications Architecture," September 2010.

[6] ——, "EN 302 636-5-1 V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol," August 2014.

[7] ——, "EN 302 636-4-1 V1.2.1 - 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-Independant Functionality," July 2014.

[8] ——, "TS 102 636-6-1 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols," March 2011.