Cooperative ITS Security Framework: Standards and Implementations Progress in Europe

Brigitte Lonc[1] and Pierpaolo Cincilla[2]

[1]DEA-SM - Alliance System Engineering Department, Renault, Guyancourt, France. E-mail: brigitte.lonc@renault.fr
[2]Technological Research Institute SystemX, Palaiseau, France. E-mail: pierpaolo.cincilla@irt-systemx.fr

***Abstract*—A number of standardization organizations and European projects dealt with security and privacy issues in Cooperative Intelligent Transport Systems (C–ITS). In this paper, we present recent standardization activities and implementations of security services in various cooperative driving applications (Release 1 use cases and next stages). We discuss the validation of C-ITS embedded systems security standards and the Public Key Infrastructure (PKI) implementation plans. We present already standardized messages as well as a new proposal for standardization. Already standardized messages focus on vehicular safety and traffic efficiency, while our proposal targets service advertisement.**

I. Introduction

Intelligent Transport Systems (ITS) refers to the integration of information and communication technologies with transport infrastructure to improve safety, mobility and environmental sustainability for the benefit of all road users. Cooperative ITS (C-ITS) applications are based on vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) wireless communications. Based on the exchanged messages, the C-ITS applications will first provide the road hazard warnings and traffic information to the driver, and later will react automatically.

Despite the many potential benefits of C-ITS, the associated wireless communications raises security and privacy issues which, if not addressed, could jeopardize their deployment.

For securing C-ITS communications, the common understanding is to use asymmetric cryptography and this requires to set up a Public Key Infrastructure (PKI) for the management of security credentials of the ITS Station (ITS–S). A key issue is to provide interoperability of secured communications for the various types of wireless communications: Vehicle-2-Vehicle (V2V), Vehicle-2-Infrastructure (V2I) and Vehicle-2-PKI when the ITS station needs to connect to the PKI entities also named Certificate Authorities (CAs) for security management purpose.

Another major issue to take into account is the user privacy [14]. Any security credential management system must consider a privacy preserving scheme to protect vehicles and users identity according to national and international legislation.

The remainder of this paper is organized as follows. Section II presents the standardization activities on C-ITS security with focus on the ETSI security framework and standardization progress. Section III describes ETSI PKI design and data models for secured messages and certificates. Section IV describes the security services implementation for various messages. C-ITS experimentation and validation is discussed in Section V. Conclusion is given in Section VI.

II. C-ITS Security: Standardization Activities

A. ITS Security Standards Framework

In order to achieve C-ITS interoperability, the development of ITS communication security standards is paramount. For this purpose, dedicated working groups within standardization organizations address security and privacy issues. For example, the ETSI TC ITS WG5 working group in Europe [1] and the IEEE 1609.2 working group in U.S [2].

The IEEE 1609 DSRC WG has developed a standard for specification of the “security WAVE services” enabling secure wireless communications of application and WAVE management messages (IEEE 1609.2 [3]). In IEEE 1609.2, the service for messages authenticity and integrity is based on digital signatures using the Elliptic Curve Digital Signature Algorithm (ECDSA). The confidentiality protection is based on AES symmetric encryption (AES-CCM authenticated encryption). An asymmetric encryption scheme using elliptic curve integrated encryption scheme (ECIES) is provided and is used to transport symmetric encryption keys [3]. The scope of IEEE 1609.2 standard is to define security data structures and especially secure message formats, and the processing of those secure messages within the DSRC/WAVE system.

In Europe, ETSI TC ITS is organized in five working groups: applications requirements, architecture cross layer, transport networks, media and security. ETSI TC ITS WG5 deals with privacy, data protection and security aspects in ITS. Three steps compose the security process of this group: (i) identify and catalogue ITS security risks, (ii) build security requirements and define a list of potential countermeasures (generic security services), (iii) specify an architecture and a standardized set of services and interfaces that enable implementation of secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications.

As part of ETSI ITS Release 1 [4], a major achievement of ETSI work in this area, has been the design of a security

framework for C-ITS including a PKI for digital certificate management. This includes the publication of documents listed in Table I.

TABLE I: ETSI ITS Security standards

Standard Reference	Title	Status
TR 102 893	Threat, Vulnerability and Risk Analysis (TVRA) technical report	v1.1.1 Published
TS 102 731	Security services and architecture	v1.1.1 Published
TS 103 097	Security header and certificate formats	v1.2.1 Published
TS 102 940	ITS communications security architecture and security management	v1.2.1 Under approval
TS 102 941	Trust and privacy management	v1.1.1 Published under revision
TS 102 942	Access Control	v1.1.1 Published
TS 102 943	Confidentiality services	v1.1.1 Published

ETSI ITS security standards cover current ITS security needs and objectives, based on Threat and Vulnerability Risk Analysis [5] (TVRA) risk analysis status. A critical feature of this security framework is to include privacy protection for users and vehicles of cooperative ITS systems, e.g., using pseudonyms certificates for wireless secure communications and changing them regularly.

TABLE II: mapping of generic security services to security architecture and associated standardized services and interfaces.

Service category	Security service	Standard Reference
Enrolment	Obtain / Remove / update Enrolment Credentials	TS 102 941 under revision
Authorization	Obtain / Update Authorization Ticket	TS 102 941 under revision
Single Message Signature	Authorize / Validate Authorization on Single Message	TS 102 940 TS 103 097
Data Encryption	Encrypt / Decrypt Single Message	TS 102 940 TS 103 097
Replay Protection	Replay Protection Based on Timestamp	TS 102 940 TS 103 097
Plausibility	Validate Data Plausibility	TS 102 940 TS 103 097
Security Associations management	Establish / Update / Remove Security Association, Send / Receive Secured Message	See RFC proposal for TLS extension [13]
Integrity	Checksum	Not supported
Accountability	Record incoming / outgoing message	Not supported
Remote management	Activate / Deactivate ITS transmission	Not supported
Report Misbehaving ITS–S	Report Misbehaviour at ITS–S, Detection and Prevention of Misbehaviour by Misbehaviour Authority	Not supported in Release 1 TS 102 940 and 941 future extension

III. Security for V2V/V2I Communications

ETSI ITS WG5 has developed requirements and technical specifications for secure and privacy-preserving communications, secured message formats, certificates, PKI structure and secure hardware for ITS–S. Requirements and technical specifications are based on TVRA and recommended security services (see Table I).

The ETSI cryptosystem for C–ITS communications is currently based on IEEE 1609.2 [3]. Recent national deployment projects in Europe have raised scalability and upgradability issues in the design: they require capability to improve crypto-algorithms over time in C–ITS system which is a major issue in embedded systems due to constrained resources (i.e., Hardware Security Module, crypto-accelerators).

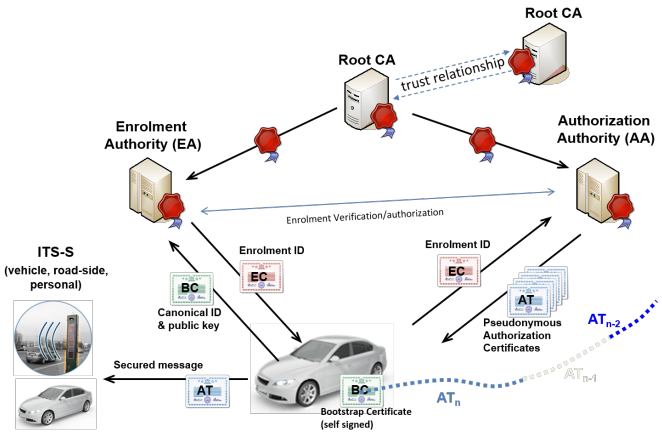

Fig. 1: ETSI ITS trust model (PKI).

A. ETSI ITS PKI Design

ETSI security concept uses long-term certificates for identification and accountability of ITS–S, named *Enrolment Certificates* (EC) and short-lived, anonymized certificates for V2V/V2I communications, named *Authorization Tickets* (AT) or *pseudonym certificates*.

Privacy concerns are introduced due to the content of safety messages, i.e., Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) (see Section IV), and due to the authentication applied to the messages (message signature). Cryptographic certificates allow tracking of ITS vehicles. Users privacy is protected by a pseudonym scheme i.e., changing frequently the pseudonym certificates (AT) used to authenticate messages such as CAM or DENM. Thereby, the tracking of vehicles is avoided or, at least, made more difficult. To meet this privacy goal, the PKI has to issue and distribute a large set of Authorization Tickets (pseudonym certificates) to each ITS–S. The discussion of other tracking methods such as radio fingerprint or mobile phones tracking is out of the scope of this paper.

ETSI design considers a hierarchical PKI structure, with the Root CA (RCA) acting as the trust anchor for a given C-ITS Trust Domain and controlling all subordinate certification authorities (CAs) and end-entities in its hierarchy (see Fig 1). The C-ITS PKI system may consist of a number of RCAs, which may cooperate and cross-certify each other. For example in Europe, RCAs could be operated by various

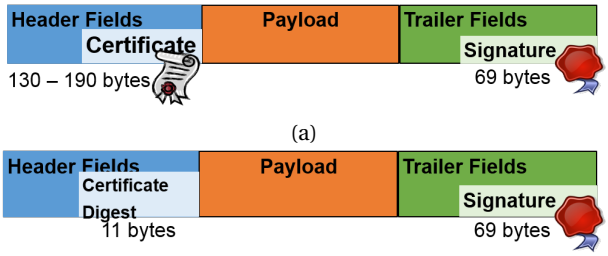

Fig. 2: (a) Signed message with Authorization Ticket. (b) Signed message with Certificate Digest.

stake-holders, such as governments (EU/National), vehicle manufacturers, telecommunication providers etc.

Due to the broadcast nature of CAM and DENM, the trust relationship between ITS stations has to be scalable (hundreds of millions of nodes) and instantaneously verifiable. To meet these requirements, the ITS–S enrolment and authorization for different services is delegated to Trusted Third Parties (TTP), composed of two types of CAs:

Enrolment Authority (EA): Validates that an ITS–S can be trusted. It issues an enrolment identifier for the ITS–S and a proof of its identity (Enrolment certificate).

Authorization Authority (AA): An ITS–S may apply for specific services and permissions. These privileges are denoted by means of authorization tickets (AT).

Within the C-ITS network, the EA provides an ITS–S with an enrolment ID and related enrolment certificate (long term). The AA provides the ITS–S with multiple pseudonyms and the related authorization tickets (short term), to be used in V2X communication.

Element	Value	Description	Length
SecuredMessage			
protocol_version	0x02		1
header_fields<var>	0x8091	Length: 145 octets	2
type	0x80	=signer_info	1
type	0x02	=certificate	1
certificate	...	certificate of signer	141
type	0x05	=its_aid	1
its_aid	...		1
payload			
type	0x01	=signed	1
data<var>	0x01	Length: 1 octet	1
[data]	...	payload	1
trailer_fields<var>	0x43	Length: 67 octets	1
type	0x01	=signature	1
signature			
algorithm	0x01	=ecdsa_nistp256_with_sha256	1
ecdsasignature			
R			
type	0x00	=x_coordinate_only	1
x	...		32
s	...		32
Total size: 219 bytes			

Fig. 3: Example of ETSI SecuredMessage (signed).

B. ETSI Secure Message Format Specification

ETSI TS 103 097 [6] specifies the data structures for secured messages. Fig. 2a depicts the general structure of a security envelope for signed messages. The document specifies Security profiles for CAM, DENM and a generic profile. The certificate format is specified and includes profiles for RCA, EA, AA, and end-entities certificates (EC, AT).

For safety messages, such as CAM and DENM, every single message carries its own certificate and signature information due to the delay-sensitive processing of safety information at the receiver side. Certificates omission allows to reduce the network bandwidth usage, at the expense of a higher latency time for message verification by the receiver (see Fig. 2b). For this purpose, ETSI TS 103 097 provides a *SignerInfo* field containing the authorization certificate identifier specified as the 8 bytes certificate digest with sha256.

The ETSI TS 103 097 specifies how the structure is encoded and should be processed by the security processing services in the ITS–S Security Entity [7]. It includes a *protocol version*, *header fields*, a *payload field* and *trailer fields*. The structure is designed to be flexible, so the header and trailer fields are of variable length and may contain any number of instances of each defined field (0, one or many). The SecuredMessage elements are formatted as follows:

- The header or trailer fields shall begin with a length field specifying the total length of the header or trailer in bytes.
- The payload field shall contain only one message payload.
- Every field in the header, payload and trailer shall be preceded, respectively, by a *HeaderFieldType*, *PayloadType* and *TrailerFieldType*.

Header fields contain information used by the security layer, such as plausibility data (*generation_time*, *expiration*, *generation_location*, *request_unrecognized_certificate*, *its_aid*, *signer_info*, *encryption_parameters*, *recipient_info*) and can be further extended (with unknown fields). Its-aid specifies the security profile to apply and defines the use of the header, payload and trailer fields corresponding to this type of message. Only one payload field is allowed and this field begin with the PayloadType and the length of the payload data. The trailer field is of variable length and contain different trailer fields, e.g., a signature. Fig. 3 gives an example of secured message encoding where the signer is identified by its certificate.

C. Roles and Permissions Modelling in ETSI Certificates

In order to access the ITS network and make full use of the available ITS applications, services and capabilities, an ITS station is required to obtain specific credentials from the Authorization Authority. These credentials, in the form of cryptographically signed certificates, are used to assure any receiving ITS–S that the sender station can be trusted and has the necessary permissions to send the particular service-specific information. Users in the ITS system may have different roles and different authorization levels (e.g., personal vehicle, emergency vehicles, RSUs, fixed or mobile roadwork units...).

Authorization certificates are only issued to an ITS–S after a comprehensive procedure has been followed in order to

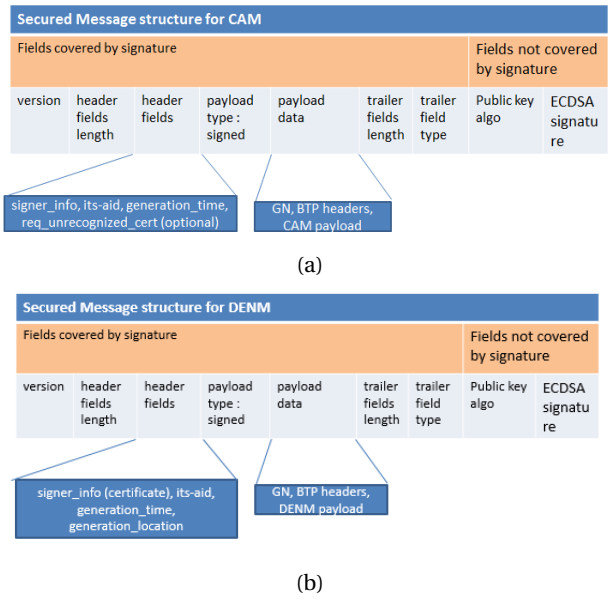

Fig. 4: Structure of a signed CAM (a) and DENM (b) message.

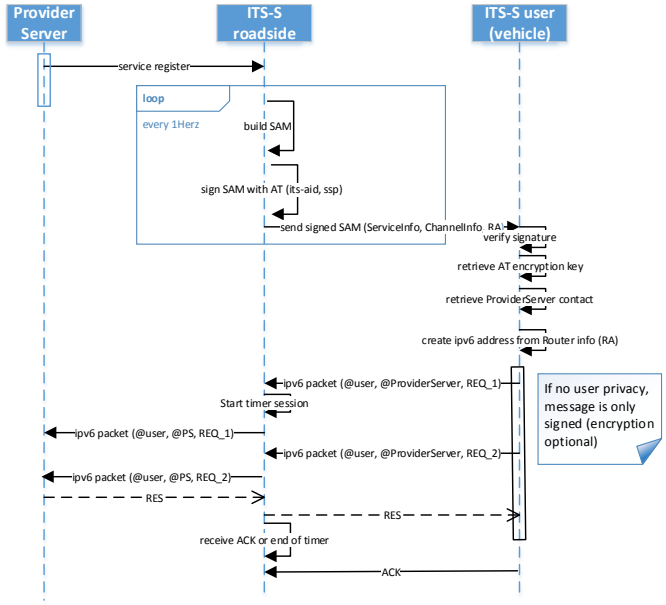

Fig. 5: Message flows for service advertisement and service usage use case.

protect its identity and avoid misuse of ITS services and network's capabilities (initialization/registration, enrolment and authorization).

In ETSI security framework, the authorization certificate indicates the permissions of the certificate holder, i.e., what statements the holder is allowed to make or what privileges it is allowed to assert in a signed message broadcasted on the ITS G5 communication channel.

In ETSI architecture, the ITS-Application Identifier (ITS-AID) allows to identify a given message, service or application. The ITS-AID field in the ITS–S certificate (AT) indicates the overall permissions granted to the vehicle: e.g., there is an ITS-AID that indicates that the sender is entitled to send CAMs, and another one to indicate that the sender is entitled to send DENMs. The Service Specific Permissions (SSP) is a field that indicates specific sets of permissions for a given message, service or application (ITS-AID). This is used to elevate the privileges of the sender within this application (or message generation facility). For example, there may be a SSP value associated with the ITS-AID for CAM that indicates that the sender is entitled to send CAMs for a specific vehicle role (e.g., emergency vehicle, public transport...) or for a specific RSU (e.g., tolling zone).

Permissions granted to an ITS station are indicated in the certificate by a pair of attributes: ITS-AID and SSP. The TS 103 097 certificate format allows a certificate to contain multiple $(ITS-AID, SSP)$ pairs.

IV. Security Services Implementation in Release 1 Use Cases and Future Applications

This section details the format of secured message used by various C–ITS applications. The formats of a *SecuredMessage* is defined in ETSI TS 103 097 for different profiles

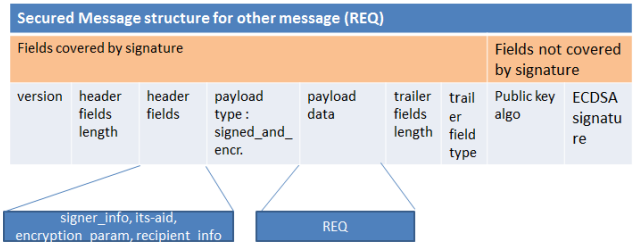

Fig. 6: Example of a signed and encrypted request.

(CAM, DENM, and generic profile). ETSI TS 103 097 security profile specifies which fields shall be included (and not included) in a security header. For some header fields, the values to be used are specified in the message standard (e.g., CAM, DENM): the ITS-AID is specified in ETSI TS 102 965 and SSP usage is specified in [8] and [9].

Section IV-A presents the structure of already standardized secured messages CAM and DENM, while Section IV-B discuss our proposal: the Service Advertisement Message (SAM). SAM is an Infrastructure–to–Vehicle communication (I2V) message currently under standardization along with other I2V messages as such as SPATEM, MAPEM, IVIM, etc. specified in [20]. These I2V messages use the generic security profile.

A. Standardized Messages

Based on the use cases specified by the Car2Car Communication Consortium (C2C-CC) for Day1 [12], two main message type have been specified to provide highly dynamic information for road safety applications. They can also be used as vehicle probe data for traffic management

such as in CORRIDOR & SCOOP@F pilot project. Those message types are:

Cooperative Awareness Message (CAM): enables to broadcast periodically information to neighbor stations (one-hop communication). CAM contains a pseudonym identity (stationID), a GNSS-based location and timestamp and vehicle dynamic information (such as speed, heading etc...). For vehicles, CAMs are constantly broadcasted at adjustable frequency between 1 and 10 Hz using the CCH channel and IEEE 802.11p protocol. Special role vehicles can use optional containers to provide situational information, e.g., an emergency vehicle using its siren or light bar.

Decentralized Environmental Notification Message (DENM): is transmitted when a vehicle detects an event (road hazard detection). A DENM contains a station ID (pseudonym), an event type, a generation time, a position, a validity time, and a relevance area and traffic direction. DENMs are broadcasted by the originating ITS-S at a given frequency (e.g. at 10 Hz) and for a given duration or until the end of the event detected. DENMs are geo-broadcasted in multi-hop mode using location information to forward packets.

CAM and DENM standards have been specified by ETSI and pushed as European Norms (see [8], [9]). As CAM and DENM are providing time-critical safety information to vehicles in their vicinity, data confidentiality is not required. In contrast, the sender's origin, data integrity, and geo-routing information need to be protected and a digital signature is applied. TS 103 097 defines the security profiles of CAMs and DENMs. Fig. 4a and Fig. 4b present respectively the structure of a signed CAM and a signed DENM.

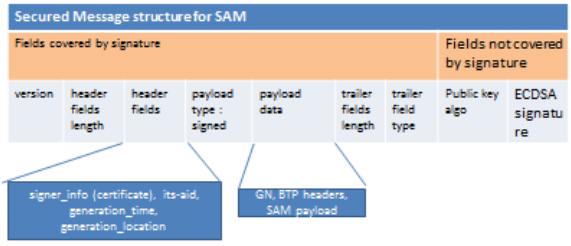

Fig. 7: Structure of a signed SAM messsage.

B. Service Advertisement Message (SAM)

We contribute to the ETSI standardization activity with a proposal for standardization of Service Advertisement Message (SAM). SAM messages are used by service providers to inform ITS stations about available local services or about services that can be accessed on a remote server. Fig. 7 gives an example of a signed SAM message. The message is currently being defined by ETSI [15] and being harmonized with WSA WAVE Service Announcement (IEEE 1609.3 [16]). SAMs/WSAs do not contain application information themselves, but they provide information about the offered services (*ServiceInfo*) and contact information about the local or remote service provider (*ChannelInfo*, *CommunicationInfo*, etc.) allowing the user to decide whether to connect or not.

SAM messages are broadcast (one-hop) as unencrypted messages and usually sent multiple times per second.

In order to protect message integrity and authenticity, ITS–S providers should sign SAM messages using an Authorization Ticket with specific permissions, i.e., with a dedicated ITS-AID and SSP empty. This way, ITS–S are protected over attacks such as fake or malicious service providers and Internet server impersonations.

As the nature of service is broadcast to any possible receivers and the sender is a static RSU or a mobile vehicle which accepts to play a distinguishable role (e.g., leader vehicle in a platooning), no privacy requirement applies.

In many cases, the responding ITS–S is associated with an end-user vehicle with a strong privacy expectation. The diagram in Fig. 5 gives an example of how a secure unicast communication can be established for the execution of the selected service.

In the example of Fig. 5, if user privacy is required, we assume that the ITS–S provider unit is signing with an AT including two keys: one verification key and one encryption key. A temporary symmetric key (AES-CCM 128 bits) is created by the user and is carried with the request REQ using asymmetric ECIES encryption scheme (i.e., the encryption key of the provider unit).

This hybrid encryption method enables integrity and encryption of medium and large data volume using the AES-CCM key (see [23] for AES-CCM method details). For instance, if the ITS–S user wants to send a REQ larger than 1000 bytes, it may be necessary to fragment/reassemble the message at the application level. Fragmentation allows packets size limitation and ITS-G5 channel congestion management. In ITS G5, the MTU (maximum transmission unit) allowed for GN packets is MTU_GN = 1492 bytes - GN & BTP headers (see [17]) and for IPv6 packets is MTU_IPv6 = 1.500 - LLC, SNAP & IPv6 headers (see [18]). For a G5 service channel (SCH) due to congestion control, the size of a frame may be limited to 750 bytes at 6 Mbit/s (see [19]). Thus, the ITS–S has to fragment the REQ message in several encrypted parts (see Fig 5). Notice that since two fragments cannot share the same key/nonce pair [23], a fresh key or a fresh nonce should be used for each message. The fresh key/nonce pair must be included in each fragment, adding a non negligible overhead on the message size. We are currently working at alternatives solutions to reduce this overhead.

Additionally, the service provider (RSU) may decide to authenticate the responding ITS–S user to control the access to its own resources and infrastructure network: using the ETSI security standard, the responding ITS–S user must send an encrypted and signed message using the

SecuredMessage data structure (see ETSI TS 103 097 clause 5.1) which carries a payload of type signed_and_encrypted (see Fig. 6).

V. C-ITS Security: Experimentations and Validations

Defining standards for the design and implementation of the C-ITS security framework is necessary but not sufficient. Experimentations, testing and validation of ETSI standards are needed [24].

Recently, ETSI has developed security testing for the base standard (TS 103 097) within STF 481 and has developed the Test Conformance platform including 64 test cases which will be further extended with more errors and exception test cases. In the 4th ITS CMS ETSI Plug test held in Helmond, 17-27 March 2015, conformity testing of the ETSI security base standard (TS 103 097) was done using the ETSI conformance test tool. The interoperability test of various implementations in face-2-face configuration was performed [21].

Moreover, continuous work towards the development of standardized ITS were done in Field Operational Testing (FOT) projects in Europe, such as DRIVE C2X, Score@F and PRESERVE [10]. New pilot projects, like SCOOP@F in France, focus on large-scale testing and deployment. See [25] for a survey on C-ITS architectures and projects.

In the ISE project from SystemX IRT [11], the main focus is the design and implementation of a scalable and flexible C-ITS PKI, as we anticipate a progressive deployment over time (with multiple trust domains controlled by a root CA and multiple CAs within a trust domain). The implementation is fully compliant with ETSI standards and extensive performance evaluation is planned, based on a laboratory test environment including security penetration testing and based on experimentation and test analysis resulting from the SCOOP@F vehicle fleet and RSUs operation. We plan as well to perform scalability tests based on large scale deployment of the geo-replicated PKI.

VI. Conclusion

ETSI Release 1 base standards are now available or in final drafting stage, allowing the deployment of first basic applications for cooperative driving and traffic efficiency, supported by secured standardized messages such as CAM, DENM and SAM (Service advertisements to ITS–S applications or users) and I2V messages such as SPATEM, MAPEM and IVIM [20]. Stakeholders groups have developed a deployment Roadmap (see C2C-CC roadmap and guidelines for Day1 applications [12]). Nowadays, the implementation of the PKI issuing security certificates to the trusted C-ITS entities is essential to support the initial deployment of ITS in Europe (see [22] for a description of the organization and structure of the C2C-CC PKI). For such a large scale ITS communication system, with several hundreds of millions of ITS–S, the scalability and extensibility of the PKI is a major issue which needs to be addressed in future technical specifications and standards, as well as in organizational, legal and policy recommendations studies within Europe and in larger harmonization initiatives between different regions (EU, US, Japan, Australia...).

ETSI security framework should be extended based on industry requirements, e.g., to support certificates and PKI extensions, crypto agility, on-board security system requirements and assurance management (evaluation scheme). Furthermore, the Release 2 of ETSI security framework should be fully interoperable with operational ITS stations already deployed in the field (backward compatibility).

Acknowledgements

This research work has been carried out in the framework of the Technological Research Institute SystemX.

References

[1] http://www.etsi.org/technologies-clusters/technologies/intelligent-transport/cooperative-its
[2] https://standards.ieee.org/develop/wg/1609_WG.html
[3] IEEE 1609.2-2016, IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages.
[4] ETSI TR 101 067: "Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS); Release 1".
[5] ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)".
[6] ETSI TS 103 097: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
[7] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".
[8] ETSI EN 102 637-2: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".
[9] ETSI EN 102 637-3: "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service".
[10] PRESERVE project, https://www.preserve-project.eu/
[11] ISE project, http://www.irt-systemx.fr/project/ise/?lang=en
[12] Car2Car Communication Consortium, https://www.car-2-car.org/
[13] Transport Layer Security (TLS) Authentication using ETSI TS 103 097 and IEEE 1609.2 certificate, draft-v2-tls-cert-ETSI-IEEE.
[14] G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, "efficient and Robust Pseudonymous Authentication in VANET", ACM VANET 2007.
[15] ETSI TS 102 890-2: "Intelligent Transport Systems (ITS); Facilities layer function; Services announcement specification".
[16] IEEE 1609.3 Rev 3, IEEE Standard for Wireless Access in Vehicular (WAVE), Networking Services, 17 March 2015.
[17] ETSI EN 302 636-4-1: 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.
[18] IETF draft-petrescu-ipv6-over-80211p-02
[19] ETSI TS 102 687: Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part.
[20] ETSI Draft TS 103 301: Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for I2V messages.
[21] Result summary of 4th ITS Cooperative Mobility Services Plugetst, Sebastian Mueller, ITS Workshop, Helmond, 27th March 2015.
[22] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, JP. Stotz and B. Lonc. A generic public key infrastructure for securing Car-to-X communication In ITS World Congress, 2012.
[23] "C-ITS Security: Standards and experimentations" published in Journées Nationales des Communications dans les Transports.
[24] R. Moalla, H. Labiod and B. Lonc "C-ITS Security: Standards and experimentations", JNCT 2013.
[25] A. Boudguiga, A. Kaiser and P. Cincilla "Cooperative-ITS Architecture and Security Challenges: a Survey", 22nd ITS World Congress, 2015.