Cooperative ITS Security Standards: Implementation, assessment and next challenges

Brigitte Lonc, Farah Haidar, Denis Filatov

Virtual ITS European Congress, 9-10 November 2020

Paper number ITS-XXXX

Cooperative ITS Security Standards: Implementation, assessment and next challenges

Brigitte LONC[1*], Farah HAIDAR[1,3], Denis FILATOV[2]

1. Renault, firstname.lastname@renault.com, Guyancourt, France
2. Filatov DV, denis.filadov@fillabs.com, Nice, France
3. IRT SystemX, farah.haidar@irt-systemx.fr, Plaiseau, France

Abstract

In the near future connected will interact with each other, the road environment and the Cloud or edge servers, through Cooperative Intelligent Transportation System (C-ITS). C-ITS will significantly improve road safety, traffic efficiency and the driving comfort. Security and privacy protection are key elements for C-ITS safety-related services. Authenticity and integrity of the communications are ensured using digital signatures and a Public Key Infrastructure (PKI) that delivers pseudonymous certificates to vehicles, Road Side Units (RSU) and Central ITS-Stations (CS).

In this paper, we present recent ETSI standardization progress, the PKI design and the overall C-ITS Trust System for Day1 deployment in Europe and we discuss open challenges for future new services and support of autonomous driving. An overview is given on interoperability testing of base standards and on pilot experimentations/ deployments in Europe dealing with trust and privacy management.

Keywords:

C-ITS, SECURITY, STANDARDS.

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), vehicle-to-infrastructure (V2I) and Vehicle-to-Centre (V2C) wireless communications using various technologies, such as short-range wireless communication, cellular wide area networks or other broadcasting network (e.g. GNSS). Based on the exchanged messages, the C-ITS applications will first provide better awareness to the driver via the road hazard warnings and traffic information, and later support cooperative driver systems and more automatic systems for the Connected, Autonomous Vehicles (CAV).

Despite the many potential benefits of C-ITS, the associated wireless communications raise security and privacy issues which, if not addressed, could jeopardize their deployment. As the main target of C-ITS and CAV is to highly contribute to primary road safety helping to avoid accidents (collision avoidance) and to enhance the support for secondary road safety functions (pre-crash), a good balance

between security, privacy and performances of Safety related applications has to be found.

For securing C-ITS communications, the best available solution is to use asymmetric cryptography, and this requires the set up of 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, collectively named V2X (Vehicle-to-Everything), and to provide necessary communication interfaces for each entity of the C-ITS network to access to the security management services provided by the Certificate Authorities (CAs) within the PKI.

Another major issue to consider is the user privacy. Any security credential management system must consider a privacy preserving scheme to protect user private information, such as user/vehicle identity, trips or behavior, 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 in ETSI and the European C-ITS trust model. Section III describes ETSI PKI design and data models for secured messages and certificates. Section IV presents the assessment and interoperability tests done in ETSI Plugtests and European pilot and deployment projects. s. Open issues and challenges for the new, extended set of C-ITS services is discussed in Section V. Conclusion is given in Section VI.

C-ITS Security: Standardization Activities

ITS Security Framework

To achieve C-ITS interoperability, the development of communication security standards is paramount. For this purpose, dedicated working groups within standardization organizations address security and privacy issues, for instance the ETSI TC ITS WG5, the IEEE 1609.2 working group.

IEEE 1609.2 standard defines security data structures and especially secure message formats, and the processing of those secure messages within the DSRC/WAVE system ([8]): the 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.

In Europe, ETSI TC ITS WG5 deals with privacy, data protection and security aspects in ITS. ETSI ITS security standards cover current ITS security needs and objectives, based on Threat and Vulnerability Risk Analysis (TVRA) report. A critical feature of this security framework is to include privacy protection for users and vehicles of C-ITS systems, e.g., using pseudonyms certificates for s secure communications and changing them regularly. Table 1 below gives the mapping of generic security services to security architecture and associated standardized services and interfaces.

Table 1:mapping of generic security services to architecture and standards

Service category	Security service	Standard Reference
Enrolment	Obtain/Remove/Update Enrolment Credentials	TS 102 941

Authorization	Obtain/Update Authorization Ticket	TS 102 941
Message Signature Service	Authorize Single Message Validate Authorization on Single Message	TS 102 940 TS 103 097
Data Encryption Service	Encrypt/Decrypt Single Message	TS 102 940/TS 103 097
Replay Protection services	Replay Protection Based on Timestamp	TS 102 940/ TS 103 097TS 103 097
Plausibility service	Validate Data Plausibility	TS 102 940/ TS 103 097
Security Associations management	Establish/Remove/Update Security Association Send/Receive Secured Message	Supported by TLS 1.2 or TLS 1.3 amended with IETF RFC proposal for TLS extension with ITS certificates
Integrity services	via checksum	Supported at MAC layer using IEEE 802.11 Forward Error Correction
Accountability services	Record incoming/outcoming message	not supported in security standard
Remote management	Activate/Deactivate ITS transmission Deactivate ITS transmission	not supported in security standards
Report Misbehaving ITS-S	Report Misbehavior at ITS-S Detection and Prevention of Misbehavior by Misbehavior Authority	not supported in Release 1 for future extension

As part of ETSI ITS Release 1, a major achievement 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 2.

Table 2: ETSI ITS Security standards

Standard Reference	Title	Status
TR 102 893	Threat, Vulnerability and Risk Analysis (TVRA)	v1.2.1 Published Updated with GEONET risk analysis
TS 102 731	Security services and architecture	v1.1.1 Published
TS 103 097	Security header and certificate formats	v1.3.1 Published (2017-10) extensions for compliance with the European Certificate Policy
TS 102 940	ITS communications security architecture and security management	v1.3.1 Published (2018-04) extensions for compliance with the Certificate Policy
TS 102 941	Trust and privacy management	v1.3.1 Published (2019-02)
TR 103 415	Pseudonym change strategies technical report	v1.1.1 Published

C-ITS Trust Model and Governance

To foster large deployment of C-ITS services, it was needed that multiple Root CAs are present within a single trust model, using the same common Certificate Policy (CP) [7]. In such situation, a trust relationship between the Root CAs shall be guaranteed in such a way that ITS-S using certificates coming from different PKIs can still communicate. In Europe, this interoperability is guaranteed by the top-level entities specified in the CP Release 1.1 (see Figure 1): - the **Certificate Policy**

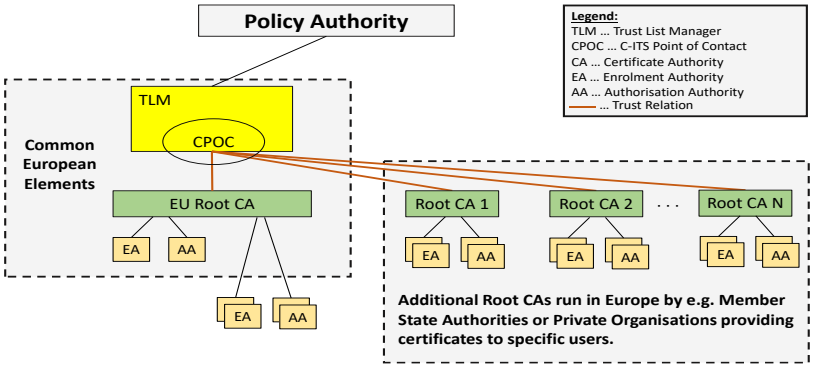

Fig. 1 European Common Trust Model, source CP Release 1.1 from DG MOVE

Authority (CPA) is designating and authorizing the TLM (Trust List Manager) and CPOC (C-ITS Point Of Contact). It decides which Root CAs are trustable and approve/revoke Root CAs certificates in the TLM. The CPA will be composed of representatives of public and private stakeholders. - The **CPOC** is a unique entity in charge of collecting the trusted Root CAs certificates and providing them to the TLM. It also provides the ECTL to interested entities in the system. - The **TLM** is creating and signing the ECTL, which consists of the list of trusted Root CAs certificates and TLM certificates.

Security for V2X communications

ETSI security concept uses long-term certificates for authentication of ITS–S, named *Enrolment Certificates* (EC) and short-lived anonymized certificates for V2X communications, named *Authorization Tickets* (AT) or *pseudonym certificates*.

Using the same pseudonym certificate allows tracking of vehicles. Users privacy is protected by a pseudonym scheme i.e., changing frequently the pseudonym certificates (AT) based on distance or time or number of sent messages. 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 pseudonyms to each ITS–S.

ETSI C-ITS PKI Design

ETSI PKI design is presented in [1]. and is depicted in Figure 2. The Root Certificate Authority (RCA) is the start point of the certificate trust chain, it signs the certificates of other authorities (Authorization

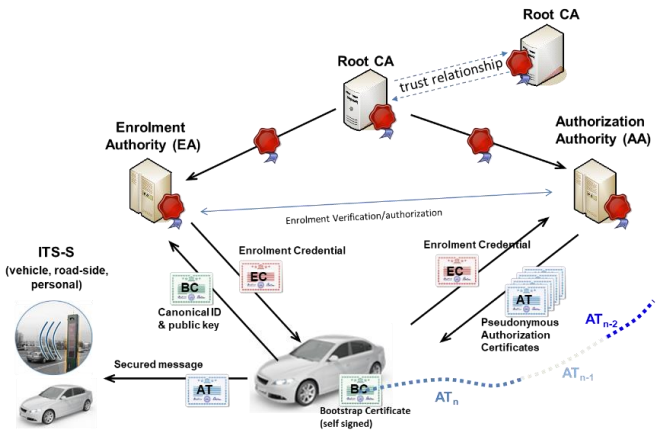

Fig. 2 ETSI ITS PKI

Authority (AA) and Enrollment Authority (EA)) and produces and maintains the Certificate Revocation List (CRL), the list of revoked authorities, and the Certificate Trust List (CTL), the list of its subordinate certificate authorities with their access points. In the European Trust model, the RCA can be managed by either a Public or a Private organization that complies to the CP. The number of RCAs deployed in Europe should be limited to reduce operational costs and provide higher privacy.

The Enrolment Authority is the authority which delivers Enrollment Certificates (ECs) and validates Authorization Tickets (ATs) requests. The Authorization Authority provides Authorization Tickets (ATs) to ITS-Ss. ATs are used by ITS-Ss to sign V2X messages. The Distribution Centre (DC) gives access to ITS-S to trust lists (CRL, CTL).The revocation of compromised authorities is based on the use of a Certificate Revocation List (CRL). CRL contains the certificate digests of revoked EAs and AAs by the RCA and possibly the digest of the RCA itself. A work item on defining the protocols to distribute up-to-date CRLs within the C-ITS in an efficient way has started.

For ITS-S revocation, when the EA is informed that an ITS-S is compromised, it refuses all validation requests coming from the AA for that specific ITS-S. As a result, the AA refuses to provide new ATs to the ITS-S, leading to exclude it from the C-ITS. Currently, ETSI ITS standards do not specify any technical solution to implement the active ITS-S revocation.

PKI management requirements and protocols

In a nutshell, the interfaces and protocols to support security management of trusted ITS-S are shown in figure 3 and are specified in ETSI TS 102 941. Machine-to-machine communications with the EA, AA, and DC components use HTTP/1.1 over TCP-IP (GET or POST). No supplementary cryptographic layer such as TLS is required. Parameters for the POST requests and responses, and complete path for GET requests are described in the corresponding messages descriptions.

For user interfaces, the European CP requires that access should be restricted only to authenticated operators.

At initialization, a trusted ITS-S shall be configured during manufacturing with its personalized credentials (Canonical ID, Canonical Key) and preconfigured with initial trust information such as its own Trust Anchors (i.e. its RCA certificates, EA/AA certificates and access point and DC access point) and trust information for interoperability (TLM certificate, CPOC access point, ECTL…). Then the process to reach the exchange of signed V2X messages between ITS-Ss is depicted in Figure 4.

An ITS-S first requests its EC to the EA using its Canonical ID and Canonical public key for authentication. After verification of the information provided by the ITS-S, the EA sends back the EC to the ITS-S. The EC is used to request pseudonym certificates (ATs) to the AA: when an ITS-S requests an AT, it sends in the request message its encrypted identity using the EC identifier (i.e. HashedId8 of the EC) and the EA identifier. The AA receives the AT request, reads the EA identifier and checks the EA access point in the CTL and the EA current status in the CRL. Then asks the EA to validate the AT request. The EA checks the ITS-S EC and validates (or not) the request. If the request is validated, the AA generates and sends the AT to the ITS-S. The ITS-S then uses this AT to sign the V2X messages it broadcasts on the short-range wireless interface (e.g. ITS-G5 network).

PKI management protocols were initially specified in ISE project [1] and used in SCOOP@F pre-deployment project[2] for validation, user experimentations and cross-tests with other countries. Security and privacy objectives have been identified and their fulfillment in protocols specified in ETSI TS 102 941 are explained in Appendix.

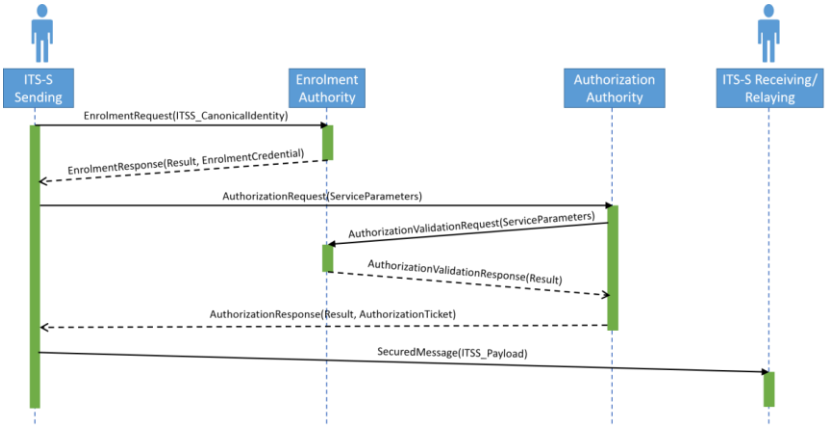

Fig. 3 ITS-S enrolment-authorization process

Secure Message Format Specification

ETSI TS 103 097 specifies the format for secured messages and for certificates. Fig. 5 depicts the general structure of a security envelope for signed messages. The document specifies Security profiles for Cooperative awareness message (CAM), Decentralized Event Notification Message (DENM) and a generic profile and defines profiles for certificates, e.g. TLM, RCA certificates (and link certificates), 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. Certificate omission allows to reduce the network bandwidth usage, at the expense of a higher latency time for message verification by the receiver. For this purpose, ETSI TS 103 097 provides a *SignerIdentifier* field containing the certificate ID of the AT specified as the 8 bytes certificate digest with sha256.

In the recent published version (ETSI TS 103 097, V1.3.1), the definition of data structures has been aligned with IEEE 1609.2 [12], thus defining the European profile.

Fig. 4 Signed Message with Pseudonym certificate

1 https://www.irt-systemx.fr/en/project/ise/ and 2 http://www.scoop.developpement-durable.gouv.fr/

ITS Stations, roles and application permissions

To enable the trustful and safe ITS network and make full use of available ITS applications, services and capabilities, the ITS station needs to obtain specific credentials (ATs) from the Authorization Authority. These credentials, in the form of cryptographically signed certificates, are used to assure any receiving ITS-S that the sender can be trusted and has the necessary permissions to send the particular service-specific information. Users in the ITS system may have different types, roles and different authorization levels (e.g. personal vehicles, emergency vehicles, Road-Side Units (RSU), fixed or mobile roadwork units etc.).

In ETSI security framework, the AT indicates the permissions of the certificate holder, i.e., what statements it is allowed to make or what privileges it is allowed to assert in a signed message broadcasted on the communication link. In ETSI architecture, ITS-Application Identifier (ITS-AID) is a unique identifier allocated in the ITS-AID registry to identify a given message, service or application. In TS 103 097, the overall application permissions granted to an ITS station are expressed in its certificate using ITS-AIDs and SSPs (Service Specific Permissions). The certificate format allows a certificate to contain multiple (ITS-AID, SSP) pairs. 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 for this application. For example, there are SSP bit values 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 etc.) or for a specific RSU (e.g., tolling zone).

Each service shall have an associated ITS-AID aka PSID (Provider Service Identifier). The sender AT shall contain the field with this ITS-AID used to send secured messages for the relevant service. The actual message content may be allowed using Service Specific Permissions (SSP).

The structure and the actual meaning of SSP is service-specific and shall be defined in the security profile. The service specific permissions granted to the ITS-S shall be accorded with the permissions of the AA and RCA. The process for checking payload consistency with PSID/SSP values is specified by the application standard.

Open issues and challenges for Day2 and beyond

E2E Hybrid communication security for C-ITS

To foster larger deployment of C-ITS services and cover more road users, a wider scale of C-ITS V2X connectivity is required supporting various cooperative systems (Central ITS-Stations, road devices such as RSUs, traffic signal controllers…, vehicles, smart devices), many C-ITS architecture options which may provide suitable communication standards and ITS hybrid communication using long-range cellular communications (3G, 4G/LTE and 5G) as well as short-range wireless (ITS-G5). Therefore, a solution for End-to-End (E2E) hybrid communication security is needed.

Providing E2E security for C-ITS is a real challenge due to the variety of potential communication technologies, the multiple interfaces and protocol stacks and the integration of standardized and

non-standardized communication chains using legacy networking solutions (e.g. VPN, TLS …).

ETSI security design allows to apply security at different layers (Network/ Transport, Facilities) and should basically support different use cases for C-ITS message signature, for instance: the trusted ITS-S is the source of data and is signing it before sending it on the C-ITS Network (DENM broadcasted by RSU), the trusted ITS-S is signing the message on behalf of a Central ITS-S (e.g. the Traffic Management Centre is sending Variable Message Signalling to the RSU and grants it permis

sions to send signed safety messages over ITS-G5 such as IVI message), the trusted ITS-S is acting as a transparent relay for the distribution of the information and may forward the message signed by the originating ITS-S e.g. using cellular or Short-range communication.

DENM messages are used in real-time safety applications, such as collision avoidance applications (ref ETSI TS 101 539-1, 2, 3 [6]). In some critical safety situations, the latency time of the exchanged DENMs shall be guaranteed. The latency time of the whole E2E system is specified in ETSI standards, e.g. a maximum E2E latency time of 300 milliseconds at a maximum CAM/DENM frequency of 10 hertz is required. Consequently, if DENMs are transmitted over multiple chains of communications, the DENM message shall only include one message signature preferably applying signature at GeoNetworking level and shall not apply several signatures at Facilities and at GeoNetworking levels. Otherwise the receiving Vehicle ITS-S will drop these messages as they do not satisfy the performance requirements for safety applications. The age of data received by the vehicles is indeed a critical aspect of the required data quality (as well as integrity, accuracy and confidence level of the information).

Misbehavior detection and revocation

The misbehavior detection goal is to monitor ITS communications and detect faulty or malicious ITS-Ss to identify and exclude them from the system. It will be a must to support new emerging C-ITS applications (Day 2 and beyond). Besides Day 1 applications, messages will be more safety relevant and the system must be robust to faulty or malicious devices that may send erroneous or forged information.

The misbehavior detection system relies on two main parts: one embedded in the ITS-S (e.g. vehicles) for monitoring exchanged information plausibility and report detected anomalies and the other one in the Cloud that receives misbehavior reports and takes a decision based on collected reports analysis and is named Misbehavior Authority (MA). Local detection mechanisms in ITS-S are using plausibility and consistency checks on the received safety messages and optionally using the vehicle environment such as its Map or Local Dynamic Map (LDM) and the vehicle sensors information. The misbehavior may also be detected by the EA or AA, if it receives abnormal solicitations from an ITS-S.

The misbehavior detection arises many privacy issues: first when sending a misbehavior report, the privacy of the reporter and the reported ITS-S should be preserved. Moreover, the MA needs a means to link pseudonym identities (either linking pseudonym certificates with their real long-term certificate or using another mechanism) for both investigation and revocation purposes.

The challenge is to develop standards that allow flexible misbehavior detection frameworks, as

detection algorithms will have to be improved continuously (e.g. Machine Learning based detection in local or global entities), without disturbing already deployed ITS stations.

Methodology and Process for permissions management in future C-ITS services

Every C-ITS service shall use an associated security profile. To support the initial C-ITS safety related services as defined in the Basic Set of Applications (ETSI TR 102 638 [2]), ETSI TS 103 097 has defined security profiles for CAM, DENM, and the generic security profile to be used for other secured messages. When specifying a service, the relevant group has to specify the associated security profiles and define appropriate application-level permissions, such as in [3], [4] and [5]. Application permissions of the Sender is determined using the ITS-AID and SSP. The group in charge of the service specifications shall reserve the ITS-AIDs and specify the meanings and the allowed value ranges used for each SSPs related to a given ITS-AID defined in the standard or specification.

Development of new C-ITS applications requires a well-structured process and guidelines for the definition of security profiles and the sender or receiver security characteristics. There is a strong requirement to provide the set of principles that could be used by applications specifiers for future extensions and maintenance of the standards and specifications to achieve necessary interoperability, performance and security level.

Due to the very specific and complex ITS ecosystem, the development of a well-structured process and methodology for management of security profiles and permissions is a real challenge. It will ensure proper and trusted operation of these services with better relations between formal permissions and real application needs. It will enable the support of more stakeholders, more cooperation between ITS systems/subsystems (Central ITS-S, Road devices, RSUs, vehicles and other kind of road users e.g. VRUs, pedestrians…), making use of the interoperable, trusted technology and broaden the deployment of the developed systems.

C-ITS Security standards implementations and assessment

As C-ITS deployment has started with the broader support of stakeholders [3] [4], interoperability and compliance to base standards is becoming key for the successful deployment in Europe.ETSI has organized two Plugtests on ITS security in 2019. The ITS CMS6 Plugtests in March was dealing with conformity and interoperability testing of security communications and ITS PKI management interfaces (with end-entities and between CAs). The scope of ETSI ITS CMS7 Plugtest[5] was extended to cover the key elements of the CCMS. For this second event, the European Commission acted as C-ITS contact point (CPOC) and TLM for the european C-ITS Trust domain. The entire process via the CPOC/ TLM has been successfully tested, e.g. sending RCA certificates to the CPOC, signing the ECTL, uploading of the new ECTL, revocation of RCA.

In SCOOP@F project, a validation and production PKI composed of one RCA, 3 Long-Term CAs

3 https://www.car-2-car.org/ and 4 http://c-its-deployment-group.eu/

5 https://www.etsi.org/events/1593-plugtests-2019-itscms and 6 https://intercor-project.eu/pki-security-testefest/

(aka. EAs) and one Pseudonym Certificate Authority (aka. AA) are deployed since September 2016. They have been implemented based on previous versions of standards and used for the validation and experimentation of C-ITS Day1 use cases on test open roads. SCOOP@F and InterCor project where 4 member states are cooperating (Netherlands, Belgium (Flanders), UK, France) have organized a PKI security TestFest[6] running on an Open Roads test site on highways A4-A344 around Reims, where a number of services were available (e.g. Roadworks Warning using DENM messages, V2V warning "Obstacle on the road"), and this event allowed to test ITS-G5 communications interoperability with multiple foreign PKIs.

C-ROADS platform is an EU-supported initiative with 16 member states and 7 Associated members which aims at coordinating and producing common specifications for the implementation of interoperable C-ITS services across Europe. C-ROADS TF1 Security[7] has published a security report with guidance, PKI set-ups plans and test scenarios using ETSI base standards. Security/PKI assessment tests using new version of ETSI standards are planned in 2020.

In ISE project, scalability and performance assessment of C-ITS PKI as well as performance tests of pseudonym change management and pseudonym refilling via ITS-G5/RSU were done in test laboratory and while driving on test tracks [9], [10].

Conclusion

ETSI standards have been improved and a new version of security standards was published recently. Improvement includes the support of crypto-agility (i.e. support of different ECDSA curves and key sizes for signature) and flexibility for future new crypto-algorithms, extensions to fulfill the requirements of the European CP. E.g. improvement of permissions formats, specification of CA certificates with constraints management (Regions, PSID/SSPs), adding extensions such as CTL and CRL format and certificates profiles (TLM, link …). Since mid-2017, the harmonization between ETSI and IEEE 1609.2 standard was done and ETSI TS 103 097 V1.3.1 was aligned with IEEE 1609.2.

ETSI ITS initial set of standards is currently being updated for Release 2 and the ETSI security framework will have to be extended to integrate required mechanisms for Misbehavior detection and revocation of trust and to develop end-to-end hybrid communications security architecture,

Eventually, there is a need to build a framework and process to develop security profiles for interoperable and trustable applications, e.g. assist developers to assess security risks for different types of ITS-Stations, to define security profile for the application, to properly define useful SSP structure etc. All these planned standard extensions are critical to enable a broader deployment of V2X communications in C-ITS, CAV and future mobilities.

Appendix

6 https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/20190125_TF1_Security_report_v1.4_final.pdf

Table A.3: security and privacy considerations in EC Request/EC Response protocol

Security req.	EC Request	EC Response
Identification	Identity is ensured by the itsId present in the request. For the first enrolment of the ITS-S to the EA, itsId contains its CanonicalId. For the following re-enrolments of the ITS-S, the identity is ensured using the current EC identifier (i.e. the itsId contains the HashedId8 of the EC).	Identity is ensured by the signer identifier of the SignedData structure (contains the HashedId8 of the EA).
Authentication & integrity	Ensured by the signature and verified by checking the signature against the canonical public key associated to its CanonicalId (for the first enrolment) or checking signature using the EC verification public key for the following re-enrolments of the ITS-S.	Ensured by the signature and verified by checking the signature against the verification public key of the EA.
Authorization	Ensured by the verification of the values set to the Service-Specific Permissions (SSP) for the corresponding PSID (i.e. the PSID value of the Secured Certificate Request service) in the EC of the ITS- S.	Same as EC Request, using the EA certificate.
Confidentiality	Ensured by encrypting the request with the session encryption key (AES key) using ECIES with the public encryption key of the EA.	Ensured by encrypting the response with the same AES session encryption key provided in the request. If this key wasn't valid, confidentiality isn't ensured, but no personal information is returned.
Anonymity	Anonymity of the requestor toward an external attacker is ensured by the confidentiality of the request and its signature. Anonymity of the requestor toward the EA isn’t a concern (EA must know and recognize the requestor).	Anonymity of the requestor toward an external attacker is ensured by encryption of the response where possible.

Table A.4: security and privacy considerations in AT Request/AT Response protocol

Security req.	AT Request	AT Response
Identification	Identity is ensured by the signer identifier present in the encrypted EC signature structure of the request	Identity is ensured by the signer identifier of the SignedData structure (contains the HashedId8 of the AA).
Authentication & integrity	Ensured by the signature and verified by checking the signature against the public keyassociated to this signer (found in the corresponding EC). The signature indirectly covers the verificationKey and encryptionKey elements, by their digests (second pre-image resistance of the hash function, which is greater than the collision resistance used in signatures). The AA cannot verify the signature, only the EA can do it, but the AA can verify the requested permissions, and can verify that the HMAC of the public keys match the given keyTag.	Same as EC Response (using verification public key of the AA).
Authorization	Ensured by the verification of the values set to the SSP for the corresponding PSID in the EC.	Ensured by the verification of the values set to the SSP for the corresponding PSID in the AA certificate.
Confidentiality	Ensured by encrypting the request with the session encryption key (AES key) using	Same as EC Response

	ECIES with the public encryption key of the AA.	
Anonymity	Anonymity of the requestor toward an external attacker is ensured by the encryption of the request and its signature. Anonymity of the requestor toward the AA is ensured by the additional encryption of the signature and the signer. Anonymity of the requestor toward the EA isn't a concern (the EA must know and recognize the requestor).	n/a
Unlinkability	Ensured by encryption. Unlinkability of the ATs toward the AA is ensured by the additional encryption of the signature and the signer. Unlinkability of the ATs toward the EA is ensured by hiding the final public keys to certify from the EA. To prevent tracking with its IP address, the ITS-S should use pseudonym IPv6 address which are changed frequently. Change is triggered after receiving the response	Anonymity of the requestor toward an external attacker is ensured by the absence of personal identifiable information returned when no encryption is possible, and by encryption of the response where possible.

References

1. Lonc, B., Cincilla, P., 2016. Cooperative ITS security framework: Standards and implementations progress in Europe, IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM). Coimbra, Portugal
2. ETSI TR 102 638. Intelligent Transportation Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, V1.1.1 (2009-06)
3. ETSI EN 302 637-2. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1 (2019-04)
4. ETSI EN 302 637-3. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, V1.3.1 (2019-04)
5. ETSI TS 103 301. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services V1.2.1 (2018-08)
6. ETSI TS 101 539-1, 2, 3. Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS), V1.1.1 (2013-08)
7. CP Release 1.1 2018. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1.
8. IEEE Std 1609.2™-2016-2017: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".
9. Cincilla P., Hicham O. and Charles B., 2016., Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios, *2016 IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, 2016, pp. 1-8.
10. Haidar, F., Kaiser, A., Lonc, B. and Urien P., 2019. C-ITS PKI protocol: Performance evaluations in a real environment, 2019 IEEE/IFIP 15th Wireless On-demand Network Systems and Services Conference (WONS), Wengen, Switzerland, 2019, pp. 1-5.