Position paper on C-ITS security and privacy

CAR 2 CAR Communication Consortium

Partners of the C2C-CC

Document information

Number:	602 002	**Version:**	1.0.0	**Date:**	2015 – 01 – 19
Title:				**Document Type:**	
Release Status:	released				
Status:	Draft – Work in progress				

Author:

Company /Institute	Author	Chapter
Volvo Car Corporation	Henrik Broberg	
Continental	Stefan Römmele	
Fraunhofer SIT	Norbert Bißmeyer	

Approval:

Function	Name, Company	Date	Signature

Outstanding Issues

Issue	Author	Chapter
Terminology		

Changes since last version

Title:	
Explanatory notes:	

Issue	Rev.	Date	Changes	Edited by	Approved
	100	2015-01..			
		2015-02-	TC comment resolution and position on certification and target of evaluation (TOE) added.		

Content

List of figures

No table of figures entries found.

List of tables

No table of figures entries found.

1 Introduction

1.1 Abstract

Cooperative intelligent transport systems (C-ITS) provides great promise for benefits in safety, environmental, economic and convenience, but has an inherent risk of that the information shared is misused to cause false warnings or other disruptions, hence causing the user to reject the system.

The day 1 C-ITS deployment is limited to warnings but is a significant investment to several stakeholders. The consensus in Europe has been to avoid the risk users rejecting the system by providing means for a sender to provide evidence of its role in the C-ITS system. (Authorisation) and to what extent the system is secured against tampering. There is also the consensus that all interested parties need to agree to the terms and conditions for the use of the information.

Authorization implies identification that is in conflict with vehicle user privacy that also is deemed as an important objective for user acceptance of the system. To this address this problem pseudonyms has been chosen to serve as identies in the authorisation rather than an identity directly linked to the user.

There has been significant investment in EU founded research projects to analyse and propose solutions the automotive industry. The results have been channelled into ETSI standards and CAR 2 CAR Communication Consortium (C2C CC) documents. A common minimum security level for sender behaviour has been agreed between the C2C CC members. The use of information and receiver behaviour has been out of scope for the standardisation work and need to be addressed by relying parties.

2 Car 2 Car Security Design overview

In order to minimize the risk of flaws in the security design, established design patterns and technology has been adopted to the constraints for the automotive context, like limited bandwidth over the air, power and resource constraints of embedded systems. Public key cryptography is used to provide integrity of data and origin of messages. The messages are sent in clear text to the community, but electronic signatures and public key certificates are attached to messages provides community members the ability to verify that the information is unaltered and the privileges of the originator is matching the information.

Security by design and Privacy by design has to be done at state of the art technology. This refers to ITS Stations as well as to the In-vehicle Network (IVN) connected to the ITS – Vehicle Station and the credential management system which creates the certificates for the ITS Stations.

The ITS stations in the field are dependent on provisioning of public key certificates from a central IT infrastructure called public key infrastructure (PKI). Public key certificates contain the public key used to verify messages and meta data like validity information, the privileges and a tamper protection level. In addition to the technical infrastructure the PKI provide administrative services to manage the lifecycle of the system. Typical services provided in a PKI system are (from [AD-1]):

- Registration service: verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation service.
  NOTE 1: This service includes proof of possession of non-CA generated subject private keys.
- Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service.
- Dissemination service: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the CA's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
- Revocation status service: provides certificate revocation status information to relying parties (example certificate revocation lists or online certificate status protocol)

The public key infrastructure is a hieratical system with a top entity, a root certificate authority, and several subordinate certificate authorities (CAs). A specific application to the automotive context is to use pseudonyms instead of identities in order to limit tracking of users. This influences the PKI architecture to have two different subordinate CAs, Long Term CAs responsible for enrolment and Pseudonym CAs responsible for issuing pseudonymous certificates.

The scope of standardisation is limited to design of sender behaviour and managing risk of vulnerabilities in sender implementations. Any design related to receiver behaviour and managing risk of vulnerable receiver implementation is up to all parties using the information.

The design adds significant overhead to the messages over the air, complexity of the embedded implementation and running costs for the PKI.

2.1 Known limitations in the day 1 deployment

There is no standardised design for revocation management; this is left to the application designer to use the information accordingly

There is no standardized design for misbehaviour reporting

3 Certification policy for C2x applications

In order to provide confidence for the recipient of a message, there has to be clear rules for the management of credential both within the public key infrastructure as well as in the on-board units. This chapter outlines the rules and responsibilities that will be used for the different certificate authorities (CAs) and the on-board units.

From [AD-3]:

"According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements."

Policy identifiers are used to identify different policies in order for the relying party (the receiver) can determine the suitability and trustworthiness for a particular application.

Refer to [AD-1] and [AD-3] for more information on certificates and certificate policies.

ITS Application ID (ITS-AID) is under the administration of ISO and the current list can be found at:

http://standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers/TS17419_ITS-AID_AssignedNumbers.pdf

The certification policy is defining the requirements for joining the system whether you are a CA or an ITS station. A certificate practice statement is the evidence provided to the authority how the requirements are fulfilled. This section captures key decisions that are going to be the basis for certification policy writing, a craft requiring formally documented skills.

3.1 Structure

The certification policy shall follow the outline of PKIX Certification Policies (IETF RFC 3647) and the intention of ETSI EN 319 411-2 V1.0.0 (2012-04):

3.2 Limitations for use

The receiver must agree to not use information to reveal the identity of the sender.

3.3 Responsibilities

3.3.1 Revocation

Misbehaviour in the system can lead to revocation on temporary or permanent basis (for RCA, LTCA, PCA or ITS stations). Revocation status shall be available 24/7 over the following interfaces;

To be confirmed.

Information for resolving the pseudonym shall be retained for the validity period + 3 months.

3.3.2 Misbehaviour reporting

Interfaces to the ITS community and the public shall be available 24/7.

Community members have the responsibility to deliver misbehaving reports on CAs within 1 h.

Misbehaving reports from ITS stations should be delivered with best effort for day 1 deployment.

Community members have the responsibility to report vulnerabilities discovered in the design, implementation or configuration of CAs or ITS stations that can affect the security level to the revocation management service within 1 work day. Vulnerabilities shall be reported and rated in a scheme determined by the revocation management service.

3.3.3 Detection

Discovery of vulnerabilities (flaws) in a make or model shall lead to demotion of the trustworthiness of the certificates issued before the vulnerability is fixed.

3.4 Security considerations

3.4.1 Cryptographic policy

Cryptographic secure solution (meaning brute force attacks are infeasible) has been selected to counter manipulation of messages over the air.

Flaws in cryptographic design are not considered in the day 1 design (only one crypto suit available) to reduce complexity and cost.

Currently a task force is investigating change to this policy for the day 1 deployment to harmonize with infrastructure policy (i.e. crypto agility).

3.4.2 Level of privacy against PKI insider

The C ITS G5 PKI infrastructure is divided into Root CA, Long-term CA and Pseudonym CA. The operator of the Root CA is not allowed to also operate sub CA's like LTCA or PCA. In case that an operator of a LTCA also operates a PCA it has to be assured that this operator is not breaking the privacy and allocating pseudonyms to long term certificates. This has to be prevented for organizations as well as for individual persons. Additionally a system (technical, organizational or related policies) has to be audited by an independent auditor 1 time per year

Any information with likability between long term identity and pseudonyms need to be treated as highly confidential.

3.4.3 Level of tamper proofing of ITS -stations

ITS-stations tamper proofing is focusing on protecting the private keys but also making sure the software is authentic and least checking that sensor data (including gps data) is plausible.

The requirements for day 1 deployment are specified in "protection profile for V2X box" using common criteria terminology and structure to model the requirements.

The ITS station manufacturer shall prove that the system is trustworthy in a security target; this may include manufacturing and bootstrapping.

The concept allows for different security levels for the in vehicle network starting at plausibility checks, but with the expectation that the security level increase in the coming years.

In general the receiver behaviour is excluded from the standardisation within car 2 car communication consortium, but communication security is an exception to this rule in order to follow best practice in the security community. The exception is justified to be able to use the existing expertise, people and labs in the security community for the certification of the system in order to save cost and improve quality. The requirements on receiver behaviour are minimised. For example in order to validate a message, receiver needs to have tests to sort valid messages from invalid message correctly. How that is done is not in scope.

3.5 Certification scheme

The module shall be certified according to a commercial certification scheme modelled after but not conforming the common criteria evaluation scheme.

3.6 Business continuity management and incident handling

All parties have a responsibility to notify without delay of incidents. Examples of incidents are loss, theft, or potential compromise of any private keys.

Disaster recovery mechanisms shall not depend on the PKI response time.

4 Appendix 1 – References

4.1 List of terminology

Not defined yet. Harmonization of HTG#6 terminology on PKI services is to be done.

4.2 List of abbreviations

EC	European Commission
C-ITS	C-ITS in this document refers to cooperative systems, in other documents it may mean Central ITS and denote a central database.
EU	European Union
GPS	Global Positioning System
ITS	Intelligent Transport System
LTCA	Long term identity certification authority
OEM	Original Equipment Manufacturer
PCA	Pseudonym certification authority
RCA	Registration certification authority

4.3 Applicable documents

[AD-2] ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates
http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

[AD-3] Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates
http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/01.00.00_20/en_31941102v010000c.pdf

[AD-4] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
https://www.ietf.org/rfc/rfc3647.txt

■ End of Document ■