C-ITS Platform

Working Group 5: Security & Certification

Final Report

v1.0

Contents

1 Objectives of the Working Group

The objectives of the C-ITS Platform working group on Security & Certification were to investigate the main security aspects in Cooperative Intelligent Transport Systems (C-ITS), which must be addressed to support a secure and safe deployment of C-ITS in Europe. For this purpose, various experts in the C-ITS community and deployment initiatives from different categories of stakeholders (e.g., vehicle and equipment manufacturers, Member States, infrastructure operators, standardisation experts) participated to the C-ITS Platform meetings of the working group. A number of relevant working items were identified in the early phase of the activities of the working group. The working items were selected with the consensus of the WG5 participants on the basis of the need to support deployment of C-ITS in Europe.

One of the first selected work items was the definition of the trust model for C-ITS in Europe to support an European harmonized approach for the provision of trust among the main participating entities of C-ITS (e.g, C-ITS stations, C-ITS applications, etc.). The European C-ITS trust framework has been defined as E-SCMS (European C-ITS Security Credential Management System). Revocation of trust was another work item suggested by the WG5 participants to ensure that non-compliant C-ITS stations or misbehaviour are addressed. Another work item was to tackle the topic of crypto-agility and updateability, which was chosen to ensure that the security framework in C-ITS have adequate flexibility in the lifetime of C-ITS stations and applications. The last work item is the overall C-ITS compliance assessment process to ensure that only valid C-ITS stations can be deployed in the field.

Each work item had the objective to produce a technical report, where all the work group experts and involved organisations contributed with their point of view. All reports and outcomes of the working group are based on consensus and have been endorsed by all participating experts (during the work process the different views have been presented accordingly in the reports if no consensus was able to be reached on specific topics or recommendations). Note that the different work items are linked among each other and cannot be seen as individual items. The splitting into different work items was only necessary in order to have a workable process within the working group. For example, revocation of trust is clearly one of the functions to be defined in the certificate policy of the trust model. In another example there is a clear link between the compliance assessment and security results of the working group, as for instance the successful compliance assessment of a C-ITS station ensures that a C-ITS station can be trusted and that it will therefore receive the trust certificate from the Certification Authority (CA).

Some topics related to security of C-ITS (e.g., general cybersecurity threats) were not selected because they are indirectly addressed through the chosen work items described above or because they were considered manufacturers responsibility or because they were dealt in other working groups (e.g. WG6 on access-to-in-vehicle data discussions on in-vehicle security / gateways, etc.).

2 Organisation of Work

The organization of work was based on regular face to face meetings (WG5 conducted a total of 13 face to face meetings from November 2014 – December 2015 in the course of the first phase of the C-ITS platform) and also on numerous phone conferences to deal with specific sub-topics in the main work items. The physical meetings were also used to approve the technical reports of section of the reports.

DG MOVE chairing WG5 took care of maintaining relationships with other Working Groups and informing the WG5 participants of work items, which could be related. In the particular case of privacy and security in C-ITS, because privacy and security can be strongly related and security frameworks can also support privacy solutions in C-ITS, a special collaboration and a number of meetings were set up between WG4 and WG5. Further topics for WG 10 on international cooperation have been identified that require further discussion beyond Europe in the future.

All results, outputs and expert recommendations of the C-ITS Platform WG5 have been produced, discussed and endorsed by the following organisations, countries and nominated experts:

Organisation	Name
Applus IDIADA	ARRÚE Álvaro
Applus IDIADA	PILLADO Marcos
ASFINAG	JANDRISITS Marko
BMW	SCHOLTEN Joachim
BOSCH / CLEPA	KNIRSCH Matthias
Car 2 Car Communication Consortium	ANDERSEN Niels Peter Skov
CECRA	ARATHYMOS Neofitos
CEDRE	OP DE BEEK Frans
CLEPA	DEIX Stefan
Continental	ERDEM Bettina
Continental	KOCH Ingolf
CSI (UK) Ltd	WILLIAMS Bob
CTAG	PRIEGUE Francisco
DENSO Automotive Deutschland GmbH	LEINMUELLER Tim
ERTICO	FISCHER Francois
FIAT	BIANCONI Maria Paola
IBM	NEVEN Gregory
Kapsch TrafficCom	LAX Richard
Kapsch TrafficCom	TIJINK Jasja
Kapsch TrafficCom	WILDMANN Guenter
Member State (AT)	FRÖTSCHER Alexander
Member State (AT)	MOLIN Helge
Member State (BE)	POURTOIS Caroline
Member State (CZ)	PICHL Martin
Member State (DE)	BERNDT Sandro
Member State (DE) - BSI - Federal Office for Information Security	Schönherr Kerstin
Member State (DE) - BSI - Federal Office for Information Security	WIESCHEBRINK Christian
Member State (EL)	AMDITIS Angelos
Member State (FR)	OLLINGER Eric
Member State (FR)	PAGNY Roger
Member State (NL)	HAVINGA Hellen
Member State (NL)	LAMAITRE Gaston
Member State (NL)	OTTO Marcel
Member State (RO)	BANICA Sorin

Member State (UK)	BOUCHER Anthony
Member State (UK)	HANSON Graham
OpenTrust (SCOOP@F)	ABALEA Erwann
OpenTrust (SCOOP@F)	BLANCHER Remi
Pauls Consultancy BV	SPAANDERMAN Paul
PSA Peugeot Citroen	SERVEL Alain
Q-Free	EVENSEN Knut
RENAULT	LONC Brigitte
RENAULT	ROUSSEAU Christian
RENAULT	TISSOT Christine
Security Innovation	WHYTE William
SIEMENS	FUEREDER Herbert
SMMT / ACEA	DAVIS Peter
SWARCO / TISA	SCHMID Andreas
Telecom ParisTech / SCOOP@F FRANCE	LABIOD Houda
University of Murcia	SKARMETA Antonio
Volkswagen AG	BUBURUZAN Teodor
VOLVO Cars	BROBERG Henrik
VOLVO GROUP	WAHLUND Jörgen
VOLVO GROUP	ZAKIZADEH Hossein

The following European Commission Services have been involved in WG5:

Services	Name
EC CNECT	FREDERIX Florent
EC CNECT	HOEFS WOLFGANG
EC CNECT	ZAMBARA Nino
EC GROW	ESCOBAR GUERRERO Luis
EC GROW	LAGRANGE Antony
EC INEA	PALESTINI Claudio
EC JRC	BALDINI Gianmarco
EC JRC	MAHIEU Vincent
EC MOVE	ALFAYATE Maria
EC MOVE	CARABIN Gilles
EC MOVE	DEPRE Claire
EC MOVE	MENZEL Gerhard
EC MOVE	TZAMALIS Georgios
EC MOVE	VAN DER LINDEN Geert
EC MOVE	VAN GAEVER Alain

3 Work items of WG5

3.1 Trust Models for C-ITS

The main item that has been discussed in WG5 was the design of the Trust Model for C-ITS, because it is the essential pillar to ensure security and trust among the main entities of C-ITS.

The objective of this work item and the related technical report was to identify and analyse the main Trust Models for Cooperative-C-ITS based on a Public Key Infrastructure (PKI). While other cryptographic techniques could also be used (e.g., symmetric cryptography), the report focuses specifically on PKI. The report identifies the potential PKI-based trust models from literature and other case studies and assess them on the basis of the specific features of C-ITS and metrics of evaluation based on high level requirements.

The report describes similar case studies, which could provide input to the analysis for the C-ITS trust model both from existing running systems and from standardization activities. Case studies outside ITS were also considered.

The report identifies the main trust models based on PKI and the main requirements areas, which are used to evaluate the trust models. An analysis for each requirement area has been provided. The set of analysis has been used to provide final recommendations for the most appropriate trust model in C-ITS for Europe for a day one phase and a mature deployment phase.

The final report on this work item is ANNEX 1.

3.2 Revocation of Trust in C-ITS

The work item of revocation of trust was chosen to ensure that misbehaviours of C-ITS station or applications (either intentional or unintentional) was dealt in the proper way. The work item and the related technical report presents an analysis of the expert members of the C-ITS Platform security working group 5 on the topic of revocation of trust in C-ITS in order to identify the requirements for revocation of trust in C-ITS and the related countermeasures. The report captures the relevant work from the state of the art both from research and standardization activities. The main threats and related incident scenarios are defined to illustrate the different needs (requirements) for revocation of trust, although this report does not claim to be a complete analysis. This report does not provide a full Threat, Vulnerability and Risk Analysis (TVRA) for the trust revocation function in C-ITS.

Technical solutions and design options for revocation are discussed to understand what a Trust Model can and should provide for deployment of Day 1 and beyond C-ITS services from different stakeholder viewpoints and what mechanisms can be used to control and mitigate risks. The WG5 experts agreed to a medium term solution with a strong involvement of stakeholders from private and public institutions. Some currently open aspects in the discussion of the revocation of trust topic still remain, which will need to be defined as topics and analysed further with the support of the respective stakeholders in order to facilitate the introduction of C-ITS in Europe.

The final report on this work item is ANNEX 2.

3.3 Crypto Agility / Updateability in C-ITS

Crypto-agility is the ability of a protocol to adapt to evolving cryptography and security requirements. There are various reasons why the cryptographic algorithms already deployed in C-ITS must be updated. The reasons can be both intentional and unintentional. Intentional reasons can be a migration from a previous cryptographic algorithm to a new one. Unintentional reasons are related to a broken algorithm, which could make the system unusable.

Another aspect investigated in the report is software updateability. The use of software has increased considerably in recent years in the automotive market. Software can be updated and installed in the automotive components of cars but this opens new risk and threats, which are similar to the one affecting the computer industry (e.g., virus, worms). The report investigates the approaches and techniques, which can be used to support secure software update and activations.

This report aims to map the current positions of C-ITS Platform WG5 experts on how crypto agility and software updateability can be handled when deploying C-ITS systems.

The final report on this work item is ANNEX 3.

3.4 Compliance Assessment in C-ITS

This work item was chosen because it is important that C-ITS station are fully functional before they can be trusted to be deployed in the field. The objective of the work item and the related report is to give a comprehensive, high level overview on the process definition for the compliance assessment for C-ITS systems or stations and C-ITS enabled vehicles.

The term “compliance assessment” has been used to describe the process by which a C-ITS station is validated through a set of tests to be deployed in the market. For the achievement of key public policy goals, C-ITS stations require compliance assessment before being placed on the EU’s internal market. The report looked at which technical aspects are required to achieve public policy goals, such as road safety, protection of health, environmental protection, energy efficiency, protection against unauthorised use, non-discriminatory market access, etc. Then, the report discusses, in which cases compliance assessment procedures are necessary. The report identifies and refers to other documents or reports for product/system validation and certification for deployment of C-ITS. This document points to existing procedures wherever possible, and includes outlooks on missing parts for the C-ITS domain.

The final report on this work item is ANNEX 4.

4 Recommendations/Follow Up Actions

4.1 Main high level WG5 Recommendations

The experts of WG5 have identified specific recommendations for all work items described in the previous chapters of this report. The following high level recommendations aim to summarise the main high level recommendations that can be derived from the more specific recommendations on the single work items in ANNEX 1-4:

- One common C-ITS trust model all over Europe shall be deployed that shall support full secure interoperability at the European level.
- To that end, a common certificate policy of the trust model for C-ITS day 1 deployment in Europe needs to be defined urgently.
- The appropriate legislative framework for C-ITS (e.g. new delegated acts or the identification of the amendments to the existing regulatory framework) needs to be set in place quickly to support a C-ITS deployment starting from 2019.
- The roles of the entities at European level to support the deployment and operations of C-ITS in Europe need to be identified and defined (e.g. roles within a European C-ITS security credential management system or within the compliance assessment process).
- The financing scheme needs to be discussed to identify which parties will support or contribute to the financing scheme.
- Standardization activities for the gaps identified in the reports (e.g., revocation of trust) should be addressed urgently.
- A time plan for the design and deployment of the security elements (e.g., CA) of an EU wide C-ITS with the most significant milestones should be drafted.

4.2 Specific recommendations of the single work items

An abstract of the complete set of specific recommendations on the single work items is included in the following sub-sections. For further details please check each respective ANNEX for the full context of the analysis, details and conclusions that lead to the specific WG5 expert recommendations.

4.2.1 Trust Models for C-ITS

The analysis conducted in the trust model report (ANNEX 1) has identified the following recommendations:

(1) The agreed objective is to **deploy one common C-ITS trust model all over Europe** that shall support full secure interoperability at the European level. Since the experts of WG5 recognise that this cannot sufficiently be provided by either a single EU Member State, nor by individual stakeholders (e.g. automobile manufacturers) a joint effort to develop EU-wide policy with clearly identified roles and methods is required. As described in ANNEX 1, the EU-wide C-ITS trust model is the implementation of the trust model based on a Public Key Infrastructure (PKI) system with the associated policies, organizational structures and processes including the links to the C-ITS compliance assessment process for certain types of applications.

a) This trust model **shall be implemented in a single trust domain version** (e.g., one single cryptographic algorithm and certificate format) **for the start-up day one phase** of C-ITS.

b) **Beyond the Day 1 phase, C-ITS may be extended with multiple interoperable trust domains** if deemed necessary to take the variety of stakeholders (including the global dimension) and the responsibilities for private and public entities involved into account.

In order to deploy a common C-ITS trust model specific elements and steps are needed. According to the WG5 experts the following recommendations are therefore further defined:

(2) **Need for Legal Certainty**: The appropriate legislative framework (e.g. new EU delegated acts or the identification of the amendments to the existing EU regulatory framework) needs to be set in place **quickly**.

(3) In order to achieve legal certainty a careful **analysis and discussion with the relevant stakeholders** is needed. The list of relevant stakeholders identified by the WG5 experts includes (but it is not necessarily limited) to:

- Member States
    - Responsible National Security Agencies
    - Responsible National authorities, ministries or bodies
- Vehicle manufacturers
- Infrastructure operators
- Telematics manufacturers for vehicle, roadside infrastructure and nomadic devices.

(4) The **responsible policy bodies for the definition of the security policy, certificate policy and related implementation measures (e.g. certificate practice statement) have to be identified** – this should be done in parallel with setting up the appropriate legislative framework. An independent governance structure will be needed to coordinate the definition and subsequent implementation of the commonly agreed elements (e.g. certificate policy) for *Day One* C-ITS applications deployment. This includes the definition of the entities responsible for the setting up and implementation of the components of the trust model.

(5) The **financing scheme** needs to be discussed to identify which parties will support or contribute to the financing scheme.

(6) Compliance with the identified legislative framework in (2) **will need to be reflected in the compliance assessment process** for vehicle and roadside C-ITS equipment.

(7) A **time plan for the design and deployment of the EU wide C-ITS trust model** with the most significant milestones (e.g. identification of the CAs or definition of the certificate policies) should be drafted. The experience from the EU C-ITS corridor deployment initiatives, standardisation activities and pilot projects should be taken in consideration in the drafting of the time plan. The timeplan should include at least the following milestones:

- Definition of the Certificate Policy, Certification Practice Statement and Security Policy
- Identification and design of the PKI
- Definition of the distribution channels for the certificates
- Definition of the compliance assessment process
- Definition of the financing scheme

4.2.2 Revocation of Trust in C-ITS

The analysis conducted in the revocation of trust report (ANNEX 2) identified the following recommendations:

(1) Revocation of trust is to be considered as an important aspect to be covered by the **common certificate policy** that needs to be defined for C-ITS day one deployment in Europe (in accordance to the trust model recommendations of WG5).

(2) As a part of the definition of the common certificate policy the E-SCMS (European C-ITS Security Credential Management System) support for revocation shall be defined based on the selection of countermeasures presented in this report, reflecting the stakeholder's positions appropriately.

(3) A time-plan on when the setup of the revocation countermeasures have to be finalised by all stakeholders for interoperable C-ITS Day 1 deployment should be defined at least 6 months prior to the start of operation of the E-SCMS (an envisaged goal for the start of operation of the E-SCMS would be in 2018).

(4) Further work needs to be done in the following area:

A common set of selected countermeasures related to the stakeholder's positions in this report needs to be defined for the E-SCMS operation.

- Definition of the formats, size and delivery mechanisms of the CRL (Certificate Revocation List) are urgently needed, e.g. through standardization of the design of CRL.
- Organization framework for the misbehaviour detection and subsequent revocation of trust is needed. In addition research into advanced misbehaviour detection is needed.
- Legal implications of revocation of trust need to be further analysed for operation.
- Analysis of responsibilities in the multi-application/domain setting on C-ITS stations.

4.2.3 Crypto Agility / Updateability in C-ITS

The analysis conducted in the Crypto Agility/Updateability (ANNEX 3) identified the following recommendations:

(1) The responsible policy body for the definition of the security policy shall be in charge of defining updates of the security policy due to expiry/deprecation of crypto algorithms, and a migration plan that shall be observed by the C-ITS Station system manager.

(2) It is recommended to investigate and potentially amend the existing protocol defined in ETSI to allow, in a backwards compatible manner, a second signature, which uses a new algorithm and which can co-exist with the old signature during a certain period. The design of the protocol should take in consideration the analysis provided in section 6 of ANNEX 3.

(3) C-ITS Station system managers shall estimate the risks related to certificate policy (e.g., new cryptographic algorithms) and software updates and have an appropriate risk treatment plan.

(4) Security recommendations on cryptographic algorithms for C-ITS can only be valid for a limited time and have to be reassessed on a regular basis.

(5) It is important to define a framework to reach quickly a consensus on the choice of new algorithms in case of a security breach. In other words, an organization and process should be put in place to reach quick solutions to security breaches in the cryptographic algorithms.

4.2.4 Compliance Assessment in C-ITS

The analysis conducted in the compliance assessment (ANNEX 4) identified the following recommendations:

(1) to pursue a compliance assessment process for C-ITS as proposed and described in ANNEX 4 for Day 1 deployment of C-ITS. During implementation of this process, at least the identified risks and challenges of the report have to be further analysed and discussed with the involved stakeholders in order to ensure a well-functioning C-ITS compliance assessment process. For the definition of the details of this process the main stakeholders in the C-ITS deployment, e.g. public authorities and road operators, vehicle manufacturers and C-ITS station suppliers and C-ITS station operators, should be directly involved to define the necessary next steps together.

(2) On the basis of the first recommendation, the central entities described in ANNEX 4 should be selected at European level. For example a governing body must be established which is in charge of defining the C-ITS Station requirements to both realise those technical aspects and meet the stakeholders' needs. Further a compliance assessment authority, which administers the compliance assessment criteria and the timing for the applicability, should be defined.

(3) Need for Legal Certainty: The need for an appropriate legislative framework (e.g., new EU delegated acts or the identification of the amendments to the existing EU regulatory framework) needs to be analysed.

(4) The financing scheme needs to be discussed to identify which parties will support or contribute to the financing scheme to support the compliance assessment process.

(5) A time-plan to endorse the compliance assessment process should be defined. It is important that the first set of C-ITS compliance assessment criteria is available at least 18 months before start of operation of C-ITS (an envisaged goal for the first version of the C-ITS compliance assessment criteria would be in 2017). This time-plan should define the main milestones and dependencies among the different tasks.

Annex

ANNEX 1.Trust Models for C-ITS

ANNEX 2.Revocation of Trust in C-ITS

ANNEX 3.Crypto Agility / Updateability in C-ITS

ANNEX 4.Compliance Assessment in C-ITS