C-ITS Platform

WG5: Security & Certification

Final Report

ANNEX 2: Revocation of Trust in Cooperative-Intelligent Transport Systems (C–ITS)

v1.0

Contents

1 Scope

This technical report presents an analysis of the expert members of the C-ITS Platform security working group 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. This 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 Security Credentials Management System (SCMS) 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. 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 analysis is based on the expertise of the participants and contributors of the Working Group 5 of the C-ITS Platform.

2 Introduction

Revocation of trust can be seen as a security measure in the context of C-ITS. Security measures are defined based on an analysis of the risks posed to a system: the ETSI Threat, Vulnerability and Risk Analysis (TVRA) [5] has been used to identify risks to the C-ITS system by isolating the vulnerabilities of the system, assessing the likelihood of a malicious attack on that vulnerability and determining the impact that such an attack will have on the system. This led to a set of countermeasures which includes the need to digitally sign messages over the air as defined in [6]. In order to provide C-ITS stations with the necessary security objects to do this, a security credentials management systems (SCMS) has to be set up as defined in [3], [4] and based on the trust model analysis in [10].

As explained in ETSI TS 102 165-1, a TVRA is an iterative analysis which needs to be re-done after application of the countermeasures. In this sense, given the TVRA in ETSI TS 102 165-1, and applying the countermeasure with the “PKI-like solution to Digitally sign each message using a Kerberos/PKI-like token system”, a new TVRA must be applied, to identify the threats, vulnerability and risks associated to the countermeasure that has been added to the system. This report does not perform a TVRA, because risks can only be evaluated by the stakeholders (business parties) that own the system, and result can be different for different stakeholders.

This report introduces the principles about the security analysis of the use of such a SCMS, the related security objects (private keys and certificates) and the countermeasures needed to prevent its misuse.

With reference to the same TVRA method used by [5], this report covers aspects (but not a complete analysis) related to single steps from 1 to 5:

1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

2) Identification of the objectives resulting in a high level statement of the security objectives and issues to be resolved.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

10) Specification of detailed requirements for the security services and capabilities from step 9.

The recommendations of this report define a set of security services (see step 10) that an SCMS should provide in order to support the correct operation of the C-ITS System, namely methods and applied processes for the revocation of trust.

3 References

[1].	C2C-CC: PKI Memo V 1.7. C2C-CC, "C2C-CC public key infrastructure memo," CAR 2 CAR Communication Consortium, Tech. Rep., February 2011.
[2].	NHTSA: DOT HS 812 014. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application
[3].	ETSI TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications architecture and security management, v1.1.1, June 2012.
[4].	ETSI TS 102 941 v1. 1.1-intelligent transport systems (ITS); security; trust and privacy management," Standard, TC ITS, 2012.
[5].	ETSI, TR 102 893:" Intelligent Transport System (ITS), Security, Threat, Vulnerability and Risk Analysis (TVRA).
[6].	ETSI TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats, v1.1.1, April 2013.
[7].	ETSI TS 102 731 v1. 1.1-intelligent transport systems (ITS); security; security services and architecture. Standard, TC ITS. 2010
[8].	IEEE WAVE standard: IEEE Std 1609.2™-2013 IEEE Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages
[9].	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
[10].	C-ITS Platform – WG5 Security & Certification: Trust models for Cooperative - Intelligent Transport System (C-ITS)

[11].	Whyte, W.; Weimerskirch, A.; Kumar, V.; Hehn, T., "A security credential management system for V2V communications," in Vehicular Networking Conference (VNC), 2013 IEEE , vol., no., pp.1-8, 16-18 Dec. 2013.
[12].	ISO/DIS 17427-1, Intelligent transport systems (ITS) — Co-operative systems — Roles and responsibilities in the context of co-operative ITS architecture(s)

4 Glossary

Abbreviation	Synonym	Description
Authenticity	Security property	Property that an entity is what it claims to be (ISO 27000).
AA	Authorization Authority	Authority that provides an C-ITS-S with permission to invoke C-ITS applications and services (ETSI TS 102 941,[4])
EA	Enrolment Authority	Authority that validates that an C-ITS-S can be trusted to function correctly (ETSI TS 102 941, [4])
CA	Certificate Authority	The CA is a trusted party, which authenticates entities taking part in an electronic transaction. To authenticate an entity, the CA issues a digital certificate. This certificate is a digital document which establishes the credentials of the entities participating in a transaction.
Certificates	Security material	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity.
Confidentiality	Security property	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 27000)
Cooperative		Cooperative means that the data will be sent from roadside to and from the vehicles (V2I2V) and between vehicles (V2V) by all communication means but mainly by short/range Wifi-p (control and warnings) and less by cellular 3/4G/LTE (for less critical services). In the "cooperative" situation real coordination takes place between vehicles mutually and between vehicles and roadside. This coordination can take place by a driver action (max speed; initially during day one) or automatically by the vehicle systems themselves (eg CACC).

Cooperative C-ITS (C-ITS)		C-ITS systems that can bring intelligence for vehicles, roadside systems, operators and individuals, by creating a universally understood communications "language" allowing vehicles and infrastructure to share information and cooperate in an unlimited range of new applications and services.
Cooperative Services		Cooperative services concerns the (fast) exchange of data/information with DSRC/wifi-p form V2X to support or automatically take-over the tasks of driver.
CRL	Certificate Revocation List	Certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted (source: Wikipedia).
ETSI	European Telecommunications Standards Institute	It is an European standardization body.
C-ITS	Intelligent Transport Systems	Intelligent Transport Systems (C-ITS) are systems to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (cars, trains, planes, ships).
C-ITS Application		A functional definition of a service provided to an end user, which fulfils specific needs of a user (for example, forward collision warning)
C-ITS station		A collection of (functional) equipment that participate in the provision of C-ITS services at a particular location. An C-ITS station may exist in a vehicle, at the roadside, in a central location such as a Traffic Management Centre, or in a mobile device. It has two meanings: an actual physical device and/or a functional set of services. In this report a C-ITS station is the equivalent of an ITS-station defined in ETSI documents.
C-ITS station system manager		This is the entity responsible for managing the C-ITS station from an operational and administrative point of view. This role is equivalent to the role System management defined in ISO/DIS 17427-1 [12]: "The role "system management" is responsible for all management activities in the system. It

		supports both System operation and Policy framework".
LTCA	Long Term Certification Authority	Certification authority for the long term Certificates.
Misbehavior detection		Automatic detection of misbehaving device or equipment, possibly resulting in automatic revocation.
OCSP	Online Certificate Status Protocol	It is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
PC	Pseudonym Certificate	
PCA	Pseudonym Certification Authority	Certification authority for the pseudonym Certificates.
PKI	Public Key Infrastructure	A public key infrastructure (PKI) is the combination of software, cryptographic technologies, processes, and services that enable an organization to secure C-ITS communications and business transactions.
Policies		Rules, practices, regulations, laws, official texts governing specific activities, organizations, agreements.
Privacy/Data protection		Set of rules and policies in a jurisdiction, aiming at protecting sensitive personal data belonging to individuals.
Revocation		Revocation is the act of recall or annulment. It is the reversal of an act, the recalling of a grant or privilege, or the making void of some deed previously existing (source: Wikipedia).
SCMS	Security Credentials Management System	Security system design for cooperative vehicle-to-vehicle and vehicle to infrastructure applications
Security material		Collection of cryptographic material (keys, certificates, algorithms, credentials, identifiers) that need to be created, embedded, activated, deactivated and eventually discarded at the end of life of a device.
Trust		The extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible. D. Harrison Mcknight and Norman L. Chervany. The meanings of trust. Technical report, 1996.

TVRA		Threat, Vulnerability & Risk Analysis
V2I	Vehicle to Infrastructure	Vehicle to Infrastructure communications
V2V	Vehicle to Vehicle	Vehicle to Vehicle communications
V2X	Vehicle to X	Combination of Vehicle to Vehicle communications and Vehicle to Infrastructure communications.

5 Analysis of needs for revocation of trust in C-ITS

5.1 Target of evaluation: The Security Credentials Management System (SCMS) and C-ITS-Stations

The identification of the Target of Evaluation is Step 1 in the TVRA as defined in [5].

5.1.1 Input from Literature

The **ETSI TVRA** [5] identifies the need for an SCMS that is composed of Certificate Authorities and ITS-Stations:

A secure implementation of a system based on a Public Key Infrastructure (PKI) depends on the availability of (derived from [5]*):*

- *a secure provisioning system to allow a C-ITS station to obtain certificates from the CA;*
- *timely information like access to revocation information provided by the CA;*
- *protection of the authentication keying material and other, transient keying material on the C-ITS station; and*
- *access controls and software quality mechanisms to ensure that malicious software on the C-ITS station cannot make use of the keys without extracting them.*

The various options for the trust relations and models for C-ITS are explained in [10].

5.1.2 Analysis of assets

The SCMS is further described in [3] and [10]. In addition to this, the SCMS needs an interface to external entities such as:

- vehicle registration authority
- Users
- C-ITS station system manager

5.2 Objectives for revocation of trust in C-ITS

The Identification of the security objectives is step 2 in a TVRA.

5.2.1 General Information

This subchapter provides general information about possible objectives of revocation of trust. Some examples are listed from different sectors (e.g. eCommerce) in order to illustrate general objectives of revocation of trust.

Revocation of trust is a mechanism designed to protect the provision of the core security services of *authentication* and *authorization*. Revocation of trust is used within a system model where:

- A node is provisioned with some security material (for example a cryptographic key) such that access to the security material is restricted to a set of authorized parties (for example, the security material is a private key used for signing that exists only on that node; or the security material is a password that is shared between a node and a server)
- The node carries out operations where its correct use of the security material indicates that it holds certain permissions (for example, the password allows a user to access a particular account with an

eCommerce provider; or a digital signature generated with the private key allows the user to send Cooperative Awareness Messages that can be trusted by receivers)
- The node operates in a (somewhat) hostile environment where it may at some point stop functioning correctly;
- If there are counterparties that used the node's correct use of the security material to trust the node, and if the node meets some conditions for incorrect functioning, those counterparties are instructed not to trust interactions that are authenticated with that cryptographic material, i.e. not to trust the node. The act of instructing counterparties not to trust particular cryptographic material is known as *revocation*.

A policy for revocation of trust in a node must identify:

1) What set of permissions are to be revoked
2) What conditions must be met in order for revocation of trust to occur (this is often informally referred to as "misbehaviour detection")
3) What mechanism is used to communicate information about the revocation event to counterparties and potential counterparties.

This section focuses on elements that inform the first two items in this list, i.e. what is to be revoked and how is a revocation determination to be made.

5.2.2 Input from Literature

ETSI Standards: The ETSI Standards assume that revocation will be necessary (since the C-ITS environment fits the model described above) but do not provide a lot of analysis on the reasons for revocation (only mentioning: *misbehaving or otherwise not trustworthy or accountable)*.

C2C-CC PKI Memo [1] mentions:

- De-listing of active ITS Stations, (e.g., de-registration of vehicles for repair or stolen cars).
- Permanent deactivation as the end of life of C-ITS stations (e.g., junked vehicles)
- Misbehaviour of entities in the C-ITS context (e.g., misbehaviour of a C-ITS station)

NHSTA mentions several ways by which vehicles may be added to the Certificate Revocation List (CRL):

- Administrative revocation,
- ITS-Stations that observe other ITS-Stations distributing messages report those to a so–called misbehaviour authority. This may lead to an inclusion in the CRL of those ITS-Stations depending on various detection algorithms.
- a vehicle could self-report if it determines that it is not operating properly, and this might also result in a revocation

Note that misbehaving in the NHTSA studies does include faults that also could arise from faults in the system, not caused intentionally by someone.

The CAMP SCMS design paper [11]

This paper does not give specific conditions under which revocation should take place (stating that "the format of a misbehaviour report is not fully defined yet" and "the algorithms of global misbehaviour detection have not been developed yet") but defines the interfaces necessary to support revocation once the

revocation decision has been made, i.e. provides material supporting policy item 3) above but not 1) or 2) (compare policy items in chapter 5.2.1)

5.2.3 Analysis of objectives

The SCMS mainly addresses the objectives of Authenticity and Integrity for Day 1 applications, which are broadcast. Confidentiality of Unicast communication is a topic for Day 2 applications and not further discussed here (since also not covered by current literature).

The following relevant security objectives related to the authenticity of ITS users and transmitted information are specified in [5]:

Au1. It should not be possible for an unauthorized user to pose as an ITS-S when communicating with another ITS-S.

As a result of the analysis work of the C-ITS Platform WG5 experts, this document identifies the following types of user that should be considered unauthorized:

- A C-ITS station/Application behaving incorrectly according to the system specification and whose authorization has been removed
- A C-ITS station/Application for which the cryptographic material has been obtained by an unauthorized party and may be used to authorize invalid messages (i.e. a scenario where the C-ITS station / Application is itself behaving correctly but should be de-authorized to protect the system from messages generated by an attacker).
- A C-ITS station/Application that has never been authorized
- A C-ITS station/Application that has temporarily or permanently lost its authorization by an ITS-Station due to repair or end-of-life.

Two additional types of users have been identified that may be considered unauthorized, depending on policy:

- C-ITS station that has been lost or stolen and cannot be remotely deactivated/controlled
- C-ITS station /Application that is behaving correctly according to the specification but which is interacting with flaws in implementations on other C-ITS stations in such a way as to cause harm to the system.

The following security objectives related to the integrity of stored and transmitted ITS information are specified in [5]:

In2. Information sent to or from a registered ITS user should be protected against unauthorized or malicious modification or manipulation during transmission

In3. Management Information held within a ITS-S should be protected from unauthorized modification and deletion.

In4. Management Information sent to or from an ITS-S should be protected against unauthorized or malicious modification or manipulation during transmission.

Where the term “registered ITS user” means a C-ITS station enrolled and authorized in the SCMS.

In2 should be guaranteed in case of compromise of a CA service due to:

- Breach of crypto algorithm defined in its certificate policy
- End of activity of operation of the CA
- Unauthorized access to security management information of the CA

In3 and In4 should be guaranteed also in case of loss or theft of ITS-Station.

The Objectives of Privacy should be further considered when iterating the TVRA approach for the countermeasures of section 6 (especially for the assessment of the requirements related to certificate revocation lists).

5.3 High level functional security requirements

The Identification of the functional security requirements is step 3 in a TVRA. The ETSI TVRA identifies among others two important countermeasures which are the security functional requirements at the level of this report [5]:

- Digitally sign each message using a Kerberos/PKI-like token system
- Provide remote deactivation of misbehaving ITS-S

5.4 Incident scenarios

This section points to the core steps in a TVRA, i.e. steps 5, 6 and 7:

- Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.
- Quantifying the occurrence likelihood and impact of the threats.
- Establishment of the risks.

This section summarizes threat and vulnerabilities in the form of incident scenarios that can be used to determine the risks. An incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident (see ISO/IEC 27002:2005, Clause 13). Additionally the incident scenarios also contain notions about the possible consequences of the incident.

The incident scenarios have been structured into two main groups, namely:

- CA Level incident scenarios
- C-ITS station level incident scenarios

In each of these groups the analysis policy identifies scenarios in which a C-ITS station or Application should or could, depending on policy, be identified as misbehaving and therefore a subject of revocation, i.e. this analysis identifies scenarios relevant to policy item 2) above (see Chapter 5.2.1).

Please note that the defined incident scenarios are not exclusive and some scenarios could refine specific aspects of other scenarios.

5.4.1 CA Level incident scenarios:

1. *Compromise of a CA in the Trust Model.*
   This scenario describes the case where a CA in the trust model based on PKI of a C-ITS domain has been compromised. The compromise of the CA affects all the certificates and related cryptographic

material produced though the CA. This is one of the most serious scenarios, because it can affect most or the whole of the C-ITS domain and all C-ITS stations using that CA.

2. *'Broken' cryptographic algorithm*
   This is one of the most critical scenarios where the cryptographic algorithm itself has been compromised. This means the rebooting the system or distributing new keys would only 'repair' the situation for a very short time, as the security framework of C-ITS system would have become vulnerable in essence. The entire security framework must be upgraded: key lengths, crypto algorithms, credentials and other cryptographic material.

3. *Migration to other CAs or trust model structures*
   This scenario is related to the modification of the trust model structures or its main elements including the cryptographic algorithms. In comparison to the previous scenarios, this is a planned event and adequate countermeasures (including new procedures) can be put in place to migrate from the old CA to the new CA or to upgrade the trust model and the involved C-ITS stations. A migration time can be defined where two trust models are in place; after this time, the old certificates must be revoked if they are still valid.

5.4.2 C-ITS station level incident scenarios:

4. *Malicious or misbehaving C-ITS station*
   A monitoring system (e.g., which can be part of a SCMS) has identified a C-ITS station, which evidently behaves not according to the rules defined in the C-ITS framework (e.g., it is transmitting false information on the position or speed). Note that the malicious behaviour of the C-ITS station can be intentional (because the C-ITS station has been taken over by a malicious party) or unintentional (because of a failure of the C-ITS station). The first situation is further detailed in the scenarios 7,8,9 below. Note that a C-ITS station belongs to the same jurisdiction or different jurisdictions. Trust revocation mechanisms could be different depending on whether either the revoked station, or the station receiving the revocation information, is a mobile C-ITS station or a C-ITS roadside station.

5. *C-ITS end-of-life policies*
   A device at the end of its life could be used to implement security attacks like stealing cryptographic material. Each C-ITS system would be expected to have decommissioning procedures for C-ITS stations reaching the end-of-life. With end-of-life we also include the case where C-ITS station has been damaged or destroyed (e.g., car accident).

6. *C-ITS station repair policies*
   C-ITS stations could be temporarily revoked during the repair phase if the certificate and security policies require this.

7. *Hacking of C-ITS station – extracting of cryptographic material*
   This scenario describes the compromise of a C-ITS station when the cryptographic material is extracted (*"stolen"*), i.e. it can be used outside the C-ITS station. Such extracted keys could also be published by the attacker. This scenario is different from scenario 4, since the use of the extracted

material in an unauthorized ITS station might not be evident to a monitoring system. If the malicious attacker can use the theft of cryptographic material to break the cryptographic algorithms, this scenario become scenario (2) described above. In this case revocation is strongly recommended.

8. *Hacking of C-ITS station – modification of permissions / software modification or reconfiguration*
   This scenario describes the compromise of a C-ITS station by a malicious attacker, which is able to alter the permission for access to data and services. This scenario is different from scenario 4, since the modification might not be evident to a monitoring system. This case can be considered a generalization of a scenario where malware is installed on the C-ITS station: the cryptographic material has not been extracted (if it had been, that would be scenario 7) but malicious processes have access privileges to it. This allows the malicious processes to create false messages, though possibly not with the scalability that is allowed by scenario (7). In this case revocation may be necessary, depending on policy-defined criteria that take into account the likely impact of the misbehaviour.

9. *Hacking of C-ITS station – false inputs / detaching from vehicle*
   This scenario describes the case where an attacker creates false inputs to a C-ITS station so that it will create false outputs. These false inputs could be, for example, camera, sensor, GPS, or data from a service provider. This case can be considered a generalization of the scenario where an attacker detaches a vehicular C-ITS station from the vehicle's sensors (and optionally demount it) and feeding it with other faked sensor data. In this case revocation may be necessary, depending on policy-defined criteria that take into account the likely impact of the misbehaviour (although note that in this case the C-ITS station is not itself misbehaving and would be trustworthy if it was in a trustworthy environment).

10. *Stolen C-ITS station*
    This scenario describes the case where a C-ITS station is stolen, but not compromised as such. This could for instance be the case of a stolen car. All the sensor inputs are correct but the use of the device is giving some advantage to the thief – for example, they are able to request traffic signal pre-emption. In this case revocation may be necessary, depending on policy-defined criteria that take into account the likely impact of the misbehaviour (although note that in this case the C-ITS station is not itself misbehaving and would be trustworthy if it was returned to the valid owner).

11. *Valid activity causing bad results on other C-ITS stations*
    This scenario describes the case where a C-ITS station is behaving correctly, but there are flaws on receiving devices that cause bad results. As a hypothetical example, consider a case where a string is specified as encoded with Unicode but some widespread implementation implements the receive side using ASCII and crashes when given a non-ASCII Unicode string. If the implementations that send non-ASCII Unicode are not widespread, and the implementations that crash on non-ASCII Unicode are widely used, then the most effective way of reducing damage to the system may be to revoke the nodes that send non-ASCII Unicode even though they are behaving correctly according to the specifications. (This use case is listed here for completeness).

Risks can be calculated by assessing the consequences and likelihood of the incidents. As discussed in the next section, these consequences will depend on the applications being operated.

5.4.3 Considerations for the multi-application setting

This subchapter is considered as additional information – please note that no positions, scenarios or recommendations are intended to be given in this chapter.

C-ITS stations may run multiple application processes, and in this case there are two scenarios to be considered:

1) An entire C-ITS station and all the applications on it are compromised
2) Only a single application, or a subset of applications, on the C-ITS station is compromised.

It is noted that different applications will have different definitions of "misbehavior so damaging that it requires withdrawal of privileges from the misbehaving node". Therefore there are two ways that scenario 2 can come about:

a) A bad implementation of specific applications, or a targeted attack that replaces some applications but not others
b) Some degradation in the overall performance of the C-ITS station such that it meets the security requirements for certain applications but not for others.

It is further noted that for privacy and key hygiene reasons, two applications on the same C-ITS station may have different credentials and it may not be possible for an observer to tell from the datagrams alone that the applications are running on the same device[1]. There are therefore the following possible revocation scenarios in the multi-application setting:

1) All applications running on the same C-ITS station use the same credentials (i.e. there are device credentials rather than application credentials). If the device misbehaves, i.e. if one application on the device misbehaves, the device and all applications on it are revoked.
2) Applications running on the same C-ITS station use different credentials but they are issued by the same authority and are linkable by that authority. If one application on the device misbehaves, the authority revokes that application and has the ability to revoke all other applications on the device. The authority may choose only to revoke certain applications for which the level of misbehaviour is significant.
3) Applications running on the same C-ITS station use different credentials, issued by different authorities. If one application on the device misbehaves, it is reported to the appropriate authority. The appropriate authority revokes that application and may coordinate with the other authorities to revoke their applications. The authorities may choose only to revoke certain applications for which the level of misbehaviour is significant. In this case there must be some coordination of information between authorities to determine which application instances are on the same device.
4) Applications running on the same C-ITS station use different credentials, issued by different authorities with no coordination. Applications are revoked only if they themselves are seen to misbehave. No application is revoked due solely to the misbehaviour of a different application.

Revoking all applications means someone somewhere needs to be trusted with a catalogue of all applications installed on a given device and their certificates, which may be privacy violating (and goes beyond e.g. today's smartphone OSes where your OS provider knows all the apps you have installed but doesn't know the

[1] The current proposal for geonetworking adds location information to all G5 datagrams at the network layer, meaning that two PDUs from different applications will be easy to associate with the same device because they lie on that device's trajectory. However, not all datagrams will be sent using G5 and there are systems – for example, the proposed US system – that do not use geonetworking at all.

associated credentials). Not revoking all applications means a compromised device gets to misbehave independently with each application, potentially causing more damage.

6 Design options for revocation of trust

This section defines a possible set of security services that could be provided by an SCMS in order to cope with the incident scenarios of section 5.4, without making any assumption on the risk analysis. These different design options have again been structured into the two groups of “CA Level” and “C-ITS station Level” where both input from the literature and the corresponding analysis has been summarised in this section. The analysis includes the definition of **possible countermeasures**.

6.1 General Considerations

In essence there are three mechanisms to prevent an unauthorized node from successfully behaving as it if was authorized:

- **Actively deactivate** (i.e., a management/administrative function) the C-ITS station or application ("deactivate the offender"), preventing it from sending altogether.
- Inform all possible counterparties, i.e. all relevant C-ITS stations, that the node is to be considered revoked ("warning the potential victim"). Also inform all relevant CAs so that the node cannot acquire new, valid certificates. This is referred to as **active revocation**.
- Do not directly inform counterparties that the node is to be considered revoked, but inform all relevant CAs, so that when the node’s current certificates expire it cannot acquire new, valid certificates ("waiting for the offender's credentials to expire"). This is referred to as **passive revocation** or revocation by expiry.

In terms of the policy framework given in 5.2.1, these are three different mechanisms that may be used for policy item 3). In all cases there must be an identification of the domain that revocation applies to (i.e., the permissions that are to be revoked) and of the criteria used to determine that revocation should occur. The only difference between the three options above is the specific mechanism used to enforce the revocation decision.

The following considerations apply when deciding whether to use active deactivation, active revocation, or passive revocation for a particular C-ITS station or application:

- **Time to removal of the bad actor**: In all cases, the bad actor cannot be removed until they have been detected. Once a bad actor has been detected:
  - **Active deactivation** allows the bad actor to be removed immediately
  - **Active revocation** allows the bad actor to be removed subject to whatever time delay is involved in distributing the certificate revocation list (CRL).
  - **Passive revocation** allows the bad actor to be removed once it no longer has any valid certificates.

  The effectiveness of passive revocation therefore depends on how long a device typically has valid certificates for. An application specification should provide an estimate of the longest permissible time that a misbehaving client application may stay active for (the *maximum misbehaving period)*. In order for passive revocation to be effective, the system must make it practical to provide certificates

to the C-ITS stations more often than one per maximum misbehaving period. This allows valid devices to carry on operating while not providing any device with certificates that would allow it to misbehave for longer than the maximum misbehaving period. **In summary**, passive revocation works best when devices can be provisioned with certificates that last only a short time, but runs the risk that devices that lose connectivity are locked out of the system; active revocation allows certificates to be provisioned for longer, reducing the risk of lockout. Both allow also limiting the misbehaviour time depending on how often a connectivity of C-ITS station to the SCMS is available.

- **Mechanisms necessary for support: C-ITS stations**:
    - **Active deactivation** requires the C-ITS stations to support deactivation mechanisms. These create their own risks as they may be subject to compromise, leading to valid devices being maliciously or accidentally deactivated. It also requires the C-ITS stations to have the connectivity that allows deactivation mechanisms to operate. It is not clear what the required connectivity properties are; this could conceivably be accomplished by a broadcast mechanism or by a direct data link to the deactivation centre. Active deactivation may be more effective applied to always-connected roadside and fixed C-ITS stations than to mobile and vehicular C-ITS stations; however, see the discussion under "effectiveness" of the limitations of active deactivation.
    - **Active revocation** requires the C-ITS stations to support (a) receiving, (b) processing and (c) validating certificate revocation lists. If CRLs are large it may not be straightforward to receive them over G5.
    - **Passive revocation** requires the C-ITS stations to support certificate request and update mechanisms they already support, but in a higher periodicity then what is needed without revocation.
- **Privacy**:
    - **Active revocation** needs to be implemented in such a way that revoked devices do not suffer a significant compromise of the privacy of their movements before the time they were revoked. For example, if I buy a car in January and it needs to be revoked in June, this should not reveal my movements in February. This privacy needs to be preserved against other C-ITS stations and against the SCMS.
    - **Passive revocation** automatically protects devices against privacy compromises by other C-ITS stations, but privacy does need to be preserved against the SCMS.
- **Effectiveness**:
    - **Active deactivation** does not protect against key extraction or a compromise of the deactivation mechanism on the device itself.
    - **Active revocation and passive revocation** protect against all threats. The difference is that active revocation puts the burden to the victim, whereas passive revocation puts the burden to the potential offender.

An unauthorized node may be a C-ITS station or a CA. These cases are considered separately.

6.2 CA Level

6.2.1 Input from Literature

C2C-CC PKI Memo mentions [1]:

For the revocation of Pseudonym CAs, Long-Term CAs and Root CAs a distribution of CRLs is proposed. Based on CRLs all revoked CAs have to be distributed actively in the V2X system. Several options can be considered for CRL distribution, where one of the most likely ones is to use a pseudonym refill process for that as well.

Note added by C-ITS Platform WG5: The pseudonym refill process may have a too low frequency in order to distribute the CRL. C-ITS stations which are using certificates issued by revoked CAs cannot be identified as non-trustable for a long time frame. It is unclear how a Root CA certificate can be revoked, since that would break the entire system: it is assumed that this is valid for cross-certificates of "foreign" root CAs only.

TS 102 941 mentions [4]:

If an EA or AA is added to or removed from the system, the associated authority (not defined by the present document) should inform enrolled ITS-Ss of this change. The process for achieving this is beyond the scope of the present document but possible methods include:

- *sending a certificate revocation list as specified in IEEE 1609.2 across a wireless interface; or*
- *providing information to a trusted maintenance entity to enable it to update an individual ITS-S in a controlled environment.*

Note ***added by C-ITS Platform WG5***: Both alternatives are valid but the second requires a link between the C-ITS station and the maintenance entity with a defined and reliable periodicity.

IEEE 1609.2 mentions [8]:

If a CA certificate is revoked, the security services shall also consider all certificates issued by that CA and first received after the issue date of the CRL to be revoked, even if their stated generation time if before the issue date of the revocation list. This applies to any certificate that chains back to the revoked CA.

6.2.2 Analysis - Definition of counter measures

The following possible countermeasures (CM) are defined for the **CA Level**:

CM 1.	Revocation/Status information about a set of valid communication certificates should be provided by the SCMS to all C-ITS stations within a planned/defined/communicated limit of time via fully connected and validated C-ITS-Stations.
CM 2.	Revocation/Status information for a set of valid communication certificates should be provided by the SCMS to an appropriate forwarding service provided by C-ITS station system managers for distribution to mobile and stationary C-ITS stations.
CM 3.	After an initial starting phase of C-ITS networks, each C-ITS station must be served by at least two fully independently operating CAs (including EA and AA).

Table 1: List of possible Counter Measures: CA Level

Revocation information may be distributed in form of a Certificate Revocation List (CRL), in form of a Certificate Status List (see [10]), or made available online (OCSP).

6.3 C-ITS station Level

6.3.1 Input from literature

C2C-CC PKI Memo mentions: [1]

A fast revocation of Pseudonym Certificates in the C2C system is difficult due to limited connectivity between vehicles and Pseudonym CAs. Therefore, especially in the deployment phase the distribution of CRLs may be a problem. Furthermore, due to the very large quantities of Pseudonym Certificates, the size of CRLs would increase way too much.

As a result, the proposed PKI does not consider CRL distribution for PCs within the ITS G5 network.

Yet, revocation of vehicles is still possible by rejecting the request for new Pseudonym Certificates […] In this concept the Long-Term CA link the revocation information of the vehicle to its Long-Term Certificate. If an ITS Station requests new Pseudonym Certificates then the Pseudonym CA forwards the request to the respective Long-Term CA which checks the authorization of the requester.

"Evaluation of Countermeasures" in ETSI TR 102 893 mentions: [5]

The ETSI TVRA identifies a "second level" of security requirement, to prevent misuse/threat associated to the first level countermeasure:

In the event that a known, valid ITS-S (Vehicle) is detected to be providing misleading information to other vehicles (either by malfunction or malicious intent), a CA may prevent other units from processing its messages by one or all of the following methods:

- *using a revocation process to distribute information about compromised units;*
- *dynamically adjusting the frequency of distributing revocation information about compromised units*
- *providing on-line status queries by message recipients;*
- *issuing sender certificates with a limited lifetime, renewing them frequently, and not reissuing certificates to devices that are known to be compromised.*

TS 102 940 [3] and TS 102 731 [7] mention:

TS 102 731 identifies a range of security services which may be supported by an ITS station in order to provide communications security between itself and other stations. TS 102 940 provides the list and a short description of these services. Below is an excerpt (grey columns) with respect to revocation only [3]:

Service category	Security service	Interpretation
Enrolment	*Remove Enrolment Credentials*	Removing enrolment credentials/certificate is a long term measure for revocation. The enrolment certificate can be removed only when the ITS-Station asks for new enrolment or update,
Authorization	*Publish Authorization Status*	Publish Authorization Status corresponds to providing CRLs as a push service to ITS-Stations from the AA
	Update Local Authorization Status Repository	Update Local Authorization Status Repository corresponds to providing CRLs as a pull service triggered by the ITS Station to the AA.
Remote management	*Deactivate ITS transmission*	Remote deactivation is mentioned as a possible mechanism with which the EA can deactivate misbehaving ITS-Stations

NHSTA [2] mentions:

Misbehavior Authority (MA) acts as the central function to process misbehavior reports and produce and publish the certificate revocation list. It works with the PCA, RA, and LAs to acquire necessary information about a certificate to create entries to the CRL through the CRL Generator.

To support efficient revocation, end-entity certificates contain a linkage value that is derived from cryptographic seed material. […] For protection against insider attacks, the seed is the combination of two seed values produced by two Linkage Authorities; this ensures that no single organizational entity knows enough information to identify a single device (for more information refer to [2])

TS 103 097[6] mentions:

TS 103 097 mentions CRL as a possible security object to be authenticated but it does not support it explicitly.

IEEE 1609.2 [8] mentions:

A certificate is said to be revoked if an authorized entity distributes an authenticated message stating that that certificate is known not to be trustworthy. Such an authenticated message is known as a Certificate Revocation List (CRL). If a certificate is revoked, all communications signed by that certificate and received after the issue date of the revocation list shall be considered invalid, even if their stated generation time is before the issue date of the revocation list.

1609.2 [8] explicitly supports CRL as a security object to be transmitted to C-ITS stations.

The CAMP SCMS design paper [11]: supports active revocation of C-ITS stations and provides a mechanism that allows active revocation while also providing privacy for previous movements and against insiders (or data breaches) at the SCMS.

6.3.2 Analysis - Definition of counter measures

The following possible counter measures (CM) are defined for the **C-ITS station Level**:

CM 4.	The SCMS should feature an interface for the announcement of end-of-life, stolen, lost C-ITS equipment by the vehicle owner, C-ITS station system managers or vehicle manufacturer.
CM 5.	The SCMS should be able to detect misbehavior of C-ITS stations based upon their over-the-air behavior.
CM 6.	The SCMS should support SCMS-internal revocation of long-term certificates (Enrollment Certificates).
CM 7.	The SCMS should be able to identify long-term certificates based on short-term certificates.
CM 8.	The C-ITS station system manager should be able to temporarily and/or permanently remotely and securely deactivate the C-ITS station.
CM 9.	Authorizations which have been granted to C-ITS stations/ C-ITS applications should expire in a timeframe suitable to reduce risks without requiring active revocation
CM 10.	Revocation / Status information about pseudonym / authorization certificates which have been granted to C-ITS stations/ C-ITS applications should be provided by the SCMS to C-ITS stations, directly or through some forwarding mechanism.
CM 11.	The C-ITS station should appropriately protect the security management information to resist against attacks.
CM 12.	The C-ITS station should appropriately protect its processing logic to detect attacks.
CM 13.	The C-ITS station system manager should be able to monitor the status of the C-ITS station at any time.
CM 14.	The C-ITS station should deactivate itself securely and make its cryptographic material (e.g., private keys) unusable when tampered/demounted /detached from the vehicle by unauthorized personnel.
CM 15.	C-ITS stations should monitor other misbehaving C-ITS stations and save incomplete or incorrect over the air communication records for overall C-ITS network health analysis. This comprises single records of not correct communications received by a station, and transferred as summary record to the SCMS, e.g. every time when certificates to the single station are renewed.

Table 2: List of possible Counter Measures: C-ITS station Level

7 Mapping of the design options to the incident scenarios

7.1 General Mapping

This section provides a mapping of the possible Countermeasures defined in the design options chapters (compare with chapter 6.2.2 and 6.3.2) to the defined Incident Scenarios (compare with section 5.4).

The presented table is to be understood as an agnostic general view on which of the defined countermeasures can be taken to cope with the defined incident scenarios in this report. It is the general overall summary of what CAN be done in order to cope with the effects of the incident scenarios.

	Incident Scenario	Countermeasure
CA Level	1.) *Compromise of a CA in the Trust Model.*	CM 3 AND (CM 1 OR CM 2)
	2.) *'Broken' cryptographic algorithm*	CM 3 AND (CM 1 OR CM 2)
	3.) *Migration to other CAs or trust model structures*	CM 3 AND (CM 1 OR CM 2)
C-ITS station Level	4.) *Malicious or misbehaving*	CM 5 AND (OPTIONALLY CM 15) AND CM 6 AND CM 7 AND (CM 8 OR CM 9 OR CM 10) OR CM 13 AND CM 8
	5.) *C-ITS end-of-life policies*	CM 8 OR CM 4 AND CM 6 AND (CM 9 OR CM 10)
	6.) *C-ITS station repair policies*	CM 8 OR CM 4 AND CM 6 AND CM 10
	7.) *Hacking of C-ITS station – extracting of cryptographic material*	CM 11
	8.) *Hacking of C-ITS station – modification of permissions*	CM 12 OR CM 13
	9.) *Hacking of C-ITS station – false inputs / detaching from vehicle*	(CM 5 AND (OPTIONALLY CM 15) AND CM 6 AND CM 7 AND (CM 8 OR CM 9 OR CM 10)) OR CM 14 OR (CM 13 AND CM 4 AND CM 6 AND (CM 9 OR CM 10)) OR CM 13 AND CM 8
	10.) *Stolen C-ITS station*	CM 8 OR CM 4 AND CM 6 AND (CM 9 OR CM 10)
	11.) *Valid activity causing bad results on other C-ITS stations*	CM 8 OR CM 4 AND CM 6 AND CM 15 AND (CM 9 OR CM 10)

Table 3: General mapping of counter measures to incident scenarios

7.2 Specific Mappings

This section serves to reflect specific stakeholder views which propose that either the general mapping or a specific subset of counter measures is needed to cope with the incident scenarios for C-ITS deployment.

7.2.1 Telematics equipment manufacturers' view

From the view of Telematics equipment manufacturers only a subset of the entire general mapping of counter measures to incident scenarios (Table 3) would need to be taken into account for the deployment of C-ITS. This subset is reflected in Table 4.

The Telematics equipment manufacturer's design supports passive revocation of C-ITS stations including misbehaviour detection and active revocation of CAs.

	Incident Scenario	Countermeasure
CA Level	1.) *Compromise of a CA in the Trust Model.*	CM 3 AND (CM 1 OR CM 2)
	2.) *'Broken' cryptographic algorithm*	CM 3 AND (CM 1 OR CM 2)
	3.) *Migration to other CAs or trust model structures*	CM 3 AND (CM 1 OR CM 2)
C-ITS station Level	4.) *Malicious or misbehaving*	CM 5 AND CM 6 AND CM 7 AND CM 9
	5.) *C-ITS end-of-life policies*	CM 4 AND CM 6 AND CM 9
	6.) *C-ITS station repair policies*	-
	7.) *Hacking of C-ITS station – extracting of cryptographic material*	CM 11
	8.) *Hacking of C-ITS station – modification of permissions*	CM 12
	9.) *Hacking of C-ITS station – false inputs / detaching from vehicle*	CM 14
	10.) *Stolen C-ITS station*	CM 4 AND CM 6 AND CM 9
	11.) *Valid activity causing bad results on other C-ITS stations*	CM 4 AND CM 6 AND CM 9

Table 4: Telematics equipment manufacturers' view

7.2.2 Vehicle manufacturers' view

From the view of vehicle manufacturers only a subset of the entire general mapping of counter measures to incident scenarios (Table 3) would need to be taken into account for the deployment of C-ITS. This subset is reflected in Table 5.

The C2C-CC security design supports passive revocation of C-ITS stations and active revocation of CAs.

	Incident Scenario	Countermeasure
CA Level	1.) *Compromise of a CA in the Trust Model.*	CM 3 AND (CM 1 OR CM 2)
	2.) *'Broken' cryptographic algorithm*	CM 3 AND (CM 1 OR CM 2)
	3.) *Migration to other CAs or trust model structures*	CM 3 AND (CM 1 OR CM 2)
C-ITS station Level	4.) *Malicious or misbehaving*	-
	5.) *C-ITS end-of-life policies*	CM 4 AND CM 6 AND CM 9
	6.) *C-ITS station repair policies*	-
	7.) *Hacking of C-ITS station – extracting of cryptographic material*	CM 11
	8.) *Hacking of C-ITS station – modification of permissions*	CM 12
	9.) *Hacking of C-ITS station – false inputs / detaching from vehicle*	CM 14
	10.) *Stolen C-ITS station*	CM 4 AND CM 6 AND CM 9
	11.) *Valid activity causing bad results on other C-ITS stations*	-

Table 5: Vehicle manufacturers' view

7.2.3 Member State / Infrastructure / Implementation project view?

As agreed at last WG5 meetings the member states and implementation projects will check the possibility of adding more specific views reflecting the member state/infrastructure views.

7.2.4 US approach

The US approach also includes a subset of the entire general mapping of counter measures to incident scenarios (Table 3) would need to be taken into account for the deployment of C-ITS. This subset is reflected in Table 5.

The US approach supports active revocation of both C-ITS stations and CAs.

The US approach is still under development, especially with respect to end-of-life and station repair policies which there is no publicly agreed policy on. Countermeasure CM 13 is not used in the US approach.

	Incident Scenario	Countermeasure
CA Level	1.) *Compromise of a CA in the Trust Model.*	CM 3 AND (CM 1 OR CM 2)
	2.) *'Broken' cryptographic algorithm*	CM 3 AND (CM 1 OR CM 2)
	3.) *Migration to other CAs or trust model structures*	CM 3 AND (CM 1 OR CM 2)
C-ITS station Level	4.) *Malicious or misbehaving*	CM 5 AND CM 6 AND CM 7 AND (CM 9 or CM 10)
	5.) *C-ITS end-of-life policies*	(CM 9 or CM 10), possibly others to be determined
	6.) *C-ITS station repair policies*	To be determined
	7.) *Hacking of C-ITS station – extracting of cryptographic material*	CM 5 AND CM 6 AND CM 7 AND (CM 9 or CM 10) AND CM 11
	8.) *Hacking of C-ITS station – modification of permissions*	CM 5 AND CM 6 AND CM 7 AND (CM 9 or CM 10) AND CM 12
	9.) *Hacking of C-ITS station – false inputs / detaching from vehicle*	CM 5 AND CM 6 AND CM 7 AND (CM 9 or CM 10) AND CM 14
	10.) *Stolen C-ITS station*	Approach is to be determined
	11.) *Valid activity causing bad results on other C-ITS stations*	-

Table 6: US view

8 Conclusions and Recommendations

On the basis of the analysis provided in the previous sections, the WG5 experts recommend:

(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 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.