Federal Office
for Information Security

Technical Guideline BSI TR-03164:

Guidance for Cooperative Intelligent Transport Systems (C-ITS)

Part 2: Special Requirements for Cooperative Intelligent Transport Systems Stations

Version 1.0.0
08.12.2021

Document history

Version	Date	Description
1.0.0	08.12.2021	Initial public version

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
E-Mail: cits@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Index of Tables

1 Introduction

Cooperative Intelligent Transport Systems (C-ITS) enable vehicles to communicate with other vehicles (V2V) or infrastructure (V2X) on hazardous traffic situations as well as environmental or road conditions. The aim of C-ITS is to improve traffic safety.

To provide trust in the C-ITS communication, a binding framework of common rules, duties and roles for the different participants of the *European C-ITS Security Credential Management System (EU CCMS)*, including C-ITS subscribers and C-ITS stations, called *European Certificate Policy (EU CP),* was developed in a European working group. The C-ITS Public Key Infrastructure introduced in the EU CP ensures authenticity and integrity of the communication between the C-ITS members. Furthermore, each organization or member state is allowed to define additional requirements for its operation of a Public Key Infrastructure and C-ITS stations, as long as it is ensured that these additional requirements are not in contradiction with the European Certificate Policy [CP].

This Technical Guideline serves two purposes. On the one hand it gives a guidance on implementing the requirements of the [CP] for C-ITS station manufacturers and operators (C-ITS subscribers) and on the other hand it defines additional recommendations, which should be considered when manufacturing or operating a C-ITS station.

1.1 Scope and Structure of this Document

This Technical Guideline serves as a guidance for C-ITS station manufacturers and operators giving recommendations how to participate in a fully operative[1] C-ITS PKI and operate C-ITS stations in accordance with the binding “Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)” [CP].

A detailed overview of the C-ITS architecture, functionality and the relation between all C-ITS participants including the C-ITS subscribers and C-ITS stations is given in [TR-03164-1]. Beyond this, the requirements of the *Certificate Authorities (CA)* imposed on C-ITS subscribers and stations are specified in [TR-03164-1] as well. The present document addresses these requirements only shortly and references to the technical guideline.

The present document summarizes and accordingly references the most important requirements relevant for C-ITS subscribers from the following documents:

1. [CP]: The common European Certificate Policy specifies binding rules and duties for entities participating in the European C-ITS Security Credential Management System.
2. [ETSI TS 102 941]: This Technical Specification describes the trust and privacy management with respect to the establishment and maintenance of identities and cryptographic keys in a Cooperative Intelligent Transport System.
3. [TR-03164-1]: This Technical Guideline gives an overview of the C-ITS PKI structure and specifies requirements for the PKI operators. The present document references [TR-03164-1] if requirements for C-ITS subscribers are derived from PKI specifications.
4. [TR-03116-6]: This Technical Guideline profiles the cryptographic requirements from [CP], reflecting the algorithms and key lengths recommended for Cooperative Intelligent Transport Systems by the BSI.

Furthermore this document refines requirements of [CP] and provides additional recommendations.

Chapter 2 gives an introduction to security goals of C-ITS subscribers and C-ITS stations and classifies different C-ITS station types.

[1] The test (TLM level 0 Service) and ramp-up (TLM level 1 Service) phases of the European C-ITS PKI are not taken into account in this technical guideline.

Chapter 3 introduces different types of C-ITS messages and presents recommended verification steps.

Chapter 4 defines requirements for the subscription of C-ITS subscriber and the registration of C-ITS stations.

This is followed by chapter 5, which presents demands regarding maintenance of C-ITS stations.

Chapter 6 handles the revocation of C-ITS subscribers and C-ITS stations as well as the migration of C-ITS subscribers to a different home CA.

Chapter 7 gives a guidance on how to initially insert and regularly update certificates, C*ertificate Trust Lists (CTL)* and *Certificate Revocation Lists (CRL)* by C-ITS subscriber and C-ITS stations. The guidance includes the required verification steps as well as the behaviour in error cases. The chapter closes with the description of the C-ITS message signature validation.

Chapter 8 describes the service specific permissions for C-ITS messages like CAM and DENM.

Chapter 9 follows with the requirements of pseudonymisation in C-ITS stations and chapter 10 with the requirements of the remote access by C-ITS subscriber to C-ITS stations for maintenance. Chapter 11 points out the demands of secure elements in C-ITS stations.

1.2 Definitions and Abbreviations

The abbreviations and definition of terms that are relevant in this document are given below.

Abbreviation	**Definition**
AA	Authorization Authority
AT	Authorization Ticket
CA	Certificate Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport System
CP	Certificate Policy
CPA	C-ITS Certificate Policy Authority
CPOC	C-ITS Point of Contact
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CTL	Certificate Trust List
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	Enrolment Credential
ECR	Enrolment Credential Request
ECTL	European Certificate Trust List
EU AA	European Authorization Authority
EU CCMS	European C-ITS Security Credential Management System
EU CP	European Certificate Policy
EU EA	European Enrolment Authority

Abbreviation	Definition
EU RCA	European Root CA
ITS-AID	ITS-Application Identifier
IVI	In-Vehicle Information
OEM	Original Equipment Manufacturer
PKI	Public-Key Infrastructure
PSID	Provider Service Identifier
RCA / Root CA	Root Certificate Authority
RSU	Road Side Unit
SPAT	Signal Phase And Timing
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message
SSP	Service Specific Permission
Sub CA	Subordinate CA
TCC	Traffic Control Center
TLM	Trust List Manager
V2I	Vehicle-to-infrastructure communication
V2V	Vehicle-to-vehicle communication
V2X	Vehicle-to-everything communication

Table 1: Abbreviations

Term	Definition
Authorization Authority	In this document, the term 'Authorization Authority' (AA) refers not only to the specific function of the AA, but also to the legal and/or operational entity managing it.
Canonical data	The canonical ID, the canonical key pair and profile settings/data including service specific permissions (SSP), region restrictions and assurance level of a C-ITS station.
Canonical ID	The globally unique identifier of a single C-ITS station.
Certificate attributes	In general, certificate attributes represent information that is bound to the certificate holder. End-entities in a C-ITS PKI contain certificate attributes such as validityPeriod, region, assuranceLevel (optional), permissions.Certificate attributesCertificate attributes
Certification Authority	Authority trusted by one or more entities to create and assign certificates. If not further specified, in this Technical Guideline this addresses all instances of certification authorities in the European C-ITS Security Credential Management Systems, i.e. Root CA, Enrolment Authority and Authorization Authority
C-ITS participants	Entities of the EU CCMS, i.e. the TLM, Root CAs, EAs, AAs and C-ITS stations.
C-ITS station administrator	The C-ITS station administrator is a role that is adopted by the operator of a C-ITS station in order to configure and maintain the C-ITS station.

C-ITS subscriber	Manufacturer or operator subscribing with an Enrolment Authority on behalf of one or more C-ITS stations. The manufacturer and operator can be the same instance being responsible for the C-ITS station in different stages of the C-ITS station life cycle.
C-ITS subscriber agreement	An agreement between the CA and the C-ITS subscriber that specifies the rights and responsibilities of the parties.
C-ITS subscriber certificate	A certificate that is self-signed or signed by the home EA of the C-ITS subscriber and used for the signature of messages between C-ITS subscriber and home EA
C-ITS trust model	The C-ITS trust model is responsible for establishing a relationship of trust between C-ITS stations. It is implemented through the use of a PKI composed of Root CAs, the CPOC, TLM, EAs, AAs and a secure network.
Cryptographic module	A secure hardware-based element within which keys are generated and/or stored, random numbers are generated and data is signed or encrypted.
Enrolment Authority	In this document, the term 'Enrolment authority' (EA) refers not only to the specific function of the EA, but also to the legal and/or operational entity managing it.
Home Root CA	The Root CA that issued the Sub CA certificate at which the C-ITS subscriber is registered
Home AA	The Authorization Authority at which the C-ITS subscriber is registered and from where the C-ITS station receives the Authorization Tickets.
Home CA	Home Root CA, home EA and home AA are cumulatively referred to as home CA.
Home EA	The Enrolment Authority at which the C-ITS subscriber is subscribed and will register its C-ITS stations. The C-ITS station receives the Enrolment Credential from the home EA.
Manufacturer	The manufacturer of road side units or vehicles containing the C-ITS station.
Mobile public station	This category of C-ITS stations contains vehicles which are used by public authorities like police or ambulance. The requirements in pseudonymity and unlinkability may differ for different operation purposes.
Mobile private station	This type of C-ITS stations are usually vehicles in private ownership with the highest demand for pseudonymity and unlinkability
Mobile RSU	The category of mobile road side units is operated by or on behalf of public authorities. Mobile road side units are most often road work warning units which can change their position during the operation (e.g. on a road works warning trailer).
Operator	The entity responsible for maintaining the operability of the C-ITS station.
Re-keying	*Re-keying* of a certificate is defined as issuing a new certificate based on a newly generated subscriber's key pair and a new validity period. The remaining content of the certificate (i.e. the attributes of the subscriber) stays unchanged.
Root Certification Authority	In this document, the term 'Root Certification Authority' (RCA) refers not only to the specific function of the CA, but also to the legal and/or operational entity managing it.
RSU	Stationary or mobile road side unit.
Stationary RSU	Stationary road side units are located at a fixed place for at least one week up to the complete lifetime and operated by or on behalf of public authorities (e.g. traffic lights or toll stations).
Sub CA	Enrolment Authority or Authorization Authority belonging to one Root CA.

Table 2: Definitions

2 Subscribers and stations in C-ITS

In *Cooperative Intelligent Transport Systems (C-ITS)* vehicles communicate with other vehicles, traffic signals, road side infrastructure and other road users to improve traffic safety. Therefore, C-ITS stations such as vehicles or infrastructure components send messages which are used by the recipients to create an overview of the local traffic situation.

Since C-ITS aims to assist drivers and to improve the regulation of traffic and thus, has a high impact on the driver's safety as well as on the traffic flow, it is very important to ensure the authenticity and integrity of the exchanged messages. In the C-ITS domain this shall be ensured by means of a Public Key Infrastructure as described in [TR-03164-1].

At the same time, the impact on privacy of the road users should be minimized. Because links between a vehicle and its user can be either directly or indirectly deduced, the following two key requirements that relate to privacy have to be satisfied:

- **Pseudonymity:** Pseudonymity claims that a C-ITS station may use a resource or service without disclosing its identity but can still be accountable for that use.
- **Unlinkability:** Unlinkability denotes that a C-ITS station may make multiple uses of resources or services without others being able to link the uses together.

However, the requirements regarding privacy can vary for different types of C-ITS stations, especially in terms of pseudonymity and unlinkability. In order to assign requirements to the different categories of stations in this Technical Guideline, the following categories of stations are defined within this document:

- **Mobile private stations:** This type of station is usually integrated in vehicles in private ownership with the highest demand for pseudonymity and unlinkability. This technical guideline considers the OEM of a vehicle also as operator of the mobile private station even after selling it to the vehicle owner. The category of mobile private stations contains besides the C-ITS stations in vehicles also other stations with similar requirements like after market onboard units for vehicles or devices for vulnerable road users.
- **Mobile public stations:** This category contains C-ITS stations that are integrated in vehicles which are used by public authorities like the police or ambulance. The requirements in pseudonymity and unlinkability may differ for different operation purposes. Hence, this technical guideline acts on the assumption that a high level of privacy, similar to the mobile private station, is required.
- **Mobile RSU:** The category of mobile *Road Side Units (RSU)* is operated by or on behalf of public authorities or the use is authorized by public authorities. Mobile RSUs are most often used in road work warning units which can change their position during the operation. Mobile RSUs have no requirements on privacy since they are usually not linked to a specific user.
- **Stationary RSU:** Stationary road side units are located at a fixed place for at least one week up to the complete lifetime. Stationary RSU can be operated on behalf of public authorities or on private property. The difference to mobile RSU is that the location shall not change during the operation. Stationary RSUs have no requirements on privacy like mobile RSUs but they have special requirements on security because attackers might physically access unattended stations and try to manipulate them.

Besides the requirements for C-ITS stations, the present Technical Guideline also defines demands for manufacturers and operators, both called C-ITS subscribers. The requirements embrace among others the initial installation of canonical data in the C-ITS stations and the registration of the C-ITS stations at the home *Enrolment Authority (EA)* by the C-ITS subscriber. Likewise, special requirements for the administration and configuration as well as termination of the C-ITS stations by the C-ITS subscriber are defined in this Technical Guideline.

3 C-ITS message validation

C-ITS stations use different message formats for the exchange of traffic information with other C-ITS participants. Each of the message types has its primary use in different domains like *Cooperative Awareness Messages (CAM)* in order to create awareness between C-ITS stations or *Signal Phase and Timing Messages (SPAT)* for the distribution of the traffic signal status.

The following message formats are used most often in the C-ITS domain:

- **Cooperative Awareness Message** (CAM, [ETSI EN 302 637-2]): Message type to create and maintain awareness between C-ITS stations. A CAM contains status and attribute information of the originating C-ITS station. On reception of a CAM the receiving C-ITS station becomes aware of the presence, type, and status of the originating station. The received information can be used by the receiving C-ITS station to support several ITS applications.
- **Decentralized Environmental Notification Message** (DENM, [ETSI EN 302 637-3]): An application support facilities layer message that is mainly used by C-ITS applications in order to alert road users of a detected event.
- **Signal Phase And Timing** (SPAT, [ETSI TS 103 301]): Informs drivers of the current status of the traffic signal ahead as well as when the next signal stage change will occur in the current path.
- **Map** (MAP, [ETSI TS 103 301]): Describes the topology of one or more intersections.
- **In-Vehicle Information** (IVI, [ETSI TS 103 301]): A message format to deliver information about the infrastructure to vehicles. IVI messages can provide information about existing, fixed and dynamic traffic signs to passing vehicles. This information can be processed by driver assistance systems in the vehicles and relevant data can be presented to the driver.
- **Traffic Light Control** (TLC, [ETSI TS 103 301]): The TLC service supports prioritization of public transport and public safety vehicles (ambulance, fire brigade, etc.) to traverse a signalized road infrastructure (e.g. intersection) as fast as possible or using a higher priority than ordinary traffic participants. The corresponding *Signal Request Extended Message (SREM)* is sent by a C-ITS station (e.g. vehicle) to request traffic light signal priority (public transport) or signal preemption (public safety). In response to the request the infrastructure will acknowledge with a *Signal Request Status Extended Message (SSEM)* notifying if the request has been granted, cancelled or changed.

Since the reception of the traffic control messages can influence the behaviour of a C-ITS station, like speed reduction or change of the signal phases, the C-ITS station must verify the correctness and trustworthiness of the received message before processing any of the information from the message.

The C-ITS station shall perform appropriate validation steps considering the following aspects in order to verify the correctness of the received C-ITS messages:

- **Validation of signature:** The received message must contain a signature that shall be verified as defined in [TR-03164-1], section “Signature Validation”.
- **Validation of message format:** The format of the received message must be valid as per message format specification.
- **Service specific permission validation:** Messages with data fields or data elements that require special permissions must contain the respective permissions in the *Service Specific Permissions (SSP)* element of the signing certificate (see section 8).
- **Validation of consistency:** The content of the received message shall be verified with regard to consistency. This means that information within the received message shall not contradict each other.
- **Validation of timestamp:** The C-ITS station shall check the timestamp of the C-ITS message against the reception time and accept only CAMs not older than 2 seconds and other messages within the last 10 minutes.

- **Validation of plausibility:** The content of the message shall be verified in terms of plausibility. This means that the data within the message shall not contradict with the environment the station is located in (e.g. the location given in the message must be close to the location of the C-ITS station).
- **Validation of quality:** If the data elements' quality levels are not sufficiently good, the receiving applications, according to their purpose, may ignore them (fault tolerance principle) in order to avoid the issue of false indication to the driver. CAM and *Decentralized Environmental Notification Message (DENM)* provide data elements with their associated levels of quality as well as the confidence levels which can be associated to these data elements.

The C-ITS station shall only accept and process the received traffic data, if all above mentioned verification steps succeeded. If any of the verification steps fails, the complete message shall be rejected and the forwarding to other C-ITS stations shall be omitted.

4 Subscription and Registration process

C-ITS subscriber which intend to operate C-ITS stations in the *C-ITS Public-Key Infrastructure (C-ITS PKI)* must run through a subscription and registration process beforehand. The subscription of the C-ITS subscriber is the first phase of the process and consists of the identification of the C-ITS subscriber at a home *Enrolment Authority (EA)* and in case of positive validation the admittance of the subscriber as participant of the European C-ITS PKI. In the second phase, which is the registration of C-ITS stations, the successfully subscribed C-ITS subscriber is allowed to register and enrol its C-ITS stations at the home EA.

C-ITS subscriber subscription process

In order to establish trust in the subscription of the C-ITS subscriber, a representative of the C-ITS subscriber must identify himself at the home EA. A detailed description of the subscription process including a line-up of all required documents is given in [TR-03164-1].

During the subscription process, a C-ITS subscriber certificate shall be exchanged between the C-ITS subscriber and the home EA as described in [TR-03164-1]. The C-ITS subscriber certificate shall be used to ensure the integrity and authenticity of the communication between C-ITS subscriber and home EA. Once being in possession of the C-ITS subscriber certificate, the C-ITS subscriber shall sign all messages to the home Enrolment Authority in order to ensure authenticity and integrity of the data.

After being successfully subscribed at the home Enrolment Authority, the C-ITS subscriber is allowed to register its C-ITS stations at the home EA.

Canonical data generation

For the registration of C-ITS stations so-called canonical data are required that are established in the C-ITS station by the manufacturer or by the operator, depending on the purpose of the C-ITS station. The C-ITS subscriber shall set up appropriate security measures to ensure confidentiality, authenticity and integrity of the canonical data.

The following canonical data are mandatory and shall be established in a secure process within the C-ITS station:

- **Globally unique canonical identifier** composed of the globally unique C-ITS subscriber prefix and a subscriber internal unique identifier for the C-ITS station.
- **TLM certificate** as trust anchor
- **CPOC network address** or the **subscriber interface network address**
- **Information about the home CA[2] instances** in order to identify them unambiguously consisting of one or more of the following data:
  - public key certificates
  - hashedIDs of the certificates
  - names of the CA instances that are used in the certificate

The following canonical data can be transmitted optionally to the C-ITS station:

- **Certificate attributes** consisting of the Service Specific Permissions, region restrictions and the assurance level which depends on the C-ITS station type and the intended use.
- **Network address of all home CA instances** for the download of data
- **Root CA certificates** from all or a subset of CAs that are present in the *European Certificate Trust List (ECTL)*

[2] Home Enrolment Authority, home Authorization Authority and home Root CA

- **Authorization Authority certificates** from known and trusted Root CA certificates which the C-ITS station may use to trust in communication from other C-ITS stations

The profile information can also be placed at the EA for all or a type of C-ITS stations of a C-ITS subscriber. The C-ITS subscriber shall unambiguously define to which group of C-ITS stations the profile information apply. All profile information shall be signed by the C-ITS subscriber certificate when it is transmitted to the EA to ensure authenticity and integrity. If the optional profile information is not part of the certificate request of the C-ITS station, the EA takes the previously transmitted and stored profile information.

The canonical data includes a canonical key pair. But in contrast to the data mentioned before, which are generated and gathered by the C-ITS subscriber, the canonical key pair should be calculated directly in the secure element of the C-ITS station. After creation, the canonical public key is transmitted securely to the C-ITS subscriber for the registration of the C-ITS station. If the generation in the secure element of the C-ITS station is not possible, the canonical key pair can be generated in a secure element of the C-ITS subscriber. The key material shall be transferred via an integrity and authenticity secured environment from the C-ITS subscriber to the C-ITS station. In both cases, the requirements described in chapter 11 shall be followed.

For the determination of the C-ITS station SSP the C-ITS subscriber shall ensure that the permissions are equal or less restrictive than the permissions the C-ITS subscriber received from the home EA during the subscription process. The subscriber must also ensure that a private C-ITS station does not get any permissions that are reserved for public use. If a C-ITS station requires special permissions (i.e. for road closures or siren bar use) the C-ITS subscriber needs to be registered at an EA that is entitled to issue the requested permissions.

C-ITS station registration process

Once the canonical data is composed, the C-ITS subscriber can initially register the C-ITS station at the EA. The C-ITS subscriber shall use the registration process that is provided by the home EA and is subject of the EA certification. The C-ITS station registration process shall ensure authenticity and integrity of the registration message and the provided data of the C-ITS station.

The C-ITS stations shall be registered at the EA according to [TR-03164-1]. That is by sending a C-ITS station registration message[3] from the C-ITS subscriber to the home Enrolment Authority. This message shall be signed with the C-ITS subscriber's private key and encrypted with the public key of the home EA. The registration message contains registration data which consist of the globally unique canonical identifier, the canonical public key and optionally the profile information. The EA notifies the C-ITS subscriber in a registration reply message if the registration of the C-ITS station was successful or not.

Each C-ITS station shall be registered at only one Enrolment Authority. Special purpose vehicles (such as police cars and other special purpose vehicles with specific rights) may be registered at an additional EA or have one additional C-ITS station for authorizations within the scope of the special purpose.

C-ITS station enrolment

Before a C-ITS station can go into operation and sign C-ITS messages, the station must be enrolled at the home Enrolment Authority. For this purpose, the C-ITS station sends an *Enrolment Credential Request (ECR)* containing the registration data to the home EA. The ECR shall contain the canonical ID and an outer signature signed with the canonical private key in order to identify itself at the home EA. The Enrolment Authority compares and verifies the data from the ECR with the registration data received from the C-ITS subscriber and provides an *Enrolment Credentials (EC)* to the C-ITS station if all data is correct. Once the C-ITS station is in possession of the EC, it shall request *Authorization Tickets (AT)* at the *Authorization Authority (AA)* which are used to sign traffic control messages. A detailed description of the Enrolment Credential Request, the enrolment process at the Enrolment Authority and the inquiry of ATs at the Authorization Authority can be found in [TR-03164-1].

[3] Currently the exact message format of the registration message has to be defined by the EA.

5 Update of C-ITS stations

In order to ensure the security of C-ITS stations over their complete lifetime, a software update mechanism has to be implemented by the C-ITS subscriber. When a security vulnerability in the C-ITS station software is detected it must be possible to securely update the software in the C-ITS-station. In cases where the CPA prescribes the update of cryptographic algorithms, key length or cryptographic parameters, the CPA will specify a transition period for the update of the algorithm and/or key length. In order to be able to continue the operation of the C-ITS subscriber and C-ITS stations after that period, the PKI participants should use and implement hardware and software that is capable of a changeover of key lengths and algorithms.

In case of necessity of a remote access to the C-ITS station, e.g. to change the configuration, this shall only be possible for authorized and instructed administrators via a secured channel.

The detailed requirements are described in the following:

1. Road operators and the C-ITS station supplier shall ensure that secure software updates are possible for the C-ITS stations.
2. When the C-ITS subscriber detects a vulnerability in a C-ITS station, these actions shall be taken:
   - An analysis of the vulnerability shall be started.
   - The C-ITS subscriber shall inform the home EA operator about the vulnerability and provide all relevant information about the issue in order to enable the EA operator to take a decision if a revocation of the affected C-ITS stations is required. In case of a revocation the revocation process described in 6.1 or 6.2 respectively, shall be performed.
   - The manufacturer of the C-ITS station shall implement and publish a security fix.
   - The C-ITS station operator shall install a security fix to the C-ITS stations as soon as possible.
   - After the successful update all revoked C-ITS stations must be re-registered in the same way like the initial registration was done.
3. The C-ITS station operator shall regularly check for software updates provided by the C-ITS station manufacturer and install them promptly after receipt on all operated C-ITS stations.
4. The C-ITS station operator is responsible for the installation of firmware updates in the C-ITS stations.
5. The update packages for C-ITS stations shall be created and issued under the conditions of the secure update process that has been certified within the Common Criteria certification of the C-ITS station.
6. Each remote communication channel between the C-ITS station and the administrator's maintenance interface shall be authenticity and integrity protected. It is recommended to use Transport Layer Security (TLS). The TLS versions 1.2 or 1.3 shall be used with the cryptographic algorithms and key-lengths recommended within the latest version of [TR-02102-2].
7. It shall be ensured that the administrator of the C-ITS station is trustworthy, non-hostile and well-trained which shall be indicated by the subscription of the C-ITS subscriber at the EA.
8. The C-ITS station shall support secure firmware updates, which requires the following properties:
   - Firmware update signatures are verified to ensure authenticity and integrity prior to installation
   - C-ITS station administrator authentication is required to upload the firmware update data
9. In order to enable and facilitate the transfer to new algorithms and/or key lengths, it is recommended that all C-ITS participants implement hardware and/or software that is capable of a changeover of key lengths and algorithms.

Special requirements for road side units

For *Road Side Units (RSU)* additional requirements apply to the connection by RSU operators from traffic control centres. Additionally, the information about the environment of the C-ITS station that is sent to the traffic control centre shall be secured in an adequate way. The approval of a software update provided by the C-ITS station manufacturer shall be managed according to a change management process between C-ITS station manufacturer and the C-ITS station operator. The change management process shall include the contracting body in the approval process of software updates.

1. The RSU shall implement functionality to protect its security functions against malfunctions and tampering. Specifically, the RSU shall
   - overwrite relevant information that is no longer needed to ensure that it is no longer available
   - implement and perform a self-test on a regular basis (e.g. verify correctness of stored certificates, ensure integrity of installed software and hardware)
   - physically protect the secret key material within the secure element against tampering
   - implement mechanisms to detect physical manipulation
   - ensure that the C-ITS station falls into a secure state in case of a security relevant malfunction
   - write a log of events that have effect on the security of the RSU (e.g. tries of unauthorized access, manipulated certificates)
2. For the access of RSU operators to the RSU, the following requirements apply:
   - an authorized RSU operator is allowed to have access via wide-area communication or local interfaces, but is not allowed to read, modify or write stored and/or processed assets within the RSU. Exempt from this, the assets status, logging, maintenance and update information may still be read, modified or stored.
   - an authorized traffic control centre is only allowed to interact with the RSU via a secured wide area network (WAN) interface.

6 Revocation and Migration of C-ITS subscribers and C-ITS stations

This chapter describes measures that shall be followed by C-ITS subscriber and C-ITS stations in case of revocation from the C-ITS Public Key Infrastructure or which are migrating to another home Sub CA. The goal of the described revocation procedure is to remove the C-ITS subscriber and C-ITS stations securely and fully from the PKI, if they are not longer considered trustworthy. The migration process allows the C-ITS subscriber the change of the home Sub CA with a continuous operation of the C-ITS stations.

If the contract between C-ITS subscriber and home Sub CA expires, the C-ITS subscriber has three alternatives:

- Continuation of the contract
- Migration to another EA and/or AA
- Termination of its operation

If the contract shall be continued, the C-ITS subscriber must extend the contract with the home EA and AA and comply with the conditions of the new contract.

In case of a migration to another Sub CA, the C-ITS subscriber shall follow section 6.3. For the termination of the C-ITS subscriber service, the C-ITS subscriber must be revoked together with its C-ITS stations as described in subsections 6.1 and 6.2.

6.1 Revocation of C-ITS subscriber

Revocation of the C-ITS subscriber shall be performed in cases where a removal of the C-ITS subscriber from the C-ITS PKI is required. On the one hand, the reason for a revocation can be a security incident like security issues or the breach of the requirements specified by the home CA. On the other hand the end of service of the subscriber and its stations can be a cause for the revocation. A full overview of the reasons that result in the revocation of the ITS-subscriber is given in [CP].

The revocation of a C-ITS subscriber can either be initiated by the home EA or by the C-ITS subscriber itself. In the first case the home EA must inform the C-ITS subscriber about the revocation and provide information on the reason for the revocation. This includes a notice if the C-ITS stations operated by the C-ITS subscriber must be revoked as well.

C-ITS subscriber that are revoked because of a security issue can keep the C-ITS stations operational as long as the detected security issue does not influence the security of the C-ITS station operation. The subscriber must continue to maintain and update the C-ITS stations during the time of revocation. When the security issue influences the C-ITS stations or the maintenance and the update of the C-ITS stations cannot be continued, the C-ITS stations must be revoked as described in section 6.2.

When the revocation is performed because the C-ITS subscriber is coming to the end of service the C-ITS subscriber should inform the home EA and AA operators about the planned termination before the revocation takes place. Additionally all C-ITS stations operated by the subscriber must be revoked in that case as described in section 6.2.

During the revocation of the C-ITS subscriber the following steps shall be performed:

1. The C-ITS subscriber shall revoke the C-ITS subscriber certificate at the home EA as defined in [TR-03164-1].
2. The C-ITS subscriber shall delete the C-ITS subscriber's private key from the secure element when the certificate revocation was successful.

3. If the C-ITS stations must be revoked as well, they must be notified by the C-ITS subscriber in order to start the revocation process in the C-ITS station depicted in 6.2.

In cases where the C-ITS subscriber intends to continue the service after the revocation, the C-ITS subscriber must subscribe at the same or another EA in the same way like the initial subscription. If the C-ITS stations were operational with a non revoked EC during the subscriber revocation, a new registration of the C-ITS stations is not necessary unless they are migrated to a different EA. Only if the C-ITS stations were also revoked they have to be newly registered at the (new) home EA.

6.2 Revocation of C-ITS stations

The revocation of Enrolment Credentials shall be performed when the C-ITS station is taken out of operation or when it is suspected to be affected by security issues.

In order to detect security issues, the C-ITS subscriber shall implement processes to detect vulnerabilities in the C-ITS stations like insufficient protocol versions, security algorithms or parameters. For road side units the operator shall monitor the C-ITS stations remotely and revoke broken, stolen or manipulated stations. If the severity of the detected security issue influences the integrity of the C-ITS station, the C-ITS subscriber shall revoke the concerned C-ITS stations and send a notification to the C-ITS station.

The C-ITS station shall also contain techniques to detect security breaches by itself (e.g. during startup an unauthorized software version is detected) and be able to notify the C-ITS subscriber about the issues. When the C-ITS subscriber receives the notification, it shall start analysing and fixing the issue.

The C-ITS subscriber shall perform the following steps if an EC shall be revoked[4]:

1. The C-ITS subscriber shall revoke the EC of a C-ITS station at the home EA by means of an authenticated and integrity protected message according to [TR-03164-1].
2. After the successful revocation of the EC at the home EA, the C-ITS subscriber should send a notification about the successful revocation to the C-ITS station in order to deactivate the station.

As soon as the C-ITS station detects a vulnerability by itself or it receives the notification of its revocation from the C-ITS subscriber, the following steps shall be performed in the C-ITS station:

1. The C-ITS station or the C-ITS station administrator shall delete the EC private key from the secure element of the C-ITS station.
2. The C-ITS station or the C-ITS station administrator shall delete all ATs and the corresponding private keys from the secure element.
3. The C-ITS station shall stop requesting new EC and AT certificates.
4. The C-ITS station shall stop sending C-ITS messages.

When the reason for the revocation is solved, the C-ITS station can be re-registered by the ITS-subscriber in the same way like the initial registration at the home EA.

6.3 Migration of C-ITS subscriber and C-ITS station

The migration of the C-ITS subscriber from the home Sub CA to another Sub CA is the termination of the C-ITS subscriber at the home Sub CA and the re-subscription at a new Sub CA. The migration process allows the C-ITS subscriber and the C-ITS stations to stay operational during the migration process.

In order to ensure the continuation of the C-ITS subscriber operation and the related C-ITS stations during the migration, the process is split in two parts. The first is the preparation phase and should be processed sufficiently in advance of the migration date. The second phase is started right after the migration date and

[4] Either the C-ITS subscriber initiates the revocation by itself or it is notified by the C-ITS station about the need of a revocation.

should be performed as promptly as possible to avoid a down time of the C-ITS stations. As the ATs signed by the old home AA will not be revoked there is a sufficient time period to load new ATs used to sign C-ITS messages.

A C-ITS subscriber can migrate only to another EA or to only another AA or both at the same time. The following two sub-chapters describe the processes for the migration of EA and AA separately.

6.3.1 C-ITS subscriber migration to another EA

For the migration of the home EA, the C-ITS subscriber and the C-ITS stations need to run through the following steps:

Preparation of the Migration:

1. A new EA must be chosen and the complete subscription process has to be followed as described in [TR-03164-1].
2. The C-ITS subscriber shall inform the old home EA about the planned migration date if the C-ITS subscriber is still operational.
3. The C-ITS subscriber shall download and validate the new EA certificate by verifying the presence on the Root CA CTL and running through the steps described in section “Certificate Validation” of [TR-03164-1]. If the corresponding Root CA changed, the C-ITS subscriber must download and use the new Root CA certificate, Root CA CTL and Root CA CRL for the validation of the EA certificate.
4. The new EA and the C-ITS subscriber shall setup an authenticated and integrity protected communication channel, e.g. by exchanging a new C-ITS subscriber certificate as defined in [TR-03164-1].
5. For each registered C-ITS station new canonical data[5] must be created and transmitted from the C-ITS subscriber to the C-ITS station and the EA in the same way like the initial canonical data creation.
6. The C-ITS stations must receive the information about the new home EA and the corresponding certificates from the C-ITS subscriber.
7. The C-ITS stations shall verify the new EA certificate and the chain as described in section “Certificate Validation” of [TR-03164-1].

Migration becoming effective:

1. The C-ITS subscriber shall revoke the old C-ITS subscriber certificate at the old home EA when the migration becomes effective. When the communicated migration date is reached, the EA shall revoke the C-ITS subscriber certificate, if it is not yet revoked.
2. The C-ITS subscriber shall delete the old C-ITS subscriber certificate’s private key from its secure element.
3. The C-ITS subscriber shall revoke the old EC of the affected C-ITS stations at the EA (e.g. by sending an EC revocation request).
4. The EC signed by the old EA shall be deleted together with the corresponding private key in the C-ITS station once the revocation request was approved by the EA.
5. The C-ITS station shall request a new EC from the new EA by using the new canonical key pair.
6. The C-ITS station shall sign new AT request messages with the new EC.

[5] The canonical key pair should be created newly in the secure element of the C-ITS station. If this is not possible, the canonical key pair can be re-used for the new canonical data if the key length and algorithm still have an appropriate level of security. For more details see [TR-03164-1].

6.3.2 C-ITS subscriber migration to another AA

For the migration from the home AA to another AA, the C-ITS subscriber needs a new contractual agreement with the new home AA. The C-ITS station must redirect its AT requests from the old AA to the new AA instance.

For the migration of the home AA, the C-ITS subscriber and the C-ITS stations need to run through the following steps:

Preparation of the Migration:

1. A new AA must be chosen and the complete subscription process has to be followed as described in [TR-03164-1].
2. The EA operator shall be informed about the migration to the new AA and requested for acceptance of the new AA operator. All necessary information about the AA contractual agreement as defined by [TR-03164-1] must be provided to the EA operator.
3. The old home AA shall be informed about the migration to a new AA.
4. After the acceptance of the migration by the EA, the C-ITS subscriber shall receive and validate the new AA certificate as depicted in section “Certificate Validation” of [TR-03164-1]. If the corresponding Root CA changed, the C-ITS subscriber must download the new Root CA certificate, Root CA CTL and Root CA CRL for the validation of the AA certificate. The new Root CA certificate, CTL and CRL must be validated as described in section “Certificate Validation” of [TR-03164-1].
5. The C-ITS stations must receive the information about the new home AA and the corresponding certificates from the C-ITS subscriber and validate them according to “Certificate Validation” of [TR-03164-1].

Migration becoming effective:

1. The C-ITS station shall request new AT certificates at the new AA.
2. The ATs signed by the old home AA can still be used until the end of the validity time by the C-ITS station, but it is recommended to replace them with the ATs from the new AA as soon as possible.

7 Certificate Management Process of C-ITS subscriber and -stations

In this chapter the update and validation process of certificates, *Certificate Trust Lists (CTL)* and *Certificate Revocation Lists (CRL)* for C-ITS subscriber and C-ITS stations is described. In addition the validation process of the signature of C-ITS messages that shall be performed by C-ITS stations is described. All sub-sections reference the “Validation” chapter of [TR-03164-1] which describes the validation procedure of certificates, CTLs and CRLs step by step.

The first sub-chapter describes how certificates, Certificate Revocation Lists and Certificate Trust Lists of the CPOC and the CA members are initially loaded to the C-ITS subscriber during the registration at the EA and to the C-ITS station during the production. Additionally, the update of the data at the C-ITS subscriber and the C-ITS station is depicted in the second sub-chapter. For the verification procedure description it is assumed that the data were successfully downloaded from the web-interfaces and the message is valid. In cases where the communication fails or the received message is faulty, following requirements apply:

- **no connection:** If the connection to any web interface, used for the update of certificates, trust lists or revocation lists, is not available for three days or longer, the relating data shall be rejected and all received messages authenticated with the rejected data shall be declined.
- **no reply of web interface:** If any web interface hosting certificates, trust lists or revocation lists does not reply the requested data for three days or longer, the corresponding data shall be rejected and all received messages authenticated with the rejected data shall be declined.
- **invalid signature:** The behaviour of the C-ITS subscriber and C-ITS stations in case of an invalid signature will be described in the following sub-chapters.

The verifications described in the following sub-chapters shall be performed embracing the secure element of the C-ITS subscriber or the C-ITS station in order to ensure the reliability of the received data and the validation itself. Moreover, all C-ITS stations supplied with certificate data by a back-end system, shall verify the received data in the C-ITS station according to the following sub-chapters even if the validation was already performed in the back-end system.

7.1 Initial Certificate Insertion

7.1.1 TLM Certificate

In order to establish initial trust to the TLM, the C-ITS subscriber needs to ensure the authenticity and integrity of the initial TLM certificate. To achieve this, the C-ITS subscriber shall fetch the TLM certificate from the home EA or the home Root CA during the subscription process in a secured way. The C-ITS subscriber shall also load the TLM certificate from the CPOC web interface and ensure that it is identical to the one received from the EA or Root CA. Only if both are identical the certificate shall be verified.

During the manufacturing or initialisation process of the C-ITS station, the C-ITS subscriber shall transmit the validated TLM certificate to the C-ITS station.

Upon receipt of the TLM certificate the recipient shall always verify the correctness of the TLM certificate according to section “Certificate Validation” of [TR-03164-1]. If the validation succeeds, the TLM certificate shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.2 ECTL

The *European Certificate Trust List (ECTL)* should be downloaded by the C-ITS subscriber and C-ITS station from the CPOC web-interface. Alternatively the ECTL is transmitted in the same process like the initial TLM certificate to the C-ITS subscriber or C-ITS station (see section 7.1.1).

In both cases the recipient shall validate the ECTL according to chapter "Certificate Trust List Validation" of [TR-03164-1], on reception. The successfully validated ECTL shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.3 Root CA Certificate

The initial issuance of the home Root CA certificate at the C-ITS subscriber or C-ITS station can be done in two ways.

The first method is the transmission of the home Root CA certificate

- by the home EA to the C-ITS subscriber during the subscription process at the home EA or
- by the C-ITS subscriber to the C-ITS station during the registration process.

Upon receipt of the home Root CA certificate the recipient shall verify the correctness of the certificate according to "Certificate Validation" of [TR-03164-1].

The other method is loading the home Root CA certificate from the ECTL. The unique home Root CA's HashedID shall be securely transmitted

- by the home EA to the C-ITS subscriber during the subscription process at the home EA or
- by the C-ITS subscriber to the C-ITS station during the registration process.

After that the home Root CA certificate must be taken from the ECTL and validated as described in "Certificate Validation" of [TR-03164-1].

In both cases, if the validation succeeds the home Root CA certificate shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.4 Root CA Certificate Trust List

For the initial reception of the home Root CA *Certificate Trust List (CTL), the* C-ITS subscribers and C-ITS stations shall download the home Root CA CTL from the Root CA's web interface listed in the ECTL. The C-ITS subscriber and C-ITS station shall validate the CTL following section "Certificate Trust List Validation" of [TR-03164-1].

The successfully validated home Root CA CTL shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.5 Root CA Certificate Revocation List

For the initial reception of the home Root CA *Certificate Revocation List (CRL), the* C-ITS subscriber and C-ITS stations shall download the home Root CA CRL from the Root CA's web interface listed in the ECTL. The C-ITS subscriber and C-ITS station shall validate the CRL following section "Certificate Revocation List Validation" of [TR-03164-1].

[6] It is recommended to store the data in the secure storage of the secure element. If this is not possible (e.g. because of storage space) the data (the certificates itself or the hashedID of the verified certificates) can be stored outside the secure element but shall be encrypted using a symmetric key that is stored in the secure element (see section 11).

The successfully validated home Root CA CRL shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.6 Home EA and home AA certificates

The initial issuance of the home EA and home AA certificates at the C-ITS subscriber or C-ITS station can be done in two ways.

The first method is the transmission of the home EA and home AA certificates

- by the home EA to the C-ITS subscriber during the subscription process at the home EA or
- by the C-ITS subscriber to the C-ITS station during the registration process.

Upon receipt of the home EA and AA certificates the recipient shall verify that the received certificate is an exact copy of the one in the home Root CA CTL. Additionally the correctness of the certificate shall be validated according to “Certificate Validation“ of [TR-03164-1].

The other method is loading the home EA and home AA certificates from the home Root CA CTL. Home EA and home AA unique identifier shall be securely transmitted

- by the home EA to the C-ITS subscriber during the subscription process at the home EA or
- by the C-ITS subscriber to the C-ITS station during the registration process.

After that the home EA and home AA certificates must be taken from the home Root CA CTL and validated as described in “Certificate Validation” of [TR-03164-1].

In both cases, if the validation succeeds the home EA and AA certificates shall be securely stored under protection of the secure element from malicious manipulation[6].

7.1.7 Enrolment Credentials

The initial enrolment credential (EC) request is executed by the C-ITS station after the successful registration at the EA in order to become operational. Before the C-ITS station can build the enrolment request message it must generate a new key pair in the secure element. Then the C-ITS station creates the EC request message and enriches it with the canonical data which were created during the registration process. At the end the message will be signed according to [TR-03164-1] with the private canonical key and the new private key.

After reception of the message, the EA validates the signatures on the EC request message and compares the canonical data to the data which were transferred during the registration process. If the validation succeeded, the EA will sign the EC certificate and provide it to the station in an enrolment credential reply message. The certificate shall be validated according to the chapter “Certificate Validation” of [TR-03164-1] and in case of success the Enrolment Credential shall be stored in the C-ITS station under protection of the secure element from malicious manipulation[6].

7.1.8 Authorization Tickets

There are no authorization tickets initially loaded by the subscriber to the C-ITS station. The first Authorization Ticket request is equal to the consecutive authorization requests messages.

7.1.9 C-ITS subscriber certificate

The C-ITS subscriber shall create a C-ITS subscriber certificate according to [TR-03164-1] and store the corresponding private key in its secure element.

The C-ITS subscriber certificate shall then be used for the secure communication between C-ITS subscriber and home EA.

7.2 Certificate Re-keying

The following subchapters describe regular updates of the certificates, CTLs and CRLs handled by the C-ITS subscribers and C-ITS stations. Besides the deletions performed during the evaluation of the received data in the following sub-chapters, the C-ITS subscriber and C-ITS stations shall regularly check for outdated certificates, CTLs and CRLs and delete them in case of expiration.

In cases where C-ITS subscriber or C-ITS stations make use of stored certificates, CTLs or CRLs in order to verify a certificate chain or signatures, they must always check if the data has expired. If the validity period expired, the affected data shall be removed and the certificate chain or signature verification shall be performed with newly loaded data.

7.2.1 TLM Certificate

The CPOC offers the C-ITS participants two different methods to update the TLM certificate. C-ITS participants shall support at least one of the methods and can optionally support the second method as fall back option.

One method is the publication of the old, a new and a link certificate message via the CPOC web interface. In this case, the C-ITS participant must regularly check if a re-keyed certificate is published by the CPOC and download the new certificate and the link certificate message. If the C-ITS subscriber or C-ITS station chooses this option, the following verifications have to be done on the downloaded files:

1. the old certificate shall be permitted to issue link certificates (see [CPOC])
2. the new self-signed TLM certificate shall be verified as defined in “Certificate Validation” of [TR-03164-1]
3. the TLM link certificate message shall be signed with the currently valid and trusted TLM private key and contain the hash of the new TLM certificate as well as the expiration date of the signer certificate.

The other method to update the re-keyed TLM certificate is by means of a special ECTL. Every time the TLM re-keys its certificate, the CPOC publishes an ECTL which contains besides the root CA certificates, additionally the new TLM certificate. As the ECTL is signed with the old TLM private key and contains the new TLM certificate, a trust relationship between old and new certificate is established. When choosing this option, the ECTL shall be verified as described in chapter “Certificate Trust List Validation” of [TR-03164-1] and then the following steps shall be performed to ensure the correctness of the new TLM certificate:

1. the old and new certificates must be issued with the same name in the certificate
2. the new self-signed TLM certificate shall be verified as defined in section “Certificate Validation” of [TR-03164-1].

If a C-ITS station’s backend is existing that extracts the new TLM certificate from the ECTL and validates it before sending it to the C-ITS station, the C-ITS station shall still validate the new TLM certificate with the TLM link certificate available on the CPOC web interface according to the first method.

In both cases after the successful verification the new TLM certificate shall be securely stored under protection of the secure element from malicious manipulation[6.] The old TLM certificate shall be deleted right after the end of the validity period given in the TLM certificate.

Fault behaviour

If any of the validation steps of the newly received TLM certificate or the TLM link certificate fails, the new certificate shall be discarded by the recipient. The active TLM certificate shall be kept valid until the end of the validity time.

In case the end of the validity time of the active TLM certificate is reached and the new TLM certificate is not successfully loaded, the active TLM certificate shall not be used any more. In that case the C-ITS station loses the trust anchor and needs to be manually re-configured by the C-ITS administrator to obtain the valid TLM certificate. A re-registration of the C-ITS station by the C-ITS subscriber is only necessary if the loss of the TLM certificate is suspected to be caused by a security issue.

7.2.2 ECTL

The ECTL is updated every three months by the TLM with an overlap time of one week to one month, where the recommended overlap time is 3-4 weeks. Additionally an earlier issuance can take place in not foreseen cases, like revocations of Root CA certificates. During the overlap time, the old ECTL still remains valid and the validity period of the new ECTL starts at the end of the overlap period. [CPOC]

The C-ITS subscriber shall ensure that the ECTL has been downloaded or obtained not more than **seven days** before communicating with the home EA. The C-ITS stations shall regularly update the ECTL at least every **seven days** either from the CPOC web interface, an interface provided by the C-ITS subscriber or via ITS G5 proxy application using the GeoNetworking protocol. The C-ITS subscriber and C-ITS stations shall verify the ECTL by performing “Certificate Trust List Validation” of [TR-03164-1]. After successfully validating the ECTL, the Root CA certificates listed in the ECTL shall be compared to the stored Root CA certificates.

The C-ITS subscriber shall check the following:

- Is the home Root CA certificate present in the new ECTL? If not, the certificate is not trustworthy and the C-ITS subscriber shall not trust the home CA instances any more (see fault behaviour below for the recommended behaviour).
- Is a re-keyed home Root CA certificate present in the ECTL? Then the re-keyed home Root CA certificate shall be validated according to [TR-03164-1] section “Certificate Validation”. If the validation succeeded, the certificate shall be securely stored under protection of the secure element from malicious manipulation[6].

The C-ITS station shall check the following:

- Is each Root CA certificate stored by the C-ITS station present in the new ECTL? If not, the certificate is not trustworthy anymore and the corresponding certificate shall be deleted.
- For a not trustworthy Root CA certificate the C-ITS station shall:
    - delete the Root CA certificate and all certificates of the Sub CAs which are belonging to the domain of the Root CA
    - not trust in C-ITS messages signed by C-ITS participants in the domain of that Root CA
    - stop sending C-ITS messages and requesting ECs and ATs if the revoked Root CA is the home Root CA. It might be necessary that the C-ITS subscriber migrates with the C-ITS stations as described in section 6.3.
- Is each certificate present in the ECTL stored in the C-ITS station? If not, the missing certificate shall be validated following the procedure of [TR-03164-1] section “Certificate Validation”. If the validation succeeded, the certificate shall be securely stored under protection of the secure element from malicious manipulation[6].
- Is a re-keyed Root CA certificate present in the ECTL? Then the re-keyed Root CA certificate shall be validated according to [TR-03164-1] section “Certificate Validation”. If the validation succeeded, the certificate shall be securely stored under protection of the secure element from malicious manipulation[6].

The valid ECTL shall be securely stored under protection of the secure element from malicious manipulation[6].

Fault behaviour

If the ECTL validation fails at any step, the new ECTL shall be refused. The recipient of a faulty ECTL shall continue to update the ECTL regularly until a new valid ECTL is received. The C-ITS subscriber and C-ITS stations shall not trust the loaded Root CA certificates if the validity period of the last successfully loaded ECTL has expired. In that case the C-ITS subscriber and C-ITS station have no valid Root CA certificates anymore and shall stop sending C-ITS messages.

In case that the ECTL is valid but the C-ITS subscriber detects the deletion of the home Root CA from the ECTL, the C-ITS subscriber shall contact the home EA and evaluate if the registration of C-ITS stations needs to be stopped or even a migration to another CA is necessary (see section 6.3). If possible, the C-ITS subscriber should also prevent the C-ITS stations from sending C-ITS messages as they would be rejected from the other C-ITS participants anyway.

If the C-ITS station detects that the home Root CA is revoked, the C-ITS station should send a notification to the C-ITS subscriber so that the subscriber can evaluate if a re-configuration or a migration to a new home CA is necessary.

7.2.3 Root CA Certificate

If a new Root CA certificate is loaded from the ECTL or directly from the web interface of the Root CA, the validation steps according to the section “Certificate Validation” of [TR-03164-1] shall be performed before securely storing the certificate under protection of the secure element.

In case of Root CA certificate re-keying, the new Root CA certificate is inserted by the CPOC in the ECTL. The new Root CA certificate entry in the ECTL shall also contain the field successorTo with the EtsiTs103097Certificate of the old, still valid, Root CA certificate. Through this insertion in the ECTL, a link between the old and the new re-keyed Root CA certificate is established inside the ECTL and the C-ITS subscriber and C-ITS stations can identify the re-keyed certificate of the home Root CA.

When the C-ITS subscriber or the C-ITS station detects a re-keyed Root CA certificate in the ECTL, besides the certificate validation, it shall be additionally checked, that the old certificate in the ECTL and the old certificate in the successorTo element of the re-keyed Root CA certificate entry are equal.

If the validation is successful, the re-keyed Root CA certificate shall be securely stored under protection of the secure element from malicious manipulation[6].

Fault behaviour

If a newly loaded Root CA certificate or re-keyed Root CA certificate is invalid, the certificate shall be refused and not be used or stored.

7.2.4 Root CA Certificate Trust List

The C-ITS subscriber shall ensure that the Root CA CTLs belonging to each of the stored Root CA certificates have been downloaded or obtained not more than **seven days** before communicating with the home EA. The C-ITS stations shall regularly update the Root CA CTLs at least every **seven days** from the corresponding Root CA web interface, an interface provided by the C-ITS subscriber or via ITS G5 proxy application using the GeoNetworking protocol. The C-ITS subscriber and C-ITS stations shall verify the CTL by performing “Certificate Trust List Validation” of [TR-03164-1].

If the validation is successful, all EA and AA certificates listed in the Root CA CTLs shall be compared to the EA and AA certificates stored at the C-ITS subscriber or C-ITS station.

The C-ITS subscriber shall perform the following checks:

- Is the home EA certificate present in the new Root CA CTL? If not, the certificate is not trustworthy and the C-ITS subscriber shall delete the home EA certificate.

- Is a re-keyed home EA certificate present in the Root CA CTL? If so, the certificate shall be verified according to 7.2.6.

The C-ITS station shall check the following:

- Is each EA or AA certificate belonging to the Root CA stored by the C-ITS station present in the new Root CA CTL? If not, the certificate is not trustworthy and the C-ITS station shall delete the certificate.
- Is a re-keyed EA or AA certificate present in the Root CA CTL? If so, the certificate shall be verified according to 7.2.6.
- Is an AA certificate present in the Root CA CTL which is not stored by the C-ITS station? If so, the certificate shall be verified according to 7.2.6.

The successfully validated Root CA CTL shall be securely stored under protection of the secure element from malicious manipulation[6].

Fault behaviour

If the received Root CA CTL is invalid, the new CTL shall be refused. The recipient of a faulty CTL shall continue to update the CTL regularly until a new valid CTL is received.

If the CTL of the home Root CA does not contain any valid home EA or home AA certificate the C-ITS subscriber should contact the home Root CA for a clarification of the reasons. If the home EA or AA was revoked a migration to another Sub CA might be necessary.

7.2.5 Root CA Certificate Revocation List

The C-ITS subscriber shall ensure that the home Root CA CRL is not older than **one day** before communicating with the home EA. The C-ITS stations shall update the Root CA CRLs belonging to each of the stored Root CA certificates at least **every day** from the corresponding Root CA web interface, an interface provided by the C-ITS subscriber or via ITS G5 proxy application using the GeoNetworking protocol. The C-ITS subscriber and C-ITS stations shall verify the CRL by performing “Certificate Revocation List Validation” of [TR-03164-1]. If the validation succeeded, the EA and AA certificates listed in the CRL shall be compared to the stored EA and AA certificates.

The C-ITS subscriber shall perform the following checks:

- Is either the home Root CA, home EA or home AA certificate present in the new Root CA CRL? If so, the C-ITS subscriber shall not trust the home Root CA, home EA or home AA any more (see fault behaviour below for the recommended behaviour).

The C-ITS station shall check the following:

- Is the Root CA certificate of the Root CA issuing the CRL present in the CRL? If so, the Root CA certificate was revoked and shall not be trusted anymore including all subordinate certificates.
- Is any of the stored AA certificates present in the Root CA CRL? If so the C-ITS station shall delete the affected certificate and shall not trust any C-ITS messages signed by participants of the removed AA.
- Is the home Root CA certificate present in the home Root CA CRL? If so, the Root CA certificate was revoked and shall not be trusted anymore and the C-ITS station shall not send any C-ITS messages and shall not request ECs or ATs. It might be necessary to migrate the C-ITS subscriber and the C-ITS stations to another home CA as described in section 6.3.2.
- Is the home AA present in the Root CA CRL? If so the C-ITS station shall delete the affected certificate and shall not send any C-ITS messages and shall not request new ATs. It might be necessary to migrate the C-ITS subscriber and the C-ITS stations to another AA as described in section 6.3.2.
- Is the home EA present in the Root CA CRL? If so, the C-ITS station shall delete the affected certificate and shall not trust the home EA and stop requesting new ECs and ATs.

The successfully validated Root CA CRL shall be securely stored under protection of the secure element from malicious manipulation[6].

Fault behaviour

If the Root CA CRL is invalid, the new CRL shall be refused. The recipient of a faulty CRL shall continue to update the CRL regularly until a new valid CRL is received.

In case that the Root CA CRL is valid and any of the home CA instances of the C-ITS subscriber is listed in the CRL, the C-ITS subscriber shall contact the affected home CA instance. If the home Root CA or home EA is affected, the C-ITS subscriber shall stop the registration of C-ITS stations or even evaluate if a migration to another CA is necessary (see section 6.3). If the home AA is affected, the C-ITS subscriber should also prevent the C-ITS stations from sending C-ITS messages as they would be rejected from the other C-ITS participants anyway.

If the C-ITS station detects that the home Root CA or home EA certificates are revoked, the C-ITS station shall not request any EC certificates. In case of revoked home Root CA or home AA instances, the C-ITS station shall stop sending C-ITS messages. The C-ITS station should also send a notification to the C-ITS subscriber so that the subscriber can evaluate if a re-configuration or a migration to a new home CA is necessary.

7.2.6 EA and AA certificates

If a new EA or AA certificate is loaded from the Root CA CTL or directly via the web interface of the EA or AA, the validation depicted in section "Certificate Validation" of [TR-03164-1] shall be executed by the C-ITS subscriber or the C-ITS station respectively. If the validation succeeded, the certificates shall be securely stored under protection of the secure element from malicious manipulation[6]. All certificates with the same name shall be deleted from the C-ITS station if the validity period exceeded.

The C-ITS station shall also scan the stored EA and AA certificates regularly to find certificates that reached the end of validity in order to delete them.

Fault behaviour

If a newly loaded EA or AA certificate is invalid, the certificate shall be refused and all subordinate certificates shall not be accepted. All C-ITS messages from C-ITS stations belonging to an invalid AA shall be rejected.

If the C-ITS subscriber detects the invalidity of the home EA certificate, it shall be evaluated if the registration of C-ITS stations needs to be stopped or even a migration to another EA is necessary (see section 6.3). If possible, the C-ITS subscriber should also prevent the C-ITS stations from requesting new ECs from the affected home EA.

If the C-ITS station detects the invalidity of the home AA certificate, the station shall stop requesting new ATs and sending C-ITS messages as they would be rejected by the other C-ITS participants anyway. The C-ITS station should send a notification to the C-ITS subscriber so that the C-ITS subscriber can evaluate if a re-configuration or a migration to another home AA is necessary.

7.2.7 Enrolment Credentials

Before the enrolment credential expires, the C-ITS station shall request a new EC at the EA. First, the C-ITS station needs to create a new key pair in its secure element. Then an enrolment credential request message shall be created by the station which, in opposite to the original EC request message, does not contain the canonical data from the registration. The structure of the message with the signatures by the new and old EC private keys shall be in accordance to [TR-03164-1].

After the validation of the EC request message by the EA, the EA signs the enrolment credential certificate and sends it to the C-ITS station in the enrolment credential reply message. The certificate shall be securely stored under protection of the secure element from malicious manipulation[6] after the successful validation of the received EC according to the steps described in the section “Certificate Validation” of [TR-03164-1].

The EC and the corresponding private key shall be deleted from the C-ITS station once they exceeded the validity time.

Fault behaviour

The C-ITS station shall request a new EC in good time before the old certificate expires so that enough time remains if a request for a new certificate fails for any reason. If the old EC expired the C-ITS station shall perform an initial EC request using the canonical ID and the canonical key. Therefore, it has to be ensured that at time of re-usage the canonical key still provides an appropriate level of security as described in [TR-03164-1].

7.2.8 Authorization Tickets

In order to request authorization tickets from the AA the C-ITS station shall create a new key pair in the secure element. Then the new key pair shall be used to create the authorization ticket request message. The request message content shall be composed according to [TR-03164-1].[7]

The Authorization Authority and the Enrolment Authority shall verify the validity of the AT request and the Authorization Authority replies with a signed AT in case of success. The C-ITS station shall validate the AT according to “Certificate Validation” of [TR-03164-1] and shall securely store the ATs under protection of the secure element from malicious manipulation[6].

Especially for mobile C-ITS stations it is required to hold multiple valid ATs at the same time in order to increase the privacy goals of unlinkability and pseudonymity. With a large set of ATs the C-ITS stations can shuffle the ATs used for signature of C-ITS messages depending on parameters like mileage, time or location. Therefore it is allowed to request multiple ATs at the same time with an overlapping validity period.

In order to have a reliable stock of Authorization Tickets for the future it is allowed to preload ATs three months in advance. This preloading interval can be used to bridge longer time periods without the possibility to request new AT certificates.

Fault behaviour

The C-ITS station shall request new ATs in good time before the old ATs expire or the set of valid ATs becomes too small to reach the privacy goals. In combination with the preloading interval, enough time should remain if a request for a new certificate fails for any reason.

7.2.9 Subscriber certificate

Before the C-ITS subscriber certificate reaches the end of validity, the C-ITS subscriber shall create a new key pair in the secure element and update the C-ITS subscriber certificate according to the process described in [TR-03164-1].

The old private key and the corresponding certificate shall be deleted when key and certificate expire. The certificate shall be securely stored under protection of the secure element from malicious manipulation[6] and shall be used to secure the communication between C-ITS subscriber and home EA.

Fault behaviour

The C-ITS subscriber shall updatethe new C-ITS subscriber certificate in good time before the old certificate expires so that enough time remains if a request for a new certificate fails for any reason.

[7] As an alternative to the AT generation method described in [TR-03164-1], the C-ITS station can also request ATs by the authorization management with butterfly keys as described in [ETSI TS 102 941].

7.3 C-ITS Message Signature Validation

After the reception of a message, the C-ITS station shall verify the certificate chain of the signature added to the message to ensure authenticity and integrity of the received message. For performance reasons the C-ITS station might resort to previously stored certificates during the validation instead of loading the certificates during the validation.

The signature of the C-ITS message shall be validated as described in the section “Certificate Validation” of [TR-03164-1]. In cases where a high number of C-ITS messages are received in a short time frame by the C-ITS station and verification of the full certificate chains would lead to an overload of the C-ITS station or the secure element, the C-ITS station can fall back to the securely stored certificates (see section 7.2). This means that a certificate that must be validated in the certificate chain can be considered as valid if the same certificate has been successfully validated in advance and is securely stored from manipulation in the secure storage of the secure element or is authentically encrypted outside of the secure element.

The receiving C-ITS station shall always compare the `appPermissions` present in the AT certificate used for the signature of the C-ITS message with the content of the received C-ITS message. It shall be ensured that the sending C-ITS station is entitled to create the C-ITS message type (e.g. CAM or DENM) and if the C-ITS message contains special containers (e.g. an emergencyContainer), the required permissions must be present in the `appPermissions` of the sending C-ITS station’s certificate. If the permissions are not present, the validation fails.

In case any validation step fails, the message shall be refused by the C-ITS station and no data shall be processed.

The verification steps of digital signatures and certificates of incoming messages from other C-ITS stations described in chapter “Certificate Validation” of [TR-03164-1] may be done outside the secure element in software if the number of messages is that high that the secure element is not able to handle them. This operation is less critical as it does not need access to the private key. If the C-ITS station resorts to certificates or public keys (like the TLM certificate) that are stored encrypted outside the secure element, the secure element must be used for the decryption in order to keep the encryption key in the secure element.

8 Service Specific Permissions

Service specific permissions within a C-ITS Public-Key Infrastructure indicate the actions the certificate holder is entitled to. According to [ETSI TS 103 097], a certificate can contain `appPermissions` and `certIssuePermissions`. The `appPermissions` are used to indicate the permissions a certificate holder is authorized to use and the `certIssuePermissions` are used to define the permissions the certificate holder is authorized to pass to other instances of the C-ITS PKI.

This chapter puts its focus on the `appPermissions` of the AT certificate of the C-ITS station. The permissions of the other types of certificates are explained in [TR-03164-1].

The Authorization Tickets contain permissions to indicate which kind of C-ITS messages can be sent and which special data fields may be added to the messages. Those special permissions are assigned to special C-ITS stations like road works warning units to allow lane closures or police vehicles to indicate the light bar and siren are in use. The `appPermissions` related to the C-ITS messages have to be assigned by the C-ITS subscriber to the C-ITS station during the registration process according to the intended use of the C-ITS station and the granted permissions of the C-ITS subscriber. The same permissions have to be communicated to the EA in the C-ITS station registration message as well. During the initial enrolment of the C-ITS station at the EA, the requested permissions are granted by the EA to the enrolment credential. The C-ITS station shall use the same permissions in the authorization ticket request message as the EA verifies if the `appPermissions` are conformant with the EC certificate `appPermissions`. The special data field permissions in the AT certificate for the C-ITS message allow the certificate holder to sign the C-ITS messages with the related special data fields. The C-ITS station shall never add data fields to the traffic control messages if it does not hold the required permission.

When the C-ITS station verifies the certificate chain of any certificate it shall always check if the SSPs were correctly passed from the certificate issuer to the certificate holder including the validation of the minimum chain length and the minimum chain length given in the certificate. A detailed validation scheme is given in chapter “Certificate Validation” of [TR-03164-1].

The following list gives an overview of the defined *Provider Service Identifier (PSID)* values for different kinds of C-ITS messages and the related specifications defining the SSP bits of special data fields the C-ITS stations add to the traffic control message.

ITS-AID	**PSID Value**	**SSP Definition Reference**
CAM	36	[ETSI EN 302 637-2]
DENM	37	[ETSI EN 302 637-3]
SPAT	137	[ETSI TS 103 301]
MAP	138	[ETSI TS 103 301]
IVI	139	[ETSI TS 103 301]
TLC	140	[ETSI TS 103 301]
GN_MGMT	141	[ETSI TS 103 301]

Table 3: Registered ITS-AIDs for traffic control messages

Whenever a C-ITS subscriber or C-ITS station receives a message from an EU C-ITS participant, it shall verify if the sender of the message is allowed to send the message type and its content complies with the SSPs the sender owns. For C-ITS messages this means that each special data field has to be compared to the

SSP set in the certificate and if the required permissions are not present the complete message must be discarded by the C-ITS station.

The following subchapters give a detailed overview which data fields of the different kinds of C-ITS messages require special service specific permissions.

8.1 Cooperative Awareness Messages (CAM)

Cooperative Awareness Messages (CAM) are exchanged in the C-ITS network between C-ITS stations to create and maintain awareness of each other. A CAM contains status and attribute information of the originating C-ITS station. On reception of a CAM the receiving C-ITS station becomes aware of the presence, type, and status of the originating station.

The CAM is composed of a common C-ITS PDU header and multiple containers, which constitute the CAM payload.

For vehicle C-ITS stations a CAM shall comprise one basic container and one high frequency container, and may also include one low frequency container and one or more other special containers:

The basic container includes basic information related to the originating C-ITS station (e.g. station type, reference position, ...).

- The high frequency container contains highly dynamic information of the originating C-ITS station (e.g. speed, driving direction, vehicle size, ...).
- The low frequency container contains static and no highly dynamic information of the originating C-ITS station (e.g. vehicle role, exterior lights, ...).
- The special vehicle container contains information specific to the vehicle role of the originating vehicle C-ITS station (e.g. usage of light bar siren, closed lanes, emergency priority, ...).
- All CAMs generated by a RSU shall include a basic container and at least one high frequency container. Optionally a low frequency container may be added.
- Each of the container is composed of a sequence of optional or mandatory data elements and/or data frames.
- The high frequency container for vehicle C-ITS stations contains the data frame basicVehicleContainerHighFrequency, the one for RSU should contain the data frame rsuContainerHighFrequency. The data field rsuContainerHighFrequency can only be added to the container, if the required permission is set in the SSP.

The composition of the SSP field for CA Basic Service is described in [TR-03164-1].

The usage of the different special vehicle container requires specific permissions and even some data fields within the special container require additional permissions. The following table gives an overview of the special containers with their data fields and the required permissions.

Container	**Data element in container**	**Required permission**	
		Octet Position	**Bit Position**
rsuContainerHighFrequency			
	protectedCommunicationZonesRSU	1	0 (80h)
publicTransportContainer		1	1 (40h)

	embarkationStatus		
	ptActivation		
specialTransportContainer		1	2 (20h)
	specialTransportType		
	lightBarSirenInUse		
dangerousGoodsContainer		1	3 (10h)
	dangerousGoodsBasic		
roadWorksContainerBasic		1	4 (08h)
	roadworksSubCauseCode		
	lightBarSirenInUse		
	closedLanes	2	0 (80h)
rescueContainer		1	5 (04h)
	lightBarSirenInUse		
emergencyContainer		1	6 (02h)
	lightBarSirenInUse		
	incidentIndication		
	EmergencyPriority – subfield requestForRightOfWay	2	1 (40h)
	EmergencyPriority – subfield requestForFreeCrossingAtATrafficLight	2	2 (20h)
safetyCarContainer		1	7 (01h)
	lightBarSirenInUse		
	incidentIndication		
	TrafficRule – subfield noPassing	2	3 (10h)
	TrafficRule – subfield noPassingForTrucks	2	4 (08h)
	speedLimit	2	5 (04h)

Table 4: CAM data fields and required SSP

8.2 Decentralized Environmental Notification Message (DENM)

Decentralized Environmental Notification Message (DENM) is a facilities layer message that is mainly used by C-ITS applications in order to alert road users of a detected event.

A DENM is composed of a common ITS PDU header and multiple containers, which constitute the DENM payload.

The ITS PDU header is a common header that includes the information of the protocol version, the message type and the C-ITS station ID of the originating C-ITS station.

The DENM payload consists of four fixed order parts: the management container, the situation container, the location container and the à la carte container.

- The management container contains information related to the DENM management and the DENM protocol.
- The situation container contains information related to the type of the detected event (e.g. event type, information quality, ...).
- The location container contains information of the event location, and the referenced location (e.g. event speed, road type, ...).
- The à la carte container contains information specific to the use case which requires the transmission of additional information that is not included in the three previous containers (e.g. lane position, stationary vehicle, road works, ...).

For all types of DENM, the ITS PDU header and the management container shall always be present. The situation container, the location container and the à la carte container are optional containers.

All containers can be added by each station to the DENM message. There are only restrictions by SSP for the eventType data field in the situation container. The eventType provides a description of the type of event being detected. For each specific event type, a unique code shall be used. The eventType is composed of two data elements, namely the causeCode and subCauseCode:

- causeCode: the direct cause code provides a high level description of the detected event type.
- subCauseCode: This data element is used to provide more detailed information of the event related to the causeCode.

The composition of the SSP field for DENM is described in [TR-03164-1].

The following table shows the cause codes and the required permissions to be able to add the cause code to the DENM message.

Cause code description	**Direct Cause code**	**Required permission**	
		Octet Position	**Bit Position**
Traffic condition	1	1	0 (80h)
Accident	2	1	1 (40h)
Roadworks	3	1	2 (20h)
Adverse weather condition – adhesion	6	1	3 (10h)
Hazardous location – Surface condition	9	1	4 (08h)
Hazardous location – Obstacle on the road	10	1	5 (04h)
Hazardous location – Animal on the road	11	1	6 (02h)

Human presence on the road	12	1	7 (01h)
Wrong way driving	14	2	0 (80h)
Rescue and recovery work in progress	15	2	1 (40h)
Adverse weather condition – extreme weather condition	17	2	2 (20h)
Adverse weather condition – visibility	18	2	3 (10h)
Adverse weather condition – Precipitation	19	2	4 (08h)
Slow vehicle	26	2	5 (04h)
Dangerous end of queue	27	2	6 (02h)
Vehicle breakdown	91	2	7 (01h)
Post crash	92	3	0 (80h)
Human problem	93	3	1 (40h)
Stationary vehicle	94	3	2 (20h)
Emergency vehicle approaching	95	3	3 (10h)
Hazardous location indication – Dangerous Curve	96	3	4 (08h)
Collision risk	97	3	5 (04h)
Signal violation	98	3	6 (02h)
Dangerous situation	99	3	7 (01h)

Table 5: DENM cause codes and required SSP

9 Requirements on Pseudonymisation

The privacy of C-ITS station owners shall be satisfied in the EU C-ITS PKI by means of pseudonymity and unlinkability of the C-ITS stations. Those requirements are ensured by the usage of pseudonym certificates, the Authorization Tickets (AT). The ATs are certificates that do not contain any information related to the C-ITS station or its owner. The C-ITS station shall also change the ATs regularly and use them only a limited number of times to avoid the traceability of the C-ITS station over a longer period of time. The following requirements shall be followed by all types of C-ITS stations:

1. ATs shall not be changed when the Road Hazard Signalling application detects a critical traffic safety situation.
2. Unicast and multicast applications shall use link layer encryption and regular changes of the ITS MAC addresses to protect the privacy of the C-ITS station (and its user) as well as all higher layer information from radio channel eavesdropping. Further details can be found in [ETSI TS 102 941], [ETSI TS 102 942] and [ETSI TS 102 943].

The following requirements shall be followed by private mobile C-ITS stations. Public mobile C-ITS stations may also follow those requirements if a certain privacy and pseudonymisation is required:

1. When changing AT certificates:
   - All the IDs associated with a C-ITS station across different layers of the ITS stack shall be changed synchronously
   - In the communication profile for CAM and DENM, all the layers' identifiers (MAC address GeoNetworking Source address, station ID) shall be changed
   - The GeoNetworking address shall be updated as specified in [ETSI EN 302 636-4-1]. Only the last field of the address (MAC ID of length 48 bits) is updated and derived from the pseudonym. [ETSI TS 102 940]
2. The usage period of an AT depends on the AT change strategy and the amount of time that a vehicle is in operation, but is limited by the maximum number of parallel ATs and the validity period. More specifically, the average usage period for one C-ITS station is at least the operational time of the vehicle during one validity period divided by the maximum number of parallel ATs. [CP]
3. Mobile C-ITS stations shall implement an adequate AT change procedure so that at least 95% of all trips are divided into at least three segments. The change procedure can be based on fixed or variable time and distance metrics. Each of the segments shall be using different ATs.
4. A mobile C-ITS station shall have a pool of 100 ATs with a defined validity period as specified in [TR-03164-1]. The ATs are drawn randomly from the pool with equal probability and without replacement after usage. When all ATs in the pool are used, then the pool is re-started with the same ATs. This is repeated until the validity period of the ATs passed and a new pool of 100 ATs is used. [SP]

The following requirements shall be followed only by stationary road side units:

1. Following requirements on ATs apply:
   - The preloading period for ATs shall not exceed one week if a permanent connection to the AA is available.
   - The preloading period for ATs shall not exceed three months if no permanent connection to the AA is available.
   - The maximum number of parallel ATs shall not exceed two per RSU station.

10 Remote Access

For all C-ITS stations that provide a remote access from the C-ITS subscriber or the traffic control centre (TCC) must secure the access in order to avoid misuse of the C-ITS functionality by unauthorized attackers. The remote access of C-ITS subscriber to the C-ITS station can be used for functional and security updates or the change of the configuration like the change of the home CA settings or cryptographic parameters. The following requirements apply to the remote connection from the C-ITS subscriber to the C-ITS station in order to ensure the authenticity and integrity of the remote updates in the C-ITS station:

1. The remote access shall be established on a mutually authenticated and confidential channel.
2. The C-ITS station shall provide authentication mechanisms for all roles that can connect to the station.
3. The C-ITS station shall provide access control mechanisms for its functions and stored data.

Especially mobile road side units but also to a lesser degree stationary road side units must be configured by the traffic control centre during the operation in order to react on changing conditions. For example a TCC operator should be able to configure the mobile road works warning unit remotely to change the speed limit which is distributed via C-ITS messages. The misuse of the configuration channel shall be avoided by the following requirements:

1. The C-ITS station shall provide authentication mechanisms for all users that can connect to the station.
2. The RSU shall require each user to be successfully authenticated before allowing any actions for that user.
3. All messages received from or sent to the TCC, must be encrypted and authenticated (e.g. via a TLS channel in versions 1.2 or 1.3 using the cryptographic algorithms and key-lengths recommended within the latest version of [TR-02102-2]).

11 Usage and requirements of secure elements of C-ITS subscribers and -stations

C-ITS subscriber and C-ITS stations shall be equipped with a secure element as specified in [CP] that follows the cryptographic algorithms presented in [TR-03116-6] in order to support the cryptographic algorithms prescribed in the EU C-ITS PKI.

The secure element of the C-ITS subscribers and C-ITS stations shall generate, hold, use and delete key material following [KLCR] with security level 2 for the following types of keys:

For C-ITS subscriber:

- C-ITS subscriber certificate key pair

For C-ITS stations:

- Canonical key pair
- Enrolment Credential key pair
- Authorization Ticket key pairs
- Symmetric key for encryption and decryption of certificates stored outside the secure element

C-ITS subscribers are allowed to create backups of private keys following the requirements of [KLCR] with security level 2. Private keys of C-ITS stations shall not be backed up. When the certificates of C-ITS subscribers or C-ITS stations exceed the validity time, the private keys shall be securely removed from the secure element.

The initial canonical key pair which is generated during production should be generated directly in the secure element of the C-ITS station. The key material shall be handled and stored according to the requirements of [TR-03145-1]. If the generation in the secure element of the C-ITS station is not possible, the canonical key pair can be generated in a secure element of the C-ITS subscriber with the same requirements for the handling and storage as the secure element of the C-ITS station. The key material shall be transferred via an integrity and authenticity secured environment from the C-ITS subscriber to the C-ITS station. The cryptographic measures used for the canonical key pair are specified in [TR-03116-6]. In cases where the canonical key pair needs to be newly generated (e.g. because the original one has not appropriate level of security), the new canonical key pair shall be created and, if required, transferred in the same way like the initial canonical key pair to the C-ITS station or preferably the new canonical key pair shall be generated directly inside the secure element of the C-ITS station.

As described in chapter 7.3, C-ITS stations may store certificates for later use in order to avoid the full certificate chain verification of C-ITS messages. The validated certificates shall either be stored inside the secure element or they shall be stored in the C-ITS station authentically encrypted by the secure element. This is true for certificates from all levels, i.e. TLM, Root CA and Sub-CA certificates. The symmetric key for the encryption shall be generated in the secure element and shall not be exported. For the verification of certificate chains those certificates must be decrypted in the secure element.

During the creation of messages the C-ITS subscriber and C-ITS station shall adhere to the following rules for the involvement of the secure element:

- Signature of messages: The private key stored in the secure element shall be used. The creation of the signature shall be performed inside the secure element as it is not allowed to export the private key from the secure element.
- Encryption of messages: The encryption of messages to a C-ITS PKI member shall be performed inside the secure element. For the encryption of the message, the public key of the recipient is used. This public key shall be loaded from the recipient and verified as described in "Certificate Validation" of [TR-03164-1]. C-ITS stations can alternatively use previously validated and stored certificates.

When a C-ITS subscriber receives a message from a C-ITS PKI member, the following rules for the involvement of the secure element shall be followed:

- Signature verification: The verification of signatures requires the certificate of the sender. During the signature verification the C-ITS subscriber shall perform the complete certificate chain validation up to the stored TLM certificate as described in the chapter "Certificate Validation" of [TR-03164-1]. The verification should be performed inside the secure element. If this is not possible the validation can be done outside the secure element in software.
- Decryption of messages: The received messages shall be decrypted with the private key of the C-ITS subscriber. The decryption shall be done inside the secure element in order to avoid the export of the private key from the secure element.

When a C-ITS station receives a message from a C-ITS PKI member, the following rules for the involvement of the secure element shall be followed:

- Signature verification: The verification of signatures requires the certificate of the sender. The C-ITS station shall either perform the complete certificate chain validation or it falls back to the previously validated and stored certificates. The validation steps described in the chapter "Certificate Validation" of [TR-03164-1] should be performed inside the secure element. If this is not possible (e.g. because of performance reasons) the validation can be done outside the secure element in software.
- Decryption of messages: The received messages shall be decrypted with the private key of the C-ITS subscriber or the C-ITS station respectively. The decryption shall be done inside the secure element in order to avoid the export of the private key from the secure element.

In order to ensure a trustworthy and reliable operation of the C-ITS subscriber and C-ITS station, the secure element shall be protected against unauthorized removal, replacement and modification. Especially for unattended road side units a detection of manipulation shall be implemented that revokes the C-ITS station from the EA and delete all private keys if the secure element is suspected to be manipulated or stolen. The C-ITS station should be capable of verifying the authenticity and integrity of the secure element during startup and for road side units the operator shall monitor the stations during the operation and be able to revoke manipulated or stolen stations.

References

[CP] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), 2018

[TR-03164-1] Technical Guideline BSI TR-03164 Version 1.0.0 Draft, Part 1: Guidance for Operation of a Public-Key Infrastructure for Cooperative Intelligent Transport Systems (C-ITS), 2021

[ETSI TS 102 941] ETSI TS 102 941 V2.1.1, Intelligent Transport Systems (ITS) - Security; Trust and Privacy Management, 2021

[TR-03116-6] Technische Richtlinie BSI TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 6: Kooperative intelligente Verkehrssysteme (C-ITS), 2020

[ETSI EN 302 637-2] ETSI EN 302 637-2 V1.4.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, 2019

[ETSI EN 302 637-3] ETSI EN 302 637-3 V1.2.2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, 2014

[ETSI TS 103 301] ETSI TS 103 301 V 1.3.1, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services, 2020

[TR-02102-2] Technische Richtlinie TR-02102-2Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 – Verwendung von Transport Layer Security (TLS),

[CPOC] C-ITS Point of Contact (CPOC) Protocol – Description of the CPOC Protocol in the EU C-ITS Security Credential Management System (EU CCMS) ,

[ETSI TS 103 097] ETSI TS 103 097 V1.4.1, Intelligent Transport Systems (ITS); Security; Security header and certificate formats, 2020

[ETSI TS 102 942] ETSI TS 102 942 V1.1.1, Intelligent Transport Systems (ITS); Security; Access Control, 2012

[ETSI TS 102 943] ETSI TS 102 943 V1.1.1, Intelligent Transport Systems (ITS); Security; Confidentiality services, 2012

[ETSI EN 302 636-4-1] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality, 2017

[ETSI TS 102 940] ETSI TS 102 940 V1.3.1, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, 2018

[SP] Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), 2017

[KLCR] BSI, Key Lifecycle Security Requirements,

[TR-03145-1] Secure CA operation, Part 1; Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', 2017