European Commission

Result of
C-ITS Platform Phase II

Security Policy & Governance Framework for Deployment and Operation of European **Cooperative Intelligent Transport Systems** (C-ITS)

RELEASE 1
DECEMBER 2017

Security Policy & Governance Framework

for

Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

Release 1

December 2017

chaired by the

Foreword

This document is a deliverable following the adoption of the European Commission's Communication COM 2016/766 on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" adopted on 30th of November 2016.

The C-ITS Strategy of the Commission announced that the Commission will work together with all relevant stakeholders in the C-ITS domain to steer the development of a common security and certificate policy and other accompanying documents needed for the deployment and operation of C-ITS in Europe. Concretely it was announced that guidance will be published in 2017.

Hence this document is a result of the work of the Platform for the deployment of Cooperative Intelligent Transport Systems in the European Union (C-ITS Platform) which was created and chaired by the European Commission services in November 2014 to pave the way towards deployment of C-ITS in Europe. Following intensive work in a broad consultation process steered by the Commission from early 2016 onwards this document delivers the guidelines on a common C-ITS Security Policy that has been agreed upon by all involved stakeholders.

Document History

Release	Changes	Editor	Date
1	First Release*	C-ITS Platform Stakeholders	December 2017

* This document is the first published version of the Security Policy & Governance Framework for deployment and operation of European C-ITS. It complements the "C-ITS Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)". These documents lay the foundation for deployment of secure and interoperable C-ITS services in Europe.

All documents are by definition subject to future change and will hence be updated whenever required and consequently published as a new release. As soon as the described governance roles have been concretely setup in Europe in the future, the publishing of these documents will be taken over by the respective roles and entities defined in the documents.

Please note that this first release includes a few items that have been marked in yellow (marked with "TBD" – "to be defined") to indicate that these paragraphs or elements still need to be updated as soon as the lacking elements become available.

In case of remarks on this document, please contact: MOVE-JRC-C-ITS-POLICY-AUTHORITY@ec.europa.eu

Table of Contents

Scope & Purpose

Scope:

The scope of this document includes the following components and entities of C-ITS:

- the C-ITS services offered through the C-ITS system,
- the C-ITS system as a "system of systems",
- the ITS Stations,
- the EU CCMS participants and their information processing systems.

Purpose:

This document is split into two parts:

Part A: C-ITS Governance Framework

The purpose of this policy is to describe the overall governance of the European C-ITS system including the following components and entities of C-ITS: the C-ITS system as a whole and its governance and management structure, the participating C-ITS Stations, the components of the trust model (e.g., PKI services) as well as the entities running them in a secure and reliable way, the trusted third parties for the trust and privacy management on which operational entities rely and which allow running them in a secure and reliable way.

Part B: C-ITS Security Policy

The purpose of this policy is to provide a framework for the management of information security for the deployment and operation of the European Cooperative Intelligent Transport System (C-ITS). It defines how to manage information security incl. the definition of security policies for individual stakeholders and the operation of an information security management system. As such, the policy should be seen as a meta-policy. It defines the policy requirements for information security management for all organisational entities that process C-ITS data or manufacture equipment that will process C-ITS data. The C-ITS system is a distributed system with many stakeholders and many actors processing parts of the C-ITS data which makes information security not only a responsibility of the individual organisations but also a joined and shared responsibility.

Definitions and acronyms

EU CCMS	European Union C-ITS Security Credential Management System (formally known as "PKI")
CERT	Computer Emergency Response Team
C-ITS	Cooperative Intelligent Transport Systems
C-ITS-S	Cooperative ITS-S
CP	Certificate Policy

DEN	Decentralized Environmental Notification
DENM	DEN Message
ISMS	Information Security Management System
ITS-S	ITS station
IVIM	Infrastructure to Vehicle Information Message
PII	Personal Identifiable Information
SPATEM	Signal Phase And Timing Extended Message
SREM	Signal Request Extended Message
SSEM	Signal request Status Extended Message
SSP	Service Specific Permissions

Terms Definition

Actor	person or organizational unit playing a coherent set of *roles* when interacting with the system within a particular use case (ISO 17427) [11]
Availability	property of being accessible and usable upon demand by an authorized entity (ISO 27000) [2]
C-ITS Infrastructure	System of facilities, equipment and applications needed for the operation of an organization that provides C-ITS services related to fixed ITS-S.
C-ITS Service	defined C-ITS functionality which requires a defined set of data as input, processes this data and delivers a defined output (examples of C-ITS services can be found in [15]
C-ITS stakeholders	Individual, group, or organization, who has a role and responsibility in the C-ITS system
C-ITS user	Any ITS application or functional agent sending, receiving or accessing ITS-related information (ETSI TR 102 893) [9]
Confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO 27000) [2]
Information security	preservation of confidentiality, integrity and availability of information (ISO 27000) [2]
Information Security incident	single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Integrity	property of accuracy and completeness (ISO 27000) [2]
ITS station	ITS station: functional entity specified by the ITS station (ITS-S) reference architecture [18]. This policy distinguishes between mobile ITS-S (including vehicle ITS-S) and fixed ITS-S.
Local Dynamic Map	Local Dynamic Map (LDM) is an in-vehicle ITS station's dynamically updated repository of data relating to local driving conditions. It includes information received from on-board sensors and from CAM and DENM messages (ETSI TR 102 893) [9]

Manufacturer	Entity responsible for the design and manufacturing of ITS-stations
Operator	Entity responsible for the operation of ITS-stations
Protocol Control	The protocol control assets select an appropriate message transfer protocol for an outgoing message request and sends the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the ITS station and passed to the relevant functional asset for further Processing (ETSI TR 102 893) [9]
Service User	Entity that uses ITS services and their benefits
Stakeholder	individual or organisation having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations (ISO 17427) [13]

Document Name and Identification

This document is identified by the following information:

- Name: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)
- Version: 1
- OID: {iso(1) identified-organization(3) european-commission(130) information-systems(1) (TBD-proposed but not formalized yet)
- Location: https://ec.europa.eu/transport/themes/its/c-its_en (TBD - proposed but not formalized yet)

A. C-ITS Governance Framework

A.1 Approach and structure of the Part A

Section A.2 defines how the term actors, role and legal entity are used in this document and further describes a classification of roles. Section A.3 specify the sub-roles of the overall governance framework of the European C-ITS trust system and visualize them in architecture diagrams that show dependencies and interconnections between all the roles and how they work together. The tasks, respective categorisation and properties of each specific role and sub-roles are described. Further, the document identifies and recommends appropriate entities to assume all of the described specific roles and sub-roles.

A.2 Classification of roles in the EU C-ITS trust system

This document adopts the classification and definitions of roles provided in (ISO 17427) [13], but with a different definitions of the sub-roles.

In [13], the main organizational roles have the structure defined in Figure 1.

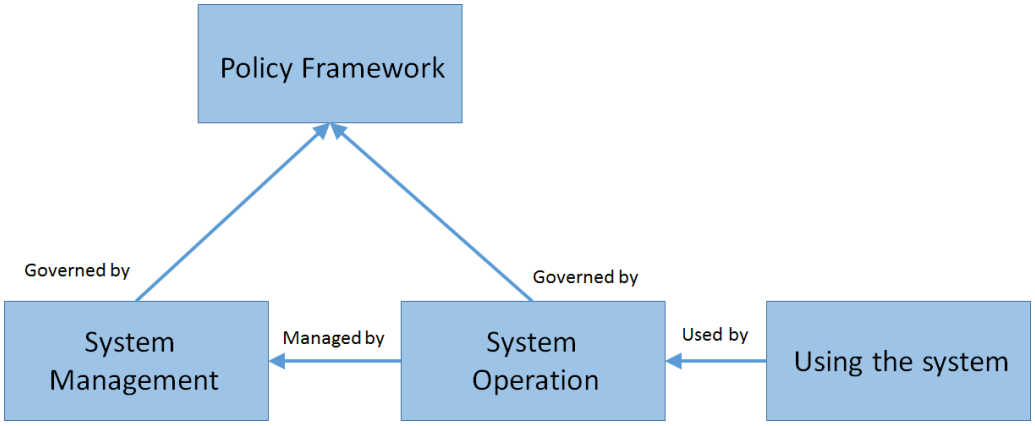

Figure 1 Main Organisational roles (from [13])

The following **main roles** are defined (inspired by [13] but tailored to the needs of the European C-ITS trust system):

1. The ***Policy framework*** role is responsible for all the governance and policy management activities required in the system. The actors in this role define policies and regulations to the actors in the European C-ITS trust system including the actors of System Operation and System Management.
2. The ***System operation*** role is responsible for the proper execution of the applications that provide the end-to-end ITS service(s).
3. The ***System management*** role is responsible to fulfil all required management activities within the system, including the definitions of requirements and guidelines for the actors in the system operations role.

The actors in the System operation role support the actors in the System management role to enable and facilitate System Management behavior and responsibilities.

The actors in the System Management role support the actors in the Policy Management role to enable and facilitate Policy Management behavior and responsibilities.

The legal entities, which are responsible for the governance and operation of the EU C-ITS trust system can have one or more roles or sub-roles. In some cases, a legal entity only fulfills a specific role or sub-role.

The main driver for prohibiting specific roles to be assumed by the same legal entity is:

- To avoid conflicts of interest.
- For segregation of duties.

Each role can have different sub-roles, which are described in the following sections.

A template (i.e., a table) is used to define the different features of each sub-role.

The template definition is provided in Table 1.

Table 1 Template for sub-role definition

Role	*Based on definitions in A.2*
Sub-Role Description	*Short description of the sub-role*
Functional Area	*If it is:* *a) Deployment and operation,* *b) Compliance Assessment* *c) EU CCMS (Upper governance levels do not have this field and it is set to All)*
Functions / Responsibilities of the sub-role	*Bullet point list of functions* *Description of what it is responsible for – associated to the functions.*
Cardinality of the sub role with respect to the legal entity	*How many entities with this sub-role can exist in the EU C-ITS trust system ?*
Participants	*Participants to this sub-role (e.g., government entities)*
Separation of duties	*Is it necessary to separate this role from other sub-roles, i.e. it cannot be combined in one legal entity with other sub-roles.*
Type of Legal Entity	*This field is used to indicate if there are limitations or indications on the type of legal entity, which can take over this sub-role (e.g., public)*
Business or Sustainability Model	*This field is used to indicate the business/sustainability model and the funding scheme (if possible).*

Figure 2 gives an overview view of the identified sub-roles and their dependencies. Each of the sub-roles is described in the following sections.

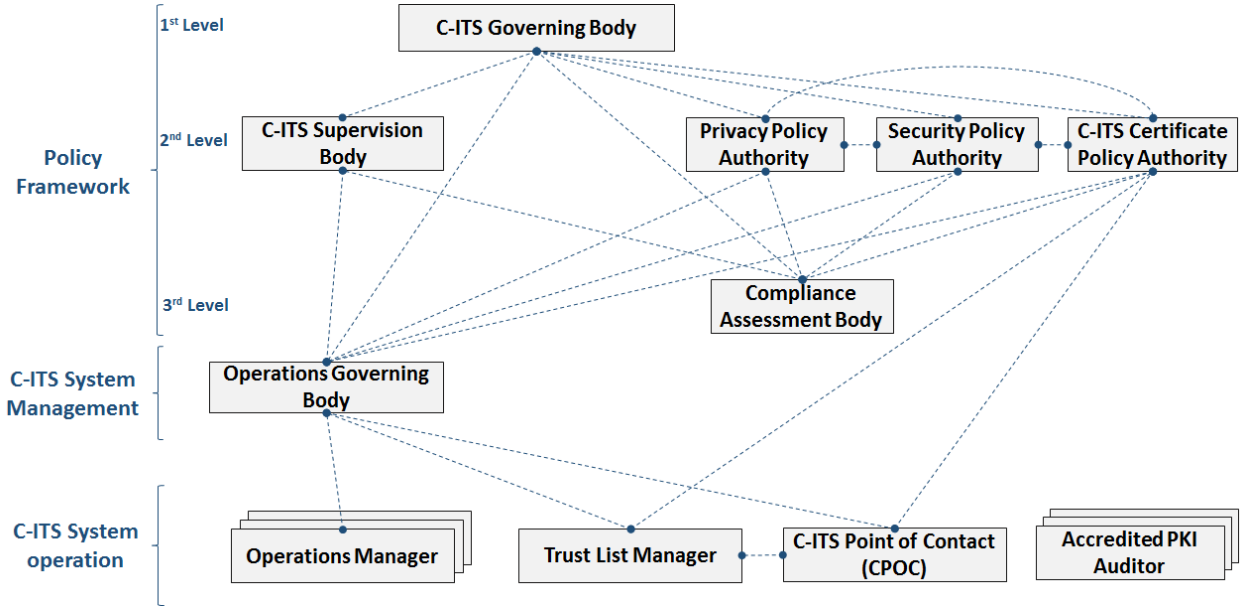

Figure 2: Detailed Structure View of the Governance Architecture

A.3 Sub-roles definition

A.3.1 Policy Framework sub-roles

A.3.1.1 C-ITS Governing body

Table 2 C-ITS Governing body sub-role definition

Role	Policy Framework
Sub-Role Description	The C-ITS Governing Body is the top sub-role of the overall C-ITS governance architecture. It only reports to bodies outside of the C-ITS domain. It provides its output to the other roles in the C-ITS policy framework and to the roles in system management.
Functional Area	All functional areas
Functions / Responsibilities of the sub-role	Main functions: • Definition and evolution of C-ITS strategy and C-ITS governance framework (i.e. Part A of this document). • Main contact to C-ITS Operators and manufacturers • Main contact point to the general European policy makers for policy decisions, which impact the C-ITS system • Main contact to end user groups • Main contact point to the counterparts from other geographical domains • Definition of Compliance Assessment Reference Framework including: o C-ITS assessment criteria, which shall be used during the compliance assessment process by testing laboratories and other assessment organizations. o C-ITS Reference Specifications, including basic and test standards, which shall be used during the different steps of the assessment process. o C-ITS system profiles, which are the selections of particular options or parts of standards to be used. The C-ITS Governing body defines the C-ITS strategy including the security strategy and derives rough guidelines from the strategy based on the input from the stakeholder groups. The C-ITS strategy is the high level plan to enable C-ITS services to be deployed and operated. On operational level other types of strategy may exists such as a short or mid-term strategy to improve or change the service due to changes in requirements. The C-ITS Governing body defines rules (including conflict resolution process) for the resolution of issues detected by the C-ITS Supervision body The C-ITS Governing body is the main contact to policy makers (e.g., European council, European parliament, Member States political figures). The C-ITS Governing body is the main contact to international counterparts responsible for the C-ITS infrastructures.
Cardinality of the sub role with respect to the legal entity	Single entity at European level

Participants	This role should be taken by a common steering committee among the stakeholders: • European Commission • Member States • Road Infrastructure operators • Manufacturers and suppliers
Separation of duties	Not required
Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership or by public funding with the presence of the European Commission.

A.3.1.2 C-ITS Supervision Body

Table 3 C-ITS Supervision body

Role	Policy Framework
Sub-Role Description	The C-ITS Supervision Body is a second level sub-role that deals with technical aspect of the deployment and operation of the C-ITS system. It reports to the C-ITS governing body. It provides its output to the other roles in the policy framework and to the roles in system management.
Functional Area	All functional areas
Functions / Responsibilities of the sub-role	• Identification of new requirements (i.e. functional, technical, security and legal including data protection) to regulations or standards, which can be used to ensure the continuous provisioning of C-ITS services and the operation of the EU CCMS. • Triggers the implementation of changes in requirements, regulations (e.g. certificate and/or security policy) or standards defining the design and operation of the EU CCMS and the C-ITS system. • Supervision and management of incidents of large scale and high severity which impact the entire C-ITS trust system (e.g., disaster recovery situation where the cryptographic algorithm is compromised) and which cannot be resolved by the Operation manager and the Operations governing body through the setup of a dedicated CERT. The C-ITS Supervision Body is responsible for the detection of issues in the deployment and operational phase, which can be reported to the C-ITS Governing Body and to the Compliance Assessment Body for further analysis and action, on the basis of rules defined by the C-ITS Governing Body. This requires a hierarchical organisation to be able to solve issues at appropriate level and/or report them to the appropriate level. Its responsibilities include identification, assessment and monitoring of newly identified security vulnerabilities as well as ambiguous, unclear or 'impractical to implement' statements in requirements, regulation or standards defining the design and operation of the EU CCMS and the C-ITS system. Once identified, the C-ITS Supervision Body makes sure that appropriate changes are made within the requirements and the other documents by the sub-governance body responsible for the particular area that the change affects including the C-ITS Governing Body, if general changes of strategy are required. In that manner, supervision is responsible for leading the continuous improvement process. In addition, the C-ITS Supervision Body is responsible for managing incidents of large scale and high severity, as reported by the Operations Governing Body. This

	includes providing directives, guidelines and recommendations to the Operations Governing Body.
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	This role should be taken by a common committee among the stakeholders: • European Commission • Member States • Infrastructure operators • Manufacturers and suppliers
Separation of duties	Not required
Type of Legal Entity	Voluntary union composed of: • Central supervision board (EU wide) • National supervision boards • Industry supervision board(s) e.g. for vehicles
Business or Sustainability Model	Funded by a Public Private partnership or by public funding

A.3.1.3 C-ITS Certificate Policy Authority

Table 4 C-ITS Certificate Policy Authority sub role

Role	Policy Framework
Sub-Role Description	The Certificate Policy Authority is the top level sub-role of the CCMS domain. It is a second level sub-role in the policy framework that reports to the C-ITS governing body.
Functional Area	EU CCMS
Functions / Responsibilities of the sub-role	The detailed functions of the Policy Authority are defined in the certificate policy [1], covering Certificate policy and PKI authorisation management. The detailed responsibilities of the Policy Authority are defined in the certificate policy [1].
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	This role should be taken by a common steering committee among the stakeholders (i.e., Member States, equipment manufacturers, vehicle manufacturers, infrastructure managers…)
Separation of duties	Not required
Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership and/or by public funding

A.3.1.4 Privacy Policy Authority

Table 5 Privacy Policy Authority

Role	Policy Framework
Sub-Role Description	The Privacy Policy Authority is the top level sub-role committee for personal data protection aspects in C-ITS. It is a second level sub-role in the policy framework that reports to the C-ITS governing body.
Functional Area	All functional areas
Functions / Responsibilities of the sub-role	To define and manage the protection data protection rules for all the users in the C-ITS. The Privacy Policy Authority is responsible for: • Be the central point of contact for the Data Protection Authorities in Europe. Data Protection Authorities can also participate to the implementation of the sub-role Privacy Policy Authority. • Draft and maintain the data protection rules for C-ITS including the ones defined in the Certificate Policy (in this aspect, the Privacy Policy Authority shall work with the Certificate Policy Authority)
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	The Privacy Policy Authority is a role composed by the representatives of public and private stakeholders (e.g. Member States, Vehicle Manufacturers, etc.) participating to the C-ITS trust model.
Separation of duties	Not required
Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership or by public funding

A.3.1.5 Security Policy Authority

Table 6 Security Policy Authority

Role	Policy Framework
Sub-Role Description	The Security Policy Authority is the top level sub-role for information security aspects in C-ITS. It is a second level sub-role in the policy framework that reports to the C-ITS governing body.
Functional Area	All functional areas
Functions / Responsibilities of the sub-role	To define and manage the Security Policy document of the European C-ITS system. It is responsible to draft, publish and maintain the Security Policy document of the European C-ITS system (i.e. Part B of this document).
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	The Security Policy Authority is a role composed by the representatives of public

	and private stakeholders (e.g. Member States, Vehicle Manufacturers, etc.) participating to the C-ITS trust model.
Separation of duties	Not required
Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership or by public funding

A.3.1.6 Compliance Assessment Body

Table 7 Compliance Assessment body

Role	Policy Framework
Sub-Role Description	The Compliance Assessment Body is the top level sub-role for C-ITS compliance assessment. It is a third level sub-role in the policy framework that reports to the C-ITS supervision body.
Functional Area	Compliance Assessment
Functions / Responsibilities of the sub-role	• it oversees the overall process and management of Compliance Assessment operation • It defines the governing rules and procedures for the compliance assessment tests and procedures. • It defines the governance for compliance testing involving external existing compliance schemes • It issues the C-ITS proof of compliance approval. • It maintains the list of approved ITS stations (i.e. concrete products based on brand, model and version of ITS stations). The Compliance Assessment Body compiles and maintains the compliance assessment criteria based on: • the Compliance Assessment Reference Framework as defined by the C-ITS Governing Body. • The Certificate Policy from the Certificate Policy Authority. • The Security Policy from the Security Policy Authority. • The Privacy Policy from the Privacy Policy Authority. It is a responsible for operating the Device Registry Database as a central service. The Device Certification Registry is a Database which lists all devices that have been validated for compliance with the criteria defined by the Compliance Assessment Body by an accredited Test Lab.
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	This sub-role should be taken over by a committee or working group of stakeholder experts in this area (e.g., for vehicle ITS stations, the security compliance assessment criteria shall be provided by a group of security experts from the automotive industry with input from other relevant stakeholders). • C-ITS Governing Body ("owner" of the process) • Testing laboratories
Separation of duties	Not required

Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership or by public funding

A.3.2 C-ITS System Management sub-roles

A.3.2.1 Operations Governing Body

Table 8 Operations governing body

Role	System Management
Sub-Role Description	The Operations governing body is the top level sub-role in system management. It reports to C-ITS governing body and the C-ITS Supervision Body in the Policy Framework. It provides its output to the sub-roles of system operation.
Functional Area	Deployment and Operation
Functions / Responsibilities of the sub-role	To compile and maintain ITS-S operational requirements based on: • The strategy from the C-ITS Governing Body • The Compliance Assessment Reference Framework as defined by the C-ITS Governing Body. • The Certificate Policy from the Certificate Policy Authority. • The Security Policy from the Security Policy Authority. • The Privacy Policy from the Privacy Policy Authority. Define operational requirements derived from the high level requirements defined by the C-ITS Supervision Body. Coordinate and manage incidents reporting from the Operations Manager. Check and ensure compliance of the operation managers with the operational requirements Definition of the minimum requirements for commissioning/decommissioning, for operational performances and implementing necessary security changes during the operation lifetime of an ITS-S. Definition and maintenance ITS-S operational requirements. Coordinate and manage incidents reporting from the Operations Manager, decide on their global relevance and aggregate those incidents to a global view and report that to the C-ITS Supervision Body. Receive directives, guidelines and recommendations from the supervision body and update the requirements accordingly. Because the Operational Governing body is unique at European level, it has also the responsibility to coordinate the respective Operation Managers for all the activities and issues, which goes beyond the jurisdiction of a specific Operation Manager.
Cardinality of the sub role with respect to the legal entity	Single entity at European level.
Participants	This role should be taken by a common steering committee among the stakeholders (i.e., Member States, equipment manufacturers, vehicle manufacturers, infrastructure managers…).
Separation of duties	Not required

Type of Legal Entity	Voluntary union
Business or Sustainability Model	Funded by a Public Private partnership or by public funding

A.3.3 C-ITS System operation sub-roles

A.3.3.1 Operations Manager

Table 9 Operations Manager

Role	System Operation
Sub-Role Description	The Operations Manager is a sub-role in system operation. It reports to the Operations governing body in system management.
Functional Area	Deployment and operation
Functions / responsibilities of the sub-role	Main functions: • Implementation of the operational requirements as published by the Operations Governing Body • Operation of a specific C-ITS infrastructure • Manage incidents on a specific C-ITS infrastructure • Escalate an incident report to the Operations Governing body It is responsible for operating: • a C-ITS infrastructure • mobile ITS-Stations and their supporting C-ITS infrastructure, or • a CCMS operational role (Root CA, EA, AA) as defined in [1] It is responsible to implement the operational requirements as published by the Operations Governing Body at the C-ITS-Station Operation roles. The proper way to enforce the criteria depends on the actual criteria to be set. In addition, the operations manager is responsible to manage incidents and report incidents to the upper layers of the Operations Governing body and the C-ITS Supervision body when it does not have the capabilities to address a specific incident or set of incidents in the C-ITS security infrastructure. The Operations Manager may be responsible only for a portion of the EU C-ITS security infrastructure: e.g. a member state or a privately owned C-ITS infrastructure.
Cardinality of the sub role with respect to the legal entity	Multiple instances at European level.
Participants	Infrastructure Manager (public or private)
Separation of duties	Not required.
Type of Legal Entity	Public or Private
Business or Sustainability Model	Member state or private funding

A.3.3.2 Trust List Manager

Table 10 Trust List Manager

Role	Operations Manager
Sub-Role Description	The Trust List Manager is a sub-role in system operation. It reports to the Operations governing body and to the Certificate Policy Authority in system management.
Functional Area	EU CCMS
Functions / Responsibilities of the sub-role	The Trust List Manager is responsible for the generation and update of the ECTL according to the common valid Certificate Policy ([1]) and regular activity reporting to the policy authority for the overall secure operation of C-ITS trust model. See [1] for a description of root CA and ECTL. Details are defined in the certificate policy [1].
Cardinality of the sub role with respect to the legal entity	Single instance at European level.
Participants	European Commission
Separation of duties	Not required
Type of Legal Entity	Public
Business or Sustainability Model	Initial public funding with a sustainable business model funded by the C-ITS users

A.3.3.3 C-ITS Point of Contact (CPOC)

Table 11 C-ITS point of contact

Role	System Operation
Sub-Role Description	The C-ITS point of contact is a sub-role in system operation. It reports to the Operations governing body and to the Certificate Policy Authority in system management.
Functional Area	EU CCMS
Functions / Responsibilities of the sub-role	The C-ITS Central Point of Contact is responsible to handle all communication with individual root CA managers, publish the common trust anchor (i.e., public key certificate of the Trust List Manager) and the ECTL. See [1] for a description of root CA and ECTL. Its detailed responsibilities are defined in the European C-ITS certificate policy [1].
Cardinality of the sub role with respect to the legal entity	Single instance at European level.
Participants	European Commission
Separation of duties	Not required.
Type of Legal Entity	Public
Business or Sustainability Model	Initial public funding with a sustainable business model funded by the C-ITS users.

A.3.3.4 Accredited PKI Auditor

Table 12 Accredited PKI Auditor

Role	System Operation
Sub-Role Description	The Accredited PKI Auditor is a sub-role in system operation.
Functional Area	EU CCMS
Functions / responsibilities of the sub-role	The C-ITS Accredited Auditor is responsible to assess the compliance of a PKI entity to the European certificate policy by carrying out an audit procedure. The exact responsibilities of the Accredited PKI Auditor are defined in the European C-ITS certificate policy [1]
Cardinality of the sub role with respect to the legal entity	Multiple instances at European level.
Participants	The Accredited Auditor is accredited by a Member listed by the European co-operation for accreditation.
Separation of duties	Separation required from all other sub-roles.
Type of Legal Entity	Private or Public
Business or Sustainability Model	Organisations based on the necessity to accredit the PKI elements, which must participate to the EU CCMS.

A.4 Legal entities

A.4.1 Legal entity definitions

Following the role and sub-role definitions in section A.2 and A.3, legal entities have to be established to fulfil all sub-roles in the C-ITS governance architecture. Table 13 depicts the potential need for separate legal entities.

Table 13 is based on the following list of stakeholders:

1. European Commission (EC)
2. Member States
3. Vehicle Manufacturers
4. Infrastructure Managers / Operators
5. Users and Transport Associations
6. Equipment Manufacturers / Operators
7. Accredited security auditors
8. Article 29 GDPR / Data Protection Authorities

Table 13: Overview of legal entities

Roles	Sub-Roles	Legal Entity	Coordinating Stakeholders	Participating Stakeholders
Policy Framework	C-ITS Governing body	C-ITS PPP #1	1 or 2	1,2,3,4,5,6
	C-ITS Supervision Body	C-ITS PPP #2	1 and/or 2	1,2,3,4,5,6,
	C-ITS Certificate Policy Authority	C-ITS PPP #3	2	1,2,3,4,5,6
	Privacy Policy Authority	C-ITS PPP #3	2	1,2,3,4,5,6,8
	Security Policy Authority	C-ITS PPP #3	2	1,2,3,4,5,6
	Compliance Assessment Body	C-ITS PPP #4	2 and/or 3 and/or 4	1,2,3,4,5,6,7,
C-ITS System Management	Operations Governing Body	C-ITS PPP #5	2 and/or 3 and/or 4	1,2,3,4,5,6,
C-ITS System operation	Operations Manager	-	-	2,3,4
	Trust List Manager	EC	1	
	C-ITS Point of Contact (CPOC)	EC	1	
	Accredited PKI Auditor	See existing List of Member States	2	7

A.4.2 Establishment of legal entities needed for C-ITS

The details of each legal entity that needs to be established are described in separate Annexes of this document for each legal entity.

- C-ITS PPP #1 → Annex A.5.1
- C-ITS PPP #2 → Annex A.5.2
- C-ITS PPP #3 → Annex A.5.3
- C-ITS PPP #4 → Annex A.5.4
- C-ITS PPP #5 → Annex A.5.5

The Annex of each legal entity includes the detailed provisions, rules, terms of references and details on

- how the legal entities are established ?
- how the legal entities are composed of in terms of members (public/private)
- the terms of references and workflow how the legal entity operate and reach decisions and deliverables
- how the legal entities are financed ?

A.5 Annex

Annex TBD. (*This is just a placeholder for the details of each legal entity identified in the previous section*)

B. C-ITS Security Policy

B.1 Strategy for information security

B.1.1 General

The strategy for information security is described through goals and objectives based on a high level purpose, vision and mission:

Purpose

The purpose of information security in C-ITS is to ensure that the stakeholder's mission can be achieved by appropriately managing information security risks. As information security management for C-ITS is a two levels approach, this top level security policy is intended to be as lean and mean as possible.

Vision

The C-ITS system provides a minimum level of trust in the information it shares and in the services that are operated. Information security is intended to protect information and information assets by maintaining the level of risk to the organisations and road traffic in general at an acceptable level.

Mission

Information security should be managed as a continuous process by an information security management system, which includes risk management. Effective information security management enables information to be used, stored and shared while protecting its value.

Goals

The overall goals for information security management are:

- compliance with current laws, regulations and guidelines,
- availability / business continuity of ITS services,
- resilience of the C-ITS System against information security incidents.

Objectives

General objectives for information security management are:

- The security of information shall be preserved throughout its lifecycle in a manner that is considered reasonable and appropriate in relation to its classification,
- The security of information processing systems shall be preserved in a manner that is considered reasonable and appropriate in relation to the information they process,
- Entities that are authorized to handle information shall preserve the security of information in a manner that is reasonable and appropriate in relation to the information they process

B.1.2 Information Security Management System (ISMS)

Each operator shall operate an ISMS according to ISO/IEC 27001 with the constraints and additional requirements defined in this section.

Each operator shall determine external and internal issues relevant to C-ITS including:

- COM(2016) 766 final [15]
- The GDPR. [19]

Each operator shall determine parties that are relevant to the information security management system and their requirements including all C-ITS stakeholders defined in Part A of this document.

The ISMS scope shall include all the operated ITS-stations and all other information processing systems that process C-ITS data in the form of C-ITS messages compliant to the following standards:

- CAM [12]
- DENM [13]
- IVIM [14]
- SPATEM [14]
- MAPEM [14]
- SSEM [14]
- SREM [14]

Each operator shall ensure that his information security policy is consistent with this policy.

Each operator shall ensure that his information security objectives include and are consistent with the security objectives and high level requirements in this policy.

The operators shall classify information as defined in section B.2.

The operators shall apply an information security risk assessment process as defined in section B.3. This shall be done at planned intervals or when significant changes are proposed or occur.

The operators and/or manufacturers shall define requirements for mitigating security risks identified in the information security risk assessment process as defined in section B.4.

The manufacturers shall design, develop and assess ITS-stations, and other information processing systems, so that they meet defined requirements.

The operators shall operate ITS-stations and all other information processing systems that implement appropriate information security risk treatment controls according to section B.4.

B.2 Information classification

This chapter defines the minimum requirements that shall be applied for information classification. Note that this does not restrict any stakeholders to apply more stringent requirements.

Operators shall classify handled information according to FIPS 199. According to this standard a security category can be represented as:

Security Category information = {(confidentiality, impact), (integrity, impact), (availability, impact)};

Stakeholders shall classify managed information systems according to FIPS 199 & NIST 800-60. According to those standards a security category can be represented as

Security Category information system = {(confidentiality, impact), (integrity, impact), (availability, impact)};

The acceptable values for potential impact are low, moderate, or high as summarized in Table 14:

Table 14 Potential impact definitions for each security objective of Confidentiality, Integrity and Availability

(from FIPS [6] 199 Table 1)

	Potential Impact		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The following information classification impact types shall be considered in terms of the degree of damage or costs to the C-ITS service and C-ITS stakeholders caused by an information security incident:

- Road Safety – when the impact places road users at imminent risk for injury
- Safety – when the impact places any of the stakeholders at imminent risk for injury
- Operational impacts – when the impact is substantially negative for road traffic efficiency or other societal impact such as environmental footprint and organised crime.
- Legal – when the impact results in significant legal and/or regulatory compliance action against one or more of the stakeholders
- Financial – when the impact results in direct or indirect monetary costs for one or more of the stakeholders.
- Privacy – the GDPR having both legal and financial impact.
- Reputation – when the impact results in a loss of reputation of one or more stakeholders and/or the ITS-System as a whole such as press coverage and/or major political pressure on reputation on a national or international scale.

Stakeholders shall respect the following minimum impact values for the information handled:

Table 15: Impacts

	Information originated by fixed ITS-stations	**Information originated by mobile ITS-stations**
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low PII contained in any of the three messages: moderate
Integrity	CAM: moderate DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	CAM: moderate DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

B.3 Risk assessment

B.3.1 General

Risk assessment shall be periodically conducted according to ISO/IEC 27005. Risk assessment shall include an appropriate documentation of:

- The scope of the risk assessment, i.e. the assessed system and its boundaries, system purpose and the handled information.
- The security risk criteria
- Risk assessment, incl. identification, analysis and evaluation.

B.3.2 Security risk criteria

Risk evaluation criteria shall be defined considering the following aspects:

- The strategic value of the C-ITS service and C-ITS system as a whole to all C-ITS stakeholders.
- The strategic value of the C-ITS service and C-ITS system to the operator of the service.
- The consequences for the reputation of C-ITS as a whole.
- Legal and regulatory requirements and contractual obligations.

Risk impact criteria shall be defined considering the information classification impact types according to section B.2.

Risk acceptance criteria shall include the identification of risks levels, which are unacceptable for the C-ITS service and C-ITS Stakeholders, per impact type.

B.3.2.1 Risk identification

Risk identification shall be done according to ISO/IEC 27005 with the following minimum requirements that apply:

The main assets to be protected are the C-ITS message as defined in section B.1.2.

Supporting assets should be identified including the following:

- Information used for C-ITS messages (e.g. Local Dynamic Map, time, Protocol Control, etc.)
- C-ITS-S and their software, configuration data and associated communication channels
- Central C-ITS control assets
- Every entity within the EU CCMS

Threats to those assets, and their sources, shall be identified.

Existing and planned controls shall be identified.

Vulnerabilities that can be exploited by threats to cause harm to assets or to the C-ITS stakeholders shall be identified and described as incident scenarios.

The consequences that security incidents may have on the assets shall be identified, based on the information classification.

B.3.2.2 Risk analysis

The following minimum requirements apply to risk analysis:

The impact of the identified information security incidents on the C-ITS service and the C-ITS stakeholders shall be assessed based on the information and information system security category using at least the three levels as defined in section B.2. Impact needs to be identified on two levels, one for the total existing C-ITS system/ services and the other for an individual stakeholder/ organisational entity: the highest shall be taken as total impact. The likelihood of the identified incident scenarios shall be assessed using at least the following three levels:

- Unlikely (value 1): the incident scenario is unlikely to occur / difficult to realise, or the motivation for an attacker is very low.
- Possible (value 2): the incident scenario is possible to occur/ possible to realise or the motivation for an attacker reasonable.
- Likely (value 3): the incident scenario is likely to occur / easy to realise and the motivation for an attacker is high.

The levels of risk shall be determined for all identified incident scenarios based on the product of impact and likelihood resulting in at least the risk levels: low (values 1,2), moderate (values 3,4), high (values 6,9) defined as follows:

Table 16: Risk levels

Risk levels as product of impact and likelihood		**Likelihood**		
		Unlikely (1)	**Possible (2)**	**Likely (3)**
Impact	**Low (1)**	Low (1)	Low (2)	Moderate (3)
	Moderate (2)	Low (2)	Moderate (4)	High (6)
	High (3)	Moderate (3)	High (6)	High (9)

B.3.2.3 Risk evaluation

Levels of risks shall be compared against risk evaluation criteria and risk acceptance criteria to determine the risks shall be subject to treatment. At least risks of level moderate or high applicable to the C-ITS service and C-ITS system as a whole shall be treated as defined in B.4.

B.4 Risk treatment

B.4.1 General

Risks shall be treated according to one of the following options:

- risk modification by using controls identified in B.4.2 or B.4.3 so that the residual risk can be reassessed as being acceptable.
- risk retention, only if the if the level of risk meets the risk acceptance criteria.
- risk avoidance.

Risk sharing or transfer is not allowed for risks for the whole C-ITS system.

Risk treatment shall be documented including the:

- Statement of Applicability according to ISO 27001 that contains the necessary controls, determination of residual likelihood of occurrence, determination of residual severity of impact and determination of residual risk level.
- Reasons for risk retention or avoidance.

B.4.2 Controls for ITS-Stations

B.4.2.1 Generic controls

ITS-Stations shall implement appropriate countermeasures to modify risk as defined in section B.4.1. Those countermeasures shall implement generic controls as defined in ISO/IEC 27001, ISO/IEC 27002, NIST 800-53, OSA.

The development of vehicle ITS-Stations should follow the recommendations of SAE J3061.

B.4.2.2 Controls for communication between ITS-Stations

The following minimum mandatory controls shall be implemented on **sender side**:

Table 17: Controls for the sender side

	Information originated by fixed ITS-stations	**Information originated by mobile ITS-stations**
Confidentiality	-	The PII contained in messages shall be secured using an adequate AT change procedure to ensure a level of security adequate to the risk of re-identification of drivers based on their broadcasted data. Therefore ITS-Stations shall change ATs adequately when sending messages and shall not re-use ATs after a change, except in case of non-average[1] driver behavior. A recommended AT change procedure is included in Annex 1.
Integrity	All messages shall be signed according to TS 103 097 [20].	All messages shall be signed according to TS 103 097 [20].
Availability	-	-

[1] The definition of average driving behaviour shall be based on relevant statistical analysis of the driving behaviour in the European Union, e.g. based on data from the German Aerospace Center (DLR)

The following minimum mandatory controls shall be implemented on **receiver side**:

Table 18: Controls for the receiver side

	Information originated by fixed ITS-stations	Information originated by mobile ITS-stations
Confidentiality		Received PII should be retained as short as possible for business purposes with a **maximum retention of 5 minutes** for raw and identifiable data-elements. A received CAM or SRM shall not be forwarded/broadcast. A received DENM may be forwarded/ broadcast only within a limited geographical area.
Integrity	The integrity of all messages used by ITS applications shall be validated according to TS 103 097 [20].	The integrity of all messages used by ITS applications shall be validated according to TS 103 097 [20].
Availability	-	A received SRM shall be processed and produce an SSM broadcast to the originator of the SRM.

To support the security requirements of confidentiality, integrity and availability defined in the previous tables, all ITS-S (mobile ITS-S (including vehicle ITS-S) and fixed ITS-S) shall be assessed and certified using security assessment criteria as specified by Common Criteria / ISO 15408 standard[2]. Due to the different features of the different types of ITS-S and different location privacy requirements, different protection profiles may be defined.

All protection profiles and related documents applicable for the security certification of the ITS stations shall be evaluated, validated and certified according to ISO 15408 applying the SOG-IS agreement[3].

Given the importance of maintaining the highest possible security level, security certificates for C-ITS stations shall be issued by a certification body recognised by the Management Committee within the framework of the 'Mutual Recognition Agreement of Information Technology Security Evaluation Certificates' of the Senior Officials Group on Information Systems Security (SOG-IS).

[2] Common Criteria Portal http://www.commoncriteriaportal.org/cc/

[3] In the road transportation sector SOG-IS has e.g. already been involved in the smart tachograph security certification. The SOG-IS agreement is currently the only organization in Europe, which can support the harmonization of security certification of electronic products. At the moment, SOG-IS only supports the Common Criteria process. Thus the ITS-stations must be assessed and certified by Common Criteria. Link to Website: https://www.sogis.org/ (accessed 12/2017)

B.4.2.3 Controls for ITS-Stations as an End-Entity

ITS-Stations shall comply with the Certificate Policy [1] according to their role as an EU CCMS End-Entity.

B.4.3 Controls for EU CCMS participants

EU CCMS participants shall comply with Certificate Policy [1], according to their role in the EU CCMS.

B.5 Compliance to this security policy

Operators shall periodically request and obtain certification for compliance with this policy following the guidelines for an ISO 27001 audit in [17].

The Auditing Body shall be accredited and certified by a member of the European Accreditation. The Auditing body shall fulfil the requirements of [16].

With the objective of obtaining certification, Operators shall generate and maintain documents addressing the requirements on documented information in [3] clause 7.5. Specifically, operators shall generate and maintain the following documents related to the ISMS:

- Scope of the ISMS (B.1.2 and [3] clause 4.3)
- Information security policy and objectives (B.1.2 and [3] clauses 5.2 and 6.2)
- Risk assessment and risk treatment methodology details (B.3 and clause 6.1.2)
- Risk assessment report (B.3 and [3] clause 8.2)
- Statement of Applicability (B.4 and [3] clause 6.1.3d)
- Risk treatment plan (B.4 and [3] clauses 6.1.3e and 8.3)
- Documents required for the implementation of selected controls (B.4 and [3] annex A).

Additionally, the operators shall generate and maintain the following records as evidence of results achieved:

- Records of training, skills, experience and qualifications ([3] clause 7.2)
- Monitoring and measurement results ([3] clause 9.1)
- Internal audit program ([3] clause 9.2)
- Results of internal audits ([3] clause 9.2)
- Results of the management review ([3] clause 9.3)
- Results of corrective actions ([3] clause 10.1)

B.6 Updating of this security policy

This security policy is subject of continuous improvement. The update process is managed by the Security Policy Authority and follows five major steps:

1. Submission of the change request.
2. Change processing.
3. Change approval.
4. Change publication and announcement.
5. Change implementation.

This Policy shall be checked and updated every 3 years and if there are no applicable changes at least an empty change request shall be submitted and approved to update the date

B.6.1 Submission of the Change Request

The change process is initialized by a change request of a stakeholder. Every stakeholder can submit a change request. The change request shall contain:

- A brief description of the change.
- A rationale for the change.
- Criticality classification for security of the system (low – medium – high)
- The exact proposal including the line/paragraphs to be changed, the old text and the new text.
- A change requester contact.

The change requester should be prepared to answer requests for additional information and/or defend the change proposal at the security policy authority.

B.6.2 Change Processing

Within one working day after receiving the change request, the Security Policy Authority shall confirm reception of the change request. Within 2 weeks after receiving a change request, the Security policy authority shall start processing the change. Processing of a change request means:

- Assessing the applicability of the change request.
- Assessing the completeness of the change request.
- Assessing the criticality of the change request.
- Assessing the impact of the change.

The change processing may confirm that the change is seen as critical for the security of the C-ITS system. If a change requests is seen as critical, the change request becomes an Emergency Change Request**.** To ensure to resolve security critical situations as quickly as possible, emergency change requests will be handled in a shortened process as described in the next steps.

The change processing phase is concluded with scheduling the processed change request for decision in the next change approval meeting of the security policy authority. If the change has been classified as an emergency change request due a disaster recovery scenario, the change approval meeting shall be scheduled for immediate decision, with at least 60% of the members of the security Policy Authority participating, as quickly as possible but at least within 48 hours.

B.6.3 Change Approval

In case of non-emergency change requests the security policy authority conducts change approval meetings to discuss and finally decide if a change request is accepted. Given that change requests have been received, the security policy authority shall conduct a change approval meeting half-yearly. The security policy

authority may invite change requestor contacts and stakeholder experts to participate in the discussion. After discussion, the change approval meeting can decide to:

1. Fully accept the change request without any changes and proceed directly to the change publication and announcement step.

2. Partially accept the change request and proceed to the change publication and announcement step.

3. Decide on a modified change request and proceed to the change publication and announcement step.

4. Request modification of the change request to the initial change requestor and resubmission of the change request.

5. Fully reject the change request.

In case of an emergency change request, the security policy authority shall hold an emergency change approval meeting within 48 hours after conclusion of the change processing. The change approval meeting shall not fully reject security critical change requests. The change approval meeting should not request modification and resubmission of the modified change request to avoid any unnecessary delay.

B.6.4 Change Publication and Announcement

Once a change request is approved by the security policy authority change approval meeting described in the previous section, the policy authority shall publish an updated provisional version of the security policy and announce the implementation with a due date to become effective and an implementation time frame for the transition.

Non-emergency changes shall not become effective until at least two weeks after the next change approval meeting. Any entities, which fulfill the roles and sub-roles defined in section A.3 and are impacted by the change, shall take appropriate preparation to ensure that the implementation can be achieved during the implementation time frame. Stakeholders may submit change requests to modify announced changes for decision on the next change approval meeting. Stakeholders may also submit change request limited on the due-date or the implementation time-frame. Changes increasing the time periods can be decided to be scheduled before the next change approval meeting.

In case of emergency changes, the new policy shall become effective as quickly as feasible and the implementation timeframe shall be as short as feasible. The effectiveness of new policies after emergency changes are not restrained to follow-up change approval meetings. Instead, in these conditions, the change requests affecting announced and not yet implemented emergency changes, automatically follow the emergency change process.

B.7 Annex

B.7.1 Annex 1 – Recommended AT change strategy

This Annex gives recommendations on an AT change strategy to be implemented according to the requirements listed in Table 17. The objective is to trigger AT changes in such a manner that at least 95% of all trips[4] are correctly divided in three segments.

To achieve this objective the following recommended practices are defined:

- An AT change shall be triggered at the interruption of a trip which implies the end of a trip and the start of new trip. This condition is established by the following rules: engine control is deactivated (ignition switched off for thermal engine vehicles, or any other activation for e.g. electric, hybrid and start/stop technologies) for at least 10 minutes AND engine control is activated AND movement detection.
- The next AT change shall be performed during the trip randomly in a range of 800 to 1500 meters from the start position.
- The next AT change shall be performed at least 800 m from the last AT change and randomly within an additional interval of 2 to 6 minutes.
- The next AT change shall be performed after 15 kilometers ± 5 kilometers (randomly)
- Further AT changes shall be performed after 30 kilometers ± 5 kilometers (randomly)

A pool size of 100 ATs with a defined validity period (a value not exceeding 1 week) is managed by the vehicle, with a fix size independently of the vehicle type, the driver profile or its actual usage. The ATs are drawn randomly from the pool with equal probability and without replacement, i.e. after use of one AT, that AT is not used again until the pool is re-started. The pool is re-started when it is completely empty.

References

[1]. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1, June 2017

[2]. ISO/IEC 27000: 2016, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

[3]. ISO/IEC 27001: 2015, Information technology — Security techniques -- Information security management systems -- Requirements

[4]. ISO/IEC 27005: 2011, Information technology -- Security techniques -- Information security risk management

[5]. NIST Special Publication 800-53A Revision 4: 2015, Assessing Security and Privacy Controls in Federal Information Systems and Organizations

[4] The definition of trips shall be based on relevant statistical analysis of the driving behaviour in the European Union, e.g. based on data from the German Aerospace Center (DLR)

[6]. FIPS PUB 199: 2004, Standards for Security Categorization of Federal Information and Information Systems

[7]. OSA: http://www.opensecurityarchitecture.org

[8]. SAE J3061: 2016, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

[9]. ETSI TR 102 893: "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)"

[10]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[11]. ISO/DIS 17427-1 Intelligent transport systems -- Cooperative ITS -- Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s).

[12]. ETSI EN 302 637-2 V1.3.2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

[13]. 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

[14]. ETSI TS 103 301 V1.1.1: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services.

[15]. COM (2016) 766 on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility", 30th of November 2016.

[16]. ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[17]. ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing.

[18]. ETSI EN 302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture.

[19]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[20]. ETSI TS 103 097 V1.3.1. Intelligent Transport Systems (ITS) Security; Security Header and certificate formats.