

WP 3 - Functional Specification and Development

SWP 3.4 Security

Version: 03.60

Release Date: 2016-07-29	
--------------------------	--

Copyright © ECo-AT

The content and information enclosed within this document is the property of ECo-AT project members and copyrighted. All rights, in particular rights of communication, distribution, reproduction, reprinting and translation remain, even in extracts, reserved.

Overview of changes

No.	Version	Status	Date	Type of Change
1	02.00	Released	2015-03-12	Second Release
2	03.00	Released	2015-07-15	Third Release
3	03.10	Released	2015-10-28	Third Release – Update
4	03.50	Released	2016-04-29	Third Release – Second Update
5	03.60	Released	2016-07-29	Third Release – Third Update

Table 1: Document History

Reference to the status- and version administration:

Status:

In progress, the document is currently in editing mode
Released, the document has been checked and released by quality assurance, it can only be modified if the
 version number is updated.

Versions:

Take place in two stages. Released documents receive the next higher integral version number.

00.01, 00.02 etc. Not released versions, with the status in progress

01, 02, etc. Released version with the status released

Table of Contents

WP 3 - Functional Specification and Development	1
SWP 3.4 Security	1
1 Document Information	7
1.1 Purpose of this document	7
1.2 Scope of the document	7
1.3 Definitions, Terms and Abbreviations	7
1.4 References	12
2 Overview	13
2.1 Security Architecture Methodologies	13
2.1.1 Jan Killmeyer	14
2.1.2 TOGAF	14
2.1.3 SABSA	15
2.1.4 TOGAF and SABSA	15
2.1.5 ETSI Threat Vulnerability Risk Analysis (TVRA)	16
2.2 ECo-AT Mapping With Methodologies	17
2.2.1 Jan Killmeyer's approach	17
2.2.2 SABSA	17
2.2.3 TOGAF-SABSA integration	18
2.2.4 ETSI TVRA	19
2.3 Scope of Security Architecture in ECo-AT	19
3 ECo-AT Security Architecture Context	21
3.1 ECo-AT Business Use Cases of Reference	21
3.2 ECo-AT System Architecture of Reference	22
3.3 ECo-AT Business Actors	23
3.4 IF4 (ITS-G5) Communications Security Architecture of Reference	23
3.5 IF4 (ITS-G5) Security Management of Reference (via IF2)	23
3.6 Security Standards of Reference	24
3.6.1 Information Security Management	24
3.6.2 ITS-G5 Communications Security	24
3.6.3 ECo-AT System Components Security	24
3.6.4 ITS-G5 Communications Security Management	25

3.7	PKI Document Framework	25
4	ECo-AT System Assets	26
5	ECo-AT Security Objectives and Security Policy	27
5.1	ECo-AT Security Objectives.....	27
5.1.1	Confidentiality and Privacy	27
5.1.2	Integrity.....	28
5.1.3	Availability	29
5.1.4	Accountability	29
5.1.5	Authenticity	30
5.2	ECo-AT Security Policy	33
6	ECo-AT Security Requirements Specification – System Level	33
6.1	Information Security Management	33
6.2	ECo-AT System Security functionality	34
6.3	IF4 (ITS-G5) Communication Security	35
6.3.1	Ensuring Confidentiality and Privacy.....	35
6.3.2	Ensuring Integrity and Authenticity.....	35
6.3.3	Ensuring Availability and Avoiding Denial of Services	35
6.3.4	Ensuring Accountability and Avoiding Non-Repudiation.....	36
6.4	IF4 (ITS-G5) Communication Security Management (via IF2).....	36
6.4.1	ITS-G5 Communications Domain Model.....	36
6.4.2	Bootstrap (Initialization)	37
6.4.3	Enrolment of ITS Stations	38
6.4.4	Authorization of ITS Stations.....	39
6.4.5	Security Associations between ITS Stations	40
6.5	IF3 (Internal Communication) Security.....	40
6.5.1	IF3 Communication Security Requirements	41
6.5.2	IF3 Security Management	41
6.6	IF1 (TCC to C-ITS-S) Communication Security	41
6.7	IF6 & 7 (R-ITS-S to TLC&Trailer) Communication Security.....	41
7	ECo-AT Security Requirements Specification – Component Level.....	42
7.1	Central ITS Station Security Functionality	42
7.1.1	Baseline Controls	42
7.1.2	Specific Controls	45
7.2	Roadside ITS Station Security Functionality	45

7.2.1	Baseline Controls	45
7.2.2	Specific Controls	47
7.3	Central ITS Station Security Management Functionality	48
7.3.1	IF3 (Internal Communication) Security Management Functionality	48
7.3.2	IF4 (ITS-G5) Security Management Functionality support.....	48
7.4	Roadside ITS Station Security Management Functionality.....	48
7.4.1	IF3 (Internal Communication) Security Management Functionality	48
7.4.2	IF4 (ITS-G5) Security Management Functionality.....	49
8	ECo-AT Security Design - Logical ITS Security Architecture.....	49
8.1	Logical Security Architecture During Operation	50
8.1.1	ITS Functionality.....	51
8.1.2	ITS Security Services	51
8.1.3	ITS Security Management Services	51
8.1.4	PKI Management Services.....	52
8.1.5	ITS-G5 Public Key Infrastructure	53
8.1.6	Traffic Control Center (TCC)	53
8.1.7	Roadside Operator System.....	53
8.1.8	Traffic Light Controller (TLC).....	53
8.1.9	RWW trailer	53
8.1.10	PVD	53
8.2	Logical Security Architecture during Manufacturing Phase	54
8.2.1	Manufacturer System	55
8.3	IF4 (ITS-G5) Communication Security Services Catalogue.....	55
8.4	IF4 (ITS-G5) Security Management Services Catalogue.....	55
8.5	IF4 (ITS-G5) PKI Management Services Catalogue.....	56
9	ECo-AT Security Design - Physical ITS Security Architecture.....	57
9.1	IF4 (ITS-G5) Security	57
9.1.1	Communication Security Specification.....	57
9.1.2	Security Management Specification.....	57
9.2	IF3 (Internal Communication) Security.....	57
9.2.1	Communication Security Specification.....	57
9.2.2	Security Management Specification.....	58
9.3	ITS Station security	58
	Annex A - High level information security Policy (Strategy).....	59

Annex B - Security Attributes and Impact classes	63
Annex C : Threat Analysis	65
Methodology	65
Security objectives and protection level	65
Security requirements	65
Assets to be protected	65
Target of evaluation	65
Thread, vulnerability and risk analysis	66

List of Tables

Table 1: Document History	2
Table 2: Definitions, Terms and Abbreviations	12
Table 3: SABSA Views and Layers	15
Table 4 SABSA-TOGAF Integration. Source: www.opengroup.org	16
Table 5 Use Cases in Scope	22
Table 6 Target protection level for information in ECo-AT	32
Table 7 OSA controls family classification	35
Table 8 OSA controls relevant for C-ITS-S	45
Table 9 OSA controls relevant for R-ITS-S	47
Table 10: G5 Communication Security Service Catalogue	55
Table 11: G5 Security Management Service Catalogue	56
Table 12: G5 PKI Management Services Catalogue	56
Table 13 Security attributes and impact classes	64

1 Document Information

1.1 Purpose of this document

This document describes the considerations regarding security for the ECo-AT project. This document is part of the work package 3, the functional specification.

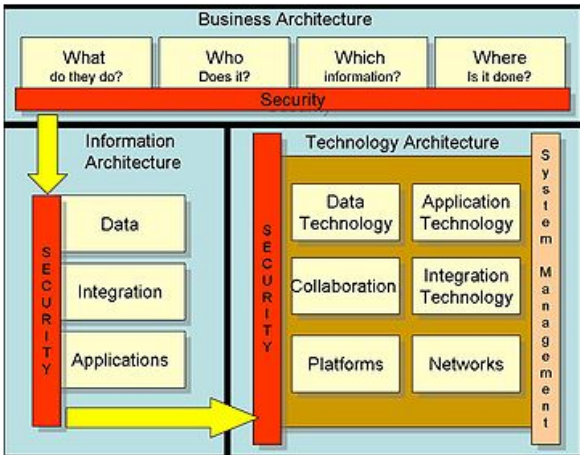
1.2 Scope of the document

This document specifies the security architecture of the ECo-AT system described in [ECo-AT SWP2.3 system overview].

1.3 Definitions, Terms and Abbreviations

Abbreviation / Term	Definition
AA	Authorization Authority
Architectural structure	A physical or logical layout of the components of a system design and their internal and external connections EXAMPLE function-oriented (structured) design, object-oriented design, and data structure- oriented design
Architecture	1. Fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution. [ISO 15288], Systems and software engineering — System life cycle processes.4.5. 2. The organizational structure of a system or component. 3. The organizational structure of a system and its implementation guidelines. Synonym: architectural structure cf.: component, module, subprogram, routine NOTE sometimes refers to the design of a system's hardware and software components
Accountability	Accountability: property that ensures that the actions of an entity can be traced

Abbreviation / Term	Definition
	uniquely to the entity [ISO/ 21827]
ADM	Architecture Development Method
AG	Amsterdam Group – co-operation of C2C-CC, CEDR, ASECAP & POLIS for European roll-out of Cooperative ITS
Authenticity	Property that an entity is what it claims to be. [ISO 27000] The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. [NIST 800-39]
Availability	Ensuring timely and reliable access to and use of information. Property of being accessible and usable upon demand by an authorized entity. [ISO 27000]
C2C-CC	Car2Car Communication Consortium
CAM	Cooperative Awareness Message
C-ITS	Cooperative ITS – C-ITS is a “subset of overall ITS that communicates and shares information between ITS stations to give advice or facilitate actions with the objective of improving safety, sustainability, efficiency and comfort beyond the scope of stand-alone systems” [ISO 17465]
C-ITS-S	Central ITS Station
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Source: [ISO 27000] Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542] [NIST 800-39]
DENM	Decentralized Environment Notification Message
EA	Enrollment Authority

Abbreviation / Term	Definition
Enterprise (Information) Security Architecture	<p>Enterprise information security architecture (EISA) is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well. Source: Wikipedia</p>  <p>The diagram illustrates the components of Enterprise Information Security Architecture (EISA). At the top is 'Business Architecture' with four sub-components: 'What do they do?', 'Who Does it?', 'Which information?', and 'Where is it done?'. Below this is a red bar labeled 'Security'. The main body is divided into two columns: 'Information Architecture' on the left and 'Technology Architecture' on the right. 'Information Architecture' includes 'Data', 'Integration', and 'Applications'. 'Technology Architecture' includes 'Data Technology', 'Application Technology', 'Collaboration', 'Integration Technology', 'Platforms', and 'Networks'. A vertical red bar labeled 'SECURITY' runs through the center of both architectures. A yellow arrow points from 'Information Architecture' to 'Technology Architecture'. On the far right, a vertical label reads 'System Management'.</p> <p>Information Security Architecture (from [NIST 800-39]):</p> <p>A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. [NIST 800-39]</p>
Enterprise architecture	<p>It is "a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach at all times, for the successful development and execution of strategy. Enterprise Architecture applies architecture principles and practices to guide organizations through the business, information, process, and technology changes necessary to execute their strategies. These practices utilize the various aspects of an enterprise to identify, motivate, and achieve these changes." Source: Wikipedia</p>

Abbreviation / Term	Definition
Entity	It may be a person, process, object or any combination of such components.
Functional Security Requirements	These are the security services that need to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations
IF	Interface
Integrity	<p>The property of protecting the accuracy and completeness of assets [ISO 27000]</p> <p>The property of safeguarding the accuracy and completeness of information and processing methods [ISO 21827]</p>
ITS-G5	V2X communication standard specified at ETSI using 5,9 GHz frequency band
IVI	In-Vehicle Information
MAP	Message to convey local, detailed network topology in specific areas, as specified in [ISO 19091]
PKI	Public Key Infrastructure
PVD	Probe Vehicle Data
R-ITS-S	Roadside ITS Station
RWW	Road Works Warning
Secure Functional Requirements	This is a security related description that is integrated into each functional requirement. Typically this also says what shall not happen. This requirement artifact can for example be derived from misuse cases
Secure System	A collection of securely interacting components organized to accomplish a specific function or set of functions within a specific environment
Secure System	The fundamental organization of a system embodied in its components, incl.

Abbreviation / Term	Definition
Architecture	the components for security management
Security Management System	The fundamental organization of a system that supports a given system and its secure functions, embodied in its components
Security Requirement	<p>The term security requirement is used by different communities and groups in different ways and may require additional explanation to establish the particular context for the various use cases. Security requirements can be stated at a very high level of abstraction, for example, in legislation, Executive Orders, directives, policies, standards, and mission/business needs statements. FISMA and FIPS Publication 200 articulate security requirements at such a level.</p> <p>Acquisition personnel develop security requirements for contracting purposes that address the protections necessary to achieve mission/business needs. Systems/security engineers, system developers, and systems integrators develop the security design requirements for the information system, develop the system security architecture and the architecture-specific derived security requirements, and subsequently implement specific security functions at the hardware, software, and firmware component level.</p> <p>Security requirements are also reflected in various nontechnical security controls that address such matters as policy and procedures at the management and operational elements within organizations, again at differing levels of detail. It is important to define the context for each use of the term security requirement so the respective communities (including individuals responsible for policy, architecture, acquisition, engineering, and mission/business protection) can clearly communicate their intent.</p> <p>Organizations may define certain security capabilities needed to satisfy security requirements and provide appropriate mission and business protection. Security capabilities are typically defined by bringing together a specific set of safeguards/countermeasures (i.e., security controls) derived from the appropriately tailored baselines that together produce the needed capability. [NIST 800-53]</p>
SPAT	Signal Phase and Timing
SWP	Subworkpackage

Abbreviation / Term	Definition
System	A collection of interacting components organized to accomplish a specific function or set of functions within a specific environment
System Architecture	The fundamental organization of a system embodied in its components. It can be of different types: enterprise, data, technical, IT
TCC	Traffic Control Center
TVRA	Threat Vulnerability Risk Analysis
V-ITS-S	Vehicle ITS Station
WP	Workpackage

Table 2: Definitions, Terms and Abbreviations

1.4 References

All references in this document can be found in the master table of references available in the “Eco-AT_SWP2.3_MasterTableOfReferences_v03.60.pdf” document.

2 Overview

Generally security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, technical equipment or information (<http://en.wikipedia.org/wiki/Security>).

Within the scope of this security architecture, security will be limited to information security. Information security is the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [ISO 27002].

To ensure security of the processed information, it is necessary to design, set up and maintain the corresponding security architecture.

In general, a security architecture can be described both as the process and the result of defining the architecture (see definitions below), components, interfaces, and other characteristics of a secure system, i.e. a system which in addition to its functional requirements fulfils the security requirements, addresses the risks of a particular environment/scenario and specifies security controls to be applied.

A security architecture can be developed with any level of granularity and scope, from a project of limited scope to an entire enterprise architectural framework. An enterprise security architecture delivers security solutions that support the enterprise's critical business goals and processes. If seen as a process, enterprise security architecture begins by defining a security policy that everyone in the corporation accepts and supports. The ultimate goal is to fully integrate the security architecture into the enterprise architecture of the operating organization. As a first step to secure the operation of cooperative ITS applications and the involved business information in the ECo-AT system, this document is focused on designing the minimal necessary security architecture. This security architecture provides the minimum technical building blocks that should be used by the operating entity to define a complete enterprise security architecture. Those minimal blocks are designed based on a security architecture that focuses on communications and data security, and as such is not a complete security architecture but rather a template to be used to define a complete enterprise security architecture for example using the SABSA and TOGAF approaches as explained below. Consequently, several artifacts and steps of a complete security architecture development will be left out.

2.1 Security Architecture Methodologies

Different approaches to set up a security architecture are available. This section provides an overview of some of these methodologies and briefly describes them.

2.1.1 Jan Killmeyer

Jan Killmeyer proposes that an integrated security architecture for an organization can be developed by a methodology comprehending the following five stages and deliverables (inspired by **[KILLMEYER]**).

It begins with a preliminary assessment of the system to be secured and its context to develop a security posture. This includes analyzing the system architecture, available security controls and **security standards**. They may be set as a **baseline** for the development of the new security architecture.

Based on the context analysis and business strategy a **security policy** needs to be defined. A policy is designed to inform all individuals operating within an organization of how they should behave related to a specific topic. Here it provides high level security objectives, direction and guidance in the development of standards and procedures. Procedures are plans, processes or operations that address the specifics of how to go about a particular action.

The next step is the **risk assessment**. This is a procedure for elaborating specific security requirements for the specific business use cases and information system by analyzing vulnerabilities of the system, deducing possible threats and evaluating their risk potential (probability of occurrence).

Taking the security policy and the security requirements into account the new **security organization and infrastructure** can be elaborated, e.g. the information technology security architecture including the security services and the security processes, guidelines and procedures are defined. Eventually a set of design artifacts result from this process, which describe how the security controls or security countermeasures are positioned and how they relate to the overall information architecture, i.e. information system. Controls can be technical, operational or managerial.

The forth step of the methodology provides **training programs** and the improvement of **security awareness** for involved personnel.

Finally, the whole process is also accompanied by an auditing process to ensure continuous **compliance** with the developed security architecture.

Other established holistic methodologies for guiding the development of enterprise security architectures are the "The Open Group Architecture Framework" (TOGAF), **[TOGAF]**, and the Sherwood Applied Business Security Architecture (SABSA) model, **[SABSA WP]**.

2.1.2 TOGAF

TOGAF is a methodology providing methods and tools for assisting in the acceptance, production, use, and maintenance of enterprise architecture. It is based on an iterative process model supported by best practices and a re-usable set of existing architecture assets. TOGAF treats security and risk either implicitly through stakeholder requirements or through a limited set of techniques (Security Architecture and the Architecture

Development Method (ADM)). The ADM contains the concept of artifacts that are consumed or produced by each phase.

2.1.3 SABSA

SABSA is a security architecture approach which proposes a layered model comprising six layers:

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Service Manager's View	Security Service Management Architecture

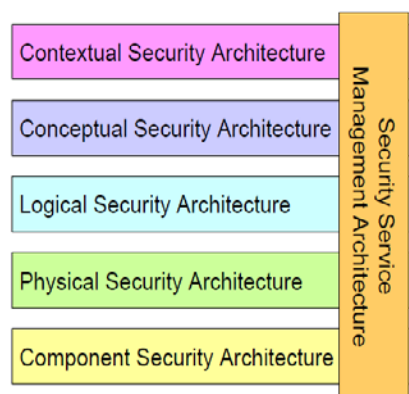


Table 3: SABSA Views and Layers

The SABSA model then provides the basis for an architecture development process. Business attribute profiling is at the heart of the SABSA framework. It is a requirements engineering technique that translates business goals and drivers into requirements using a risk-based approach. For further information and explanation about the SABSA model, refer to [SABSA WP]

2.1.4 TOGAF and SABSA

TOGAF and SABSA can be combined such that the SABSA business risk and opportunity-driven security architecture approach can be seamlessly integrated into the TOGAF business strategy-driven approach to develop richer, more complete enterprise architecture (see [TOGAF SABSA]). So SABSA artifacts can be associated with TOGAF phases as shown in the following picture.

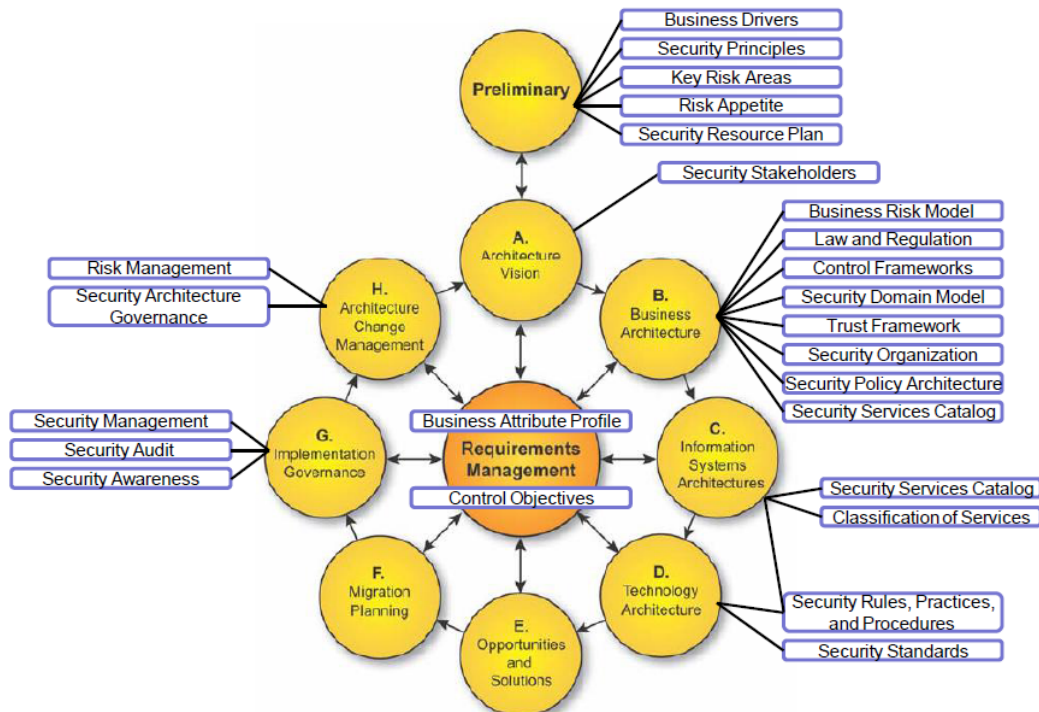


Table 4 SABSA-TOGAF Integration. Source: www.opengroup.org

The TOGAF-SABSA integration approach is based on three cornerstones:

1. Risk management is the driver for the selection of security measures – the SABSA approach to operational risk management is business-driven instead of threat-driven. The business-driven approach also considers the risk context in achieving a positive outcome, whereas the threat-driven approach only looks to minimize or eliminate the possibility of a loss event.
2. Requirements management plays a central role in successful architecture development – TOGAF follows a requirements-driven approach and SABSA Business Attribute Profiling provides a powerful technique to capture architectural requirements.
3. The relevant security architecture artifacts for each phase of the ADM, so that the security architecture becomes an integrated part of the enterprise architecture.

2.1.5 ETSI Threat Vulnerability Risk Analysis (TVRA)

This methodology is described in detail in [ETSI 102 165-1]. The description of the method is under copyright, so it shall not be recited here. In general the process of developing the security architecture is illustrated in Figure 1 on page 14 and explained in the chapter 5.1 of that document. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk. The association of security objectives, requirements, threats and assets provides the rationale for selecting the security architecture and the countermeasures.

2.2 ECo-AT Mapping With Methodologies

The following sub-chapters explain which artifacts of the above introduced methodologies are contained in the ECo-AT architecture. This mapping should help the operations organizations to design and implement or extend their enterprise security architectures.

2.2.1 Jan Killmeyer's approach

The Jan Killmeyer's approach is more abstract than the SABSA-TOGAF approach and therefore can be used as a general guideline.

2.2.2 SABSA

This methodology is concerned about the enterprise perspective on security architecture and provides practical methods and tools for the security architecture development. It maps as follows.

Contextual Security Architecture (The Business View)

The Business View, i.e. the view of the business context, is given by the customer envisaging the relevant ITS Services for ECo-AT and not further analyzed in this document. The business owner is strongly recommended to analyze the contextual architecture and create an overall security architecture covering the following:

- The business assets and needs for information security
- The potential business risk
- The business processes and functions that need to be protected
- The business location, sites, and organizational aspects of business security

Conceptual Security Architecture (The Architect's View)

The Architect's View, i.e. the conceptual security architecture, is defined by two components:

- The ITS communication security reference architecture [ETSI 102 940], and its strategy of using a Public Key Infrastructure (PKI) with a two layered structure (short and long term certificates). This reference architecture brings along a set of actors with their roles and responsibilities and the associated security domains.
- The ECo-AT system security architecture as defined by its security objectives which describe what needs to be protected.

Those two components are the basis for a set of requirements to the ECo-AT System that describes the components of the conceptual layer; mainly the "why" and also the "how" and "who".

Logical Security Architecture (The Designer's View)

The designer interprets the architect's conceptual vision and turns it into a logical structure. This logical security architecture involves the identification and specification of the logical architectural elements of the overall system and includes:

- The business specific information exchanged by ITS-Stations via G5
- The business information stored and forwarded internally in the identified system
- The security policy for the operation of ITS communication security and the security management system
- The definition of security services for ITS communication security, ITS security management and PKI management
- The definition of rules and recommendations for security services, e.g. IT security according to best practices
- The roles of the identified entities, the associated security domains and their activities

Physical Security Architecture (The Builder's View)

The builder has to choose and assemble the physical elements that will make the logical design come to life. These abstractions need to be turned into a physical architecture model that describes the actual technology model and specifies the detailed design of the various system components.

For ECo-AT this includes the security objects (data structures) exchanged by ITS Stations via G5 and the algorithms, mechanisms and processes associated with these objects.

Component Security Architecture (The Tradesman's View)

The Tradesman's View, i.e. the components architecture is under responsibility of those parties that will tender and supply the final system, e.g. the manufacturers and integrators.

Security Service Management Architecture (The Service Manager's View)

The Service Manager's View, i.e. the service management security architecture is under responsibility of the entity operating the system, e.g. the road operator or the manufacturer on its behalf.

2.2.3 TOGAF-SABSA integration

According to the TOGAF-SABSA integration the TOGAF methodology is enhanced with the SABSA approach. Therefore the ADM phases are enriched with the SABSA techniques and artifacts. This maps as follows:

In **phase A** (Architecture Vision) the scope, constraints and expectations for the project are set. See chapter 2.3 for more details.

In **phase B** (Business Architecture) baseline and target architectures are developed. This includes the SABSA conceptual and logical security architecture. The following security related artifacts result from this phase:

- The Security Organization for ITS-G5 communications based on the ITS Reference Architecture provided by [ECo-AT SWP2.3 system overview]
- Security Domain Model describing the interactions between the various domains, parties, and actors
- The Security Policy for ITS communications
- A Business Risk Model for ECo-AT specific use cases, i.e. the equivalent of the ETSI Threat, Vulnerability and Risk Analysis.
- The Security Services Catalogue for ITS communications and security management

The following security elements result from **Phase C**:

- The Security Services Catalogue for ITS-G5 communications and security management
- Security rules, practices and procedures for handling security objects.

The Technology Architecture results from the work done in **phase D**. This comprises security rules, practices and procedures and references to security standards.

2.2.4 ETSI TVRA

For ECo-AT the relevant steps (1-10) for performing the TVRA are described in [ETSI 102 165-1] on page 20 and its Annex A. It could be thought of as an extension to the TVRA described in [ETSI 102 893].

2.3 Scope of Security Architecture in ECo-AT

The ECo-AT security architecture provides the following building blocks to integrate with the enterprise security architecture of the organization designing, implementing and operating the cooperative ITS applications:

- The context, including references to the business use cases, the ECo-AT system of reference, the ITS-G5 security architecture of reference, the ITS-G5 security management systems of reference, the relevant security standards and a document framework necessary to set up and operate a Public Key Infrastructure.
- The ECo-AT business actors
- The ECo-AT system assets
- The ECo-AT security objectives
- A recommendation for a high level security policy, or security strategy
- Recommendations regarding Information Security Management

- The requirement specification that applies system wide and as a black box in front of the external interfaces:
 - the ITS-G5 communication interface (see below for clarification)
- The requirement specification that applies to the components within the ECo-AT system
 - the internal communication interfaces within the ECo-AT system
 - the ITS-G5 communication interface
- The security system design

The ITS-G5 communications security aspects have been already analyzed by the TVRA in [ETSI 102 893]. Therefore this document only provides the TVRA for the ECo-AT System without ITS communications and incorporates the ETSI TVRA by reference.

The ECo-AT security architecture also builds on existing solutions and is constrained by the system context (see chapter 3). Only the systems necessary to collaborate and communicate with the ITS-G5 Public Key Infrastructure, i.e. ITS-G5 Root Certification Authority (ITS-G5 Root-CA), Enrollment Certification Authority (E-CA) and Pseudonym Certification Authority (P-CA), also called Authorization Authority (AA), are in scope and not the ITS-G5 PKI itself. The security architecture(s) of those CAs should be developed by their operators, e.g. as specified by the C2C-CC-PKI concept.

The ECo-AT security architecture will provide requirements for host platforms, network layout or other hardware or software specifics, but not detailed requirements for their implementation. Also the security within adjacent systems, speaking of ASFINAG central network application level communication, not directly involved in the ITS-G5 data processing or transfers, is out of scope. Each supplier is self-responsible for proprietary functionality or interface extensions.

It is out of scope:

- Integrate the ECo-AT security architecture with the enterprise security architecture of the operating organization, i.e. the operator.
- The operator specific processes.
- Business requirements for use cases (non-functional requirements like reliability).

Regarding the introduced methodologies, the following clarifications should be must be considered when choosing one of them to design and implement or extend the enterprise security architecture of the operator: According to the methodology described by Jan Killmeyer, the security procedures (mainly concerning administrative controls), security awareness, training programs and compliance measures are out of scope. Procedures for maintaining the security architecture and compliance measures, such as the validation of the effectiveness of the implemented security controls and auditing of changes in security to prevent misuse and unintentional repudiation, are not considered.

For the TOGAF-SABSA-integrated approach the scope is as follows:

Only the phases A to D are relevant in ECo-AT. The preliminary phase is part of the project planning and the remaining phases are focused on implementation and not considered here.

Excluded from SABSA's Designer's View is:

- The Root CA
- An entire security policy for the entire project/system and/or enterprise

Excluded from SABSA's Builder's View is:

- Specification of host platforms and network layout, hardware and software,
- Specification of physical process and communication sequences,
- Specification of access rights and security measures of data at rest and in use in the sub-systems of ECo-AT internally, i.e. Central ITS Station and Roadside ITS Station.

The Business view, the view of the business context, i.e. the contextual security architecture is implicitly given by the customer envisaging the relevant ITS Services for ECo-AT and not further analyzed in this document, see chapter 2.2.

3 ECo-AT Security Architecture Context

This chapter describes the context in which the ECo-AT Security Architecture is designed and will be realized and maintained. ECo-AT Security Architecture cannot be set up, implemented or maintained without knowing and understanding the presented contextual elements.

3.1 ECo-AT Business Use Cases of Reference

This version of the ECo-AT Security Architecture considers the following Business Use Cases defined by the ECo-AT Sub-Work Package (SWP) 2.3:

Use Case Name	Direction of the ITS-G5 Communication	Type of Message
Road Works Warnings (RWW)	Infrastructure to Vehicle (I2V)	DENM (Day 1) / IVI (Day 2)
In-vehicle Information (IVI)	Infrastructure to Vehicle (I2V)	IVI
CAM Aggregation	Vehicle to Infrastructure (V2I)	CAM

Intersection Safety (ISS)	Infrastructure to Vehicle (I2V)	SPaT / MAP
Other DENM applications (TCC to V-ITS-S and V-ITS-S to TCC)	Vehicle to Infrastructure (V2I) Infrastructure to Vehicle (I2V)	DENM

Table 5 Use Cases in Scope

This table is subject to be updated in future releases of ECo-AT.

For more information about the Use-Cases, refer to [ECo-AT SWP2.1 UC overview].

3.2 ECo-AT System Architecture of Reference

This version of the ECo-AT Security Architecture considers the following system architecture of reference defined by the [ECo-AT SWP2.3 system overview]:

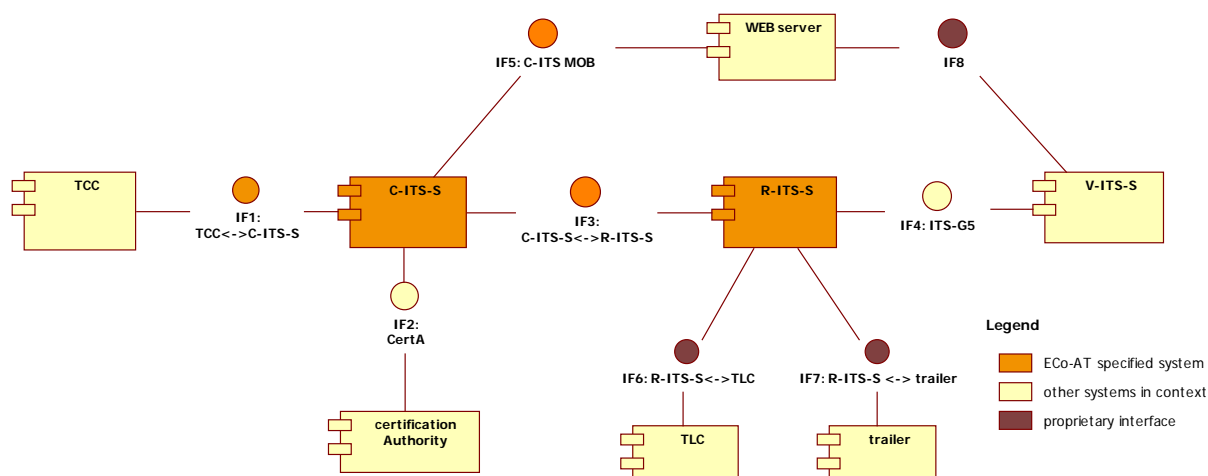


Figure 1 High level ECo-AT system architecture

Note that the term “ECo-AT System” is used in this document as the Cooperative Intelligent Transport System specified within the ECo-AT project. In the figure above is named “ECo-AT specified system”.

For more information about the ECo-AT system design, refer to [ECo-AT SWP2.3 system overview].

This version of the ECo-AT Security also considers the operational scenarios 1 and 2 defined in ECo-AT SWP 2.3, refer to [ECo-AT SWP2.3 system overview].

Note: this specification does not specify whether scenario 1 or 2 is going to be used: it supports both and leaves the choice open to a later decision.

3.3 ECo-AT Business Actors

It is assumed that the following business actors are involved in the operation of the ECo-AT System:

- System operators,
- Manufacturers of the Road ITS Station (operational scenario 2),
- Manufacturers of Central ITS Station (operational scenario 2).

Indirectly involved in the operation are:

- Road operator,
- Operator of the Root Certification Authority of ITS-G5 Public Key Infrastructure (ITS-G5 RootCA),
- Operator(s) of the Enrolment Authority(-ies) of the ITS-G5 Public Key Infrastructure,
- Operator(s) of the Authorization Authority(-ies) of the ITS-G5 Public Key Infrastructure.

It is assumed that the following business actors are involved in the manufacturing of ITS Stations:

- Manufacturers of the Road ITS Station,
- Manufacturers of Central ITS Station.

3.4 IF4 (ITS-G5) Communications Security Architecture of Reference

The communications architecture of reference is the one defined in [ETSI 302 665].

The communications security architecture of reference is the one defined in [ETSI 102 940]. See “Figure 4: Architectural ITS security layers” in [ETSI 102 940].

ECo-AT Security Architecture considers this communications security architecture as reference and adapts it by selecting and extending the security services and security management services specified by [ETSI 102 940]. The adaption is done according the requirements elicitation considering the specific ECo-AT Business Use Cases and the system architecture in scope.

3.5 IF4 (ITS-G5) Security Management of Reference (via IF2)

Important Note: The interface to the PKI will be left open. A decision needs to be taken which security concept will be chosen by the operator and if the concept is chosen, a PKI provider needs to be selected. At the moment there are quite fundamental discussions in the EC about the infrastructure security concepts. As soon as there is an agreement and clarity about the future concept, an interface of a PKI provider with an appropriate security policy can be referenced.

3.6 Security Standards of Reference

3.6.1 Information Security Management

An Information Security Management System (ISMS) “provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve, business objectives based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks” (according [ISO 27000]).

It is assumed that the organizations providing the ITS business services (road operators) have implemented and maintain such ISMS. Some of the organizations might have implemented them according the requirements defined in the international standard [ISO 27001], following the guidelines defined in [ISO 27002] and applying the IS Risk Management methodology established in [ISO 27005]. Other organizations might have used the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) [BSI ST 100-1], followed the guidelines defined in the [BSI ST 100-2] and applied the IS Risk Management methodology established in [BSI ST 100-3].

These organizations might also follow the Austrian Security Manual (*Österreichischen Informationssicherheitshandbuchs*) published by the *Bundeskanzleramt Österreich* (BKA) in collaboration with the *Zentrum für sichere Informationstechnologie – Austria*”, the *Bundesamt für Sicherheit in der Informationstechnik* (BSI) and the Swiss *Informatikstrategieorgan des Bundes* (ISB).

The ECo-AT Security Architecture intends to be compatible and to integrate with any of those ISMS.

3.6.2 ITS-G5 Communications Security

For the definition of security measures that ensure trust between ITS stations as communication end-points in the ECO-AT System and to protect them against external threats (other external communication end-points) the following standards and best practices may be used when applicable:

- ETSI TS-102940 [ETSI 102 940]

3.6.3 ECo-AT System Components Security

The following standards and best practices may be used when applicable for the definition of security measures that protect the components forming the ECo-AT System against internal and external threats and that ensure the achievement of the ECo-AT security objectives:

- ETSI TS-102940 [ETSI 102 940]
- ETSI TS-102941 [ETSI 102 941]
- Open Security Architecture [OSA]

- ISO 27002 [ISO 27002]

3.6.4 ITS-G5 Communications Security Management

For the definition of the necessary system functionality to enable and manage the defined security measures the following standards may be used when applicable:

- ETSI TS-102940
- C2C-CC specifications if available

3.7 PKI Document Framework

This chapter gives a summary of documents to install and operate a Public Key Infrastructure (PKI). or a Certificate Authority. On assessments many of the summarized documents will be requested by the assessors.

The collection was built on standard and assessment related recommendations. Also some legal aspects are enumerated. Main input documents are the [RFC 3647] from IETF and the *PKI Assessment Guidelines* from (ABA), the American Bar Association.

1. Security policy

The security policy of a system is a prerequisite document and some other PKI related documents will cross reference this document.

For further information read http://en.wikipedia.org/wiki/Security_policy.

2. Certificate Policy

A PKI system consists of several security authorities. How the authority's interwork is described in the PKI certificate Policy. This document is valid for the whole PKI.

For further information read http://en.wikipedia.org/wiki/Certificate_policy.

A common reference to generate a Certificate Policy is [RFC 3647] from IETF.

3. Certificate Practice Statement

For every component (authority) of the PKI a Certificate Practice Statements describes the rules of handling certificates.

For further information read http://en.wikipedia.org/wiki/Certification_Practice_Statement.

A common reference how to generate a Certificate Policy is [RFC 3647] from IETF.

4. PKI disclosure statement

A PKI disclosure statement is usually a short summary of the CP and the various CPS which will be published. It can also be part of another document.

5. Subscriber agreements

Are contracts and/or terms and conditions between subscribers and the CA, i.e. how to use the certificates. A frequently used template for subscriber agreements can be found in the “PKI Assessment Guidelines” from the American bar organization.

http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf

6. Relying party agreements

Are contracts and/or terms and conditions between the relying parties and the CA. Sometimes also used for PKI assessment. A frequently used template for relying party agreements can be found in the “PKI Assessment Guidelines” from the American bar organization.

http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf

7. Interoperability or cross-certification agreements

Agreements with other CAs needed for cross certification or to be part of a higher level PKI. It needs to be checked if cross certification is needed. But at least interoperability with CAs operated by other parties need to be provided.

8. Certificate management control objectives

These are the objectives in connection with an audit or assessment.

A frequently used template for Certificate management control objectives can be found in the “PKI Assessment Guidelines” from the American bar

organization. http://www.americanbar.org/content/dam/aba/events/science_technology/2013/pki_guidelines.authcheckdam.pdf

9. Legislation and regulations

All valid national and territorial laws and regulations for electronic signature or corresponding. It needs to be evaluated if the laws are applicable for this kind of communication.

10. Standards

All standards for assessment and implementing the PKI or the CA

4 ECo-AT System Assets

The following are the information security assets that should be protected:

Services and functions:

- Security services
- Security management services
- Software incl. Crypto Algorithms

- Hardware

Information assets:

- **“ITS information”** is an umbrella term that groups all pieces of **business information** (data assets) that are part of the ECo-AT business use cases.
- **“Security Management Information”** is an umbrella term that groups those pieces of information (data assets) that characterize the ECo-AT security management use cases. For example: certificate, certificate request, Certificate
- **“Security Information”** is an umbrella term that groups all the pieces of information that characterize the ECo-AT security use cases (security functionality). For example: key pairs, digital signature, time stamp, user authentication credentials (passwords, user ID, enrolment credentials) user/ITS-S authorization credentials (authorization certificates)
- **“User Information”**
- **“Operator Information”**
- **“IT System configuration data”**, e.g. parameters

5 ECo-AT Security Objectives and Security Policy

5.1 ECo-AT Security Objectives

The security objectives identify the broad aims of a standard or system in terms of the protection to be given to users and information within the framework of the CIAAA attributes. The security objectives represent the starting point for the TVRA method introduced in section 2.1.

The following general objectives are specified:

- Ge1. The ECo-AT System should follow the ETSI Standards for establishing the necessary protection at the ITS-G5 channel.
- Ge2. The ECo-AT System is the target system specified in the ECo-AT project.
- Ge3. The ECo-AT System is the system needed for the realization of the ECo-AT Business Use Cases and it is specified by the SWP 2.3

5.1.1 Confidentiality and Privacy

The security objectives defined in chapter 6.1 of [ETSI 102 893] should be also satisfied.

The following security objectives related to the confidentiality of stored and transmitted ITS information are specified:

- Co1. Information produced by the ECo-AT System based on information broadcasted by authorized vehicle ITS-S should be protected against unauthorized access with the protection level as

defined in table 7. Rationale: disclosure of information such as traffic data would imply a business advantage of third parties and loss of reputation for the ECo-AT System owner.

- Co2. Information collected by the ECo-AT System from authorized ITS-S based on special access rights should be protected against unauthorized access with the protection level as defined in table 7. Rationale: information such as probe data is only provided to the ECo-AT System on the basis that they are handled securely.
- Co3. Personally Identifiable Information (PII) collected by the ECo-AT System from authorized vehicle ITS-S should be either protected against unauthorized access with the protection level as defined in table 7 or be deleted. Rationale: if PII are collected they need to be handled in accordance to privacy regulations. This objective might overlap with C02 depending on the content of probe data.
- Co4. Information collected by the ECo-AT System from external sensors and/or legacy systems should be protected against unauthorized access with the protection level as defined in table 7. Rationale: if data is collected from external systems such as traffic light controllers, it needs to have a defined level of protection or be deleted.
- Co5. Security Management Information held within an ITS-S should be protected from unauthorized access.
- Co6. Confidentiality of information transferred on interfaces between the ECo-AT System components identified in WP2.3 should be protected with a level of protection comparable to that used on the ITS-G5 link.

5.1.2 Integrity

The security objectives defined in chapter 6.2 of [ETSI 102 893] should be also satisfied.

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

- In1. Business information held within the ECo-AT System should be protected from unauthorized modification and deletion with the protection level as defined in Table 7. Rationale: serious danger and/or loss of reputation can be caused by incorrect information provided by the ECo-AT System.
- In2. Business information transmitted from the ECo-AT System to vehicle ITS-S should be protected from unauthorized modification according to ETSI Standards for ITS-G5 security.
- In3. Security Management Information held within an ITS-S should be protected from unauthorized modification and deletion with the protection level as defined in table 7.

- In4. The parameters and software that rule the ECo-AT System's behavior should be protected from unauthorized modification and deletion with the protection level as defined in table 7.
- In5. Integrity of information transferred on interfaces between the ECo-AT System components identified in WP2.3 should be protected with a level of protection comparable to that used on the ITS-G5 link.

5.1.3 Availability

The security objectives defined in chapter 6.3 of [ETSI 102 893] should be also satisfied.

The following security objectives related to the availability of ITS services are specified:

- Av1. The operation of ITS services should be protected against disruption caused by malicious or unintended activity within the ITS-S environment with the protection level as defined in table 7.
- Av2. The availability of information provided to other systems out of the boundaries of the ECo-AT System should be protected with the protection level as defined in table 7.

5.1.4 Accountability

The security objectives defined in chapter 6.4 of [ETSI 102 893] should be also satisfied.

The following security objectives related to the accountability of ECo-AT business actors (see chapter 3.3) are specified:

- Ac1. Information generated by the ECo-AT System and transmitted from the ECo-AT System to vehicle ITS-S should be related or relatable to:
 - a. information received from the road operator's Traffic Control Center (TCC);
 - b. information received from single vehicle ITS-S;
 - c. information received from external sensor and/or legacy systems (incl. Traffic Light Controllers or Road works Warning Trailers)with the protection level as defined in table 7.

Rationale: all information sent-out should have a trace back to the source information.

- Ac2. Information generated by the ECo-AT System and transmitted from the ECo-AT System to the TCC should be related or relatable to the information originated by the roadside ITS-S with the protection level as defined in table 7. Rationale: information provided to the TCC should have a trace back to the source information produced by the roadside equipment (e.g. aggregated traffic data)

- Ac3. It should be possible to audit changes to parameters and applications (updates, additions and deletions) with the protection level as defined in table 7.

5.1.5 Authenticity

The security objectives defined in chapter 6.5 of [ETSI 102 893] should be also satisfied.

The following security objectives related to the authenticity of ITS information within the ECo-AT System are specified:

- Au1. The ECo-AT System should prevent unauthorized entities to insert information into the ECo-AT System according to the protection level as defined in table 7. Rationale: serious danger and/or loss of reputation can be caused by incorrect or false information provided by the ECo-AT System
- Au2. The ECo-AT System should prevent entities to replay data from authorized vehicle ITS-S into the ECo-AT System according to the protection level as defined in table 7. Rationale: serious danger and/or loss of reputation can be caused outdated information provided by the ECo-AT System
- Au3. The ECo-AT System should prevent entities to pose as the ECo-AT System and send information to vehicle ITS-S according to the protection level as defined in table 7. Rationale: serious danger and/or loss of reputation can be caused by incorrect or false information provided by the ECo-AT System.
- Au4. Authenticity of information transferred on interfaces between the ECo-AT System components identified in WP2.3 should be protected with a level of protection comparable to that used on the ITS-G5 link.

The ECo-AT System should prevent entities to insert parameters and software that rule the ECo-AT System's behavior according to the protection level as defined in table 7

	ECo-AT High level protection	ECo-AT Medium level protection	No ECo-AT protection
Confidentiality	Probe Data from vehicle ITS-S (not covered by the current specification) Personally Identifiable Information (if collected) (not covered by the current specification)	Aggregated Traffic Information produced by RSE Security Management Software for update, at the discretion of manufacturer	CAM, DENM from vehicle ITS-S Data from Traffic Light Controllers Data from safety trailers

	ECo-AT High level protection	ECo-AT Medium level protection	No ECo-AT protection
	Software for update, at the discretion of manufacturer		
Integrity	<p>CAM, DENM</p> <p>Probe Data from vehicle ITS-S (not covered by the current specification)</p> <p>SPAT/MAP, IVI, DENM/RWW (originated by the ECo-AT System based on TCC information) proposal for signaling on VMS by ECo-AT System to TCC</p>	<p>Aggregated traffic data (originated by the ECo-AT System) provided to TCC</p> <p>Parameters and SW</p>	
Availability	Services that use SPAT/MAP, IVI, DENM/RWW	Parameters and SW	Aggregated traffic data (originated by the ECo-AT System) provided to TCC
Accountability	SPAT/MAP, IVI, DENM/RWW (originated by the ECo-AT System)	<p>Aggregated traffic data (originated by the ECo-AT System) provided to TCC</p> <p>Parameters and SW</p>	

	ECo-AT High level protection	ECo-AT Medium level protection	No ECo-AT protection
Authenticity	<p>CAM, DENM</p> <p>Probe Data from vehicle ITS-S (not covered by the current specification)</p> <p>SPAT/MAP, IVI, DENM/RWW (originated by the ECo-AT System based on TCC information)</p>	<p>Aggregated traffic data (originated by the ECo-AT System) provided to TCC</p> <p>Parameters and SW</p>	

Table 6 Target protection level for information in ECo-AT

5.2 ECo-AT Security Policy

The ECo-AT security architecture only provides information security if the system is operated to ensure information security in accordance with business requirements. This is ensured by setting-up a framework of information security policies and operating according to them.

In general security policy is a definition of what it means to be protected for a system, organization or other entity and how it should be protected (secured). Different levels of security policies exist:

- High-level policy also called strategy, such as the Information Security Management System Policy which gives management direction and support for information security in accordance with business requirements and relevant laws and regulations; defines the strategic intention, the framework for setting objectives in a short and concise way
- Mid-level policies such as company-wide standards for data and threat classes and/or regulations for operational aspects
- Detailed low-level policies or specific procedures focused on a narrower field of security activities such as: classification policy, policy on acceptable use of information assets, backup policy, access control policy. This kind of policy usually describes a selected area of information security in more detail, with precise responsibilities, etc.

Annex A provides a recommendation for the basic content of a high level policy. It does not provide a ready to use security policy for the deployment of the ECo-AT system but a template to build up such a security policy to be released by the top management of the operating company. This template provides a structure and table of content, and core content that may be directly re-used. Text in *italics* indicates areas to be completed by the future owner of the system.

6 ECo-AT Security Requirements Specification – System Level

This chapter specifies which functional and non-functional requirements are necessary to satisfy the established ECo-AT Security Objectives.

6.1 Information Security Management

ECo-AT Security Architecture intends to be integrated in the enterprise security architecture of the different business entities, i.e. road operators, manufactures and ITS-G5 PKI operators. In other words, these business entities should adapt and extend their enterprise security architecture to integrate the specified ECo-AT Security Architecture.

It is recommended that the ECo-AT business entities implement an (if not implemented yet) or adapt their Information Security Management System according the requirements established in the [ISO 27001] so that

the ECo-AT Security Objectives are achieved and the ECo-AT System-wide security requirements are satisfied.

REQ-ISMS-1 ECo-AT business entities should implement and maintain an Information Security Management System that ensures the achievement of the ECo-AT Security Objectives and that satisfy the ECo-AT System-wide security requirements.

REQ-ISMS-2 ECo-AT business entities should document the implementation and maintenance of security measures in their organisations that ensures the achievement of the ECo-AT Security Objectives and that satisfy the ECo-AT System-wide security requirements.

REQ-ISMS-3 ECo-AT business entities should ensure the traceability between security measures (technical, operational or managerial) and the ECo-AT security objectives and requirements.

6.2 ECo-AT System Security functionality

This section describes the security features related to the ECo-AT System:

- protection of ITS applications from the actions of other applications;
- protection of shared and stored information;
- protection of shared processing and storing resources (software and hardware)

As baseline the Open Security Architecture (OSA) security controls have been selected. The controls are structured in categories. As the ECo-AT system needs to integrate in an existing system and operated by an enterprise or organization, not all categories are considered.

Family	Category	ECo-AT scope
CA - Security Assessment and Authorization	Management	No
RA - Risk Assessment	Management	No
SA - System and Services Acquisition	Management	No
AT - Awareness and Training	Operational	No
CM - Configuration Management	Operational	Selected only
CP - Contingency Planning	Operational	Selected only
IR - Incident Response	Operational	No
MA - Maintenance	Operational	No

Family	Category	ECo-AT scope
MP - Media Protection	Operational	Selected only
PE - Physical and Environmental Protection	Operational	No
PL - Planning	Operational	No
PS - Personnel Security	Operational	No
PM - Program Management	Operational	No
AC - Access Control	Technical	yes
AU - Audit and Accountability	Technical	yes
IA - Identification and Authentication	Technical	yes
SC - System and Communications Protection	Technical	yes
SI - System and Information Integrity	Technical	yes

Table 7 OSA controls family classification

6.3 IF4 (ITS-G5) Communication Security

These sections contain requirements describing the security related to the behavior of the ITS-S as a communication endpoint:

- protection and trust towards the external communication peer;
- protection and trust towards the network.

6.3.1 Ensuring Confidentiality and Privacy

Requirements according the countermeasures defined in chapter 11.4.1.3 [ETSI 102 893]

6.3.2 Ensuring Integrity and Authenticity

Requirements according the countermeasures defined in chapter 11.4.1.2 [ETSI 102 893]

6.3.3 Ensuring Availability and Avoiding Denial of Services

Requirements according the countermeasures defined in chapter 11.4.1.1 [ETSI 102 893]

6.3.4 Ensuring Accountability and Avoiding Non-Repudiation

Requirements according the countermeasures defined in chapter 11.4.1.4 [ESTI 102 893]

6.4 IF4 (ITS-G5) Communication Security Management (via IF2)

This section specifies the requirements that the ECo-AT Security Architecture should satisfy to enable the above specified ITS-G5 Communication Security. In other words, it specifies the required functionality that ensures that the necessary information, such as cryptographic objects, credentials, lists of Canonical IDs, etc. required by the ITS Stations to operate in a secure way are in place.

6.4.1 ITS-G5 Communications Domain Model

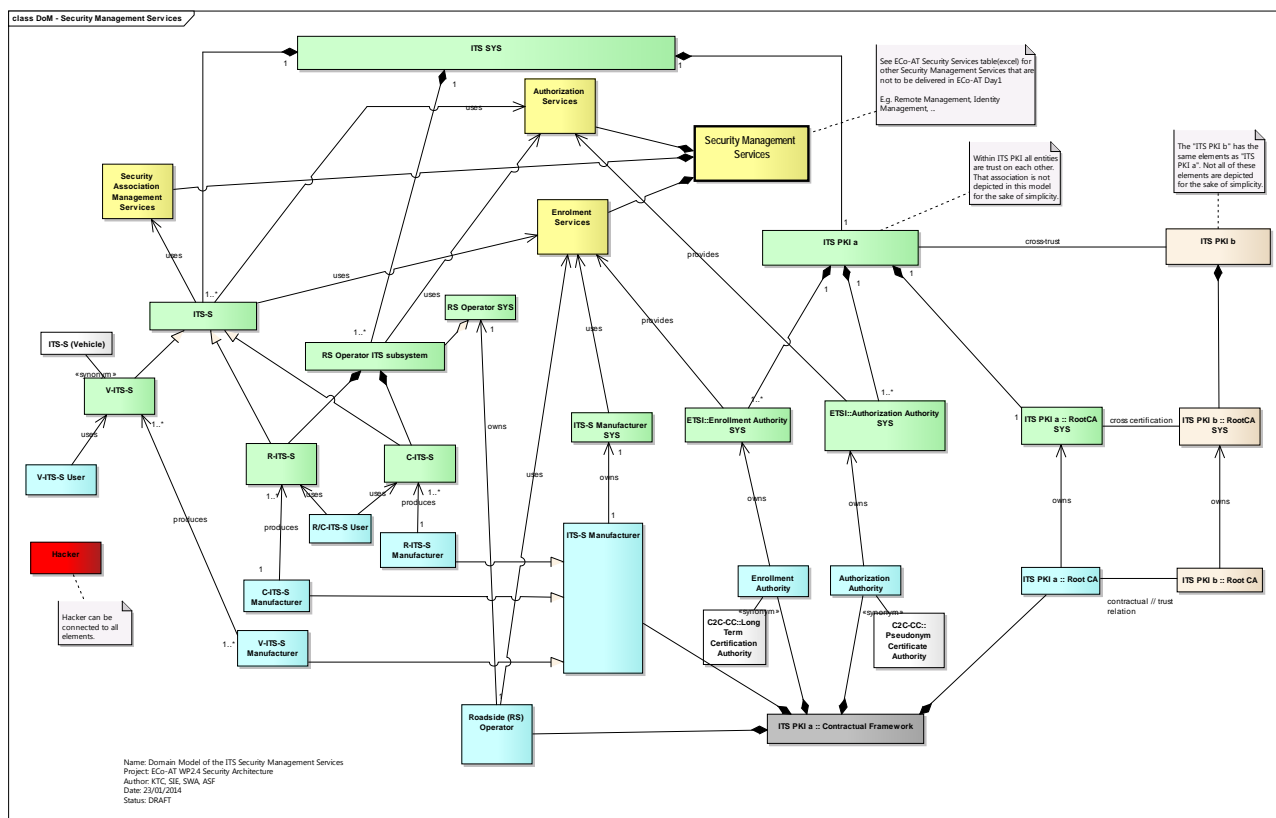


Figure 2 ITS-G5 communications domain model

6.4.2 Bootstrap (Initialization)

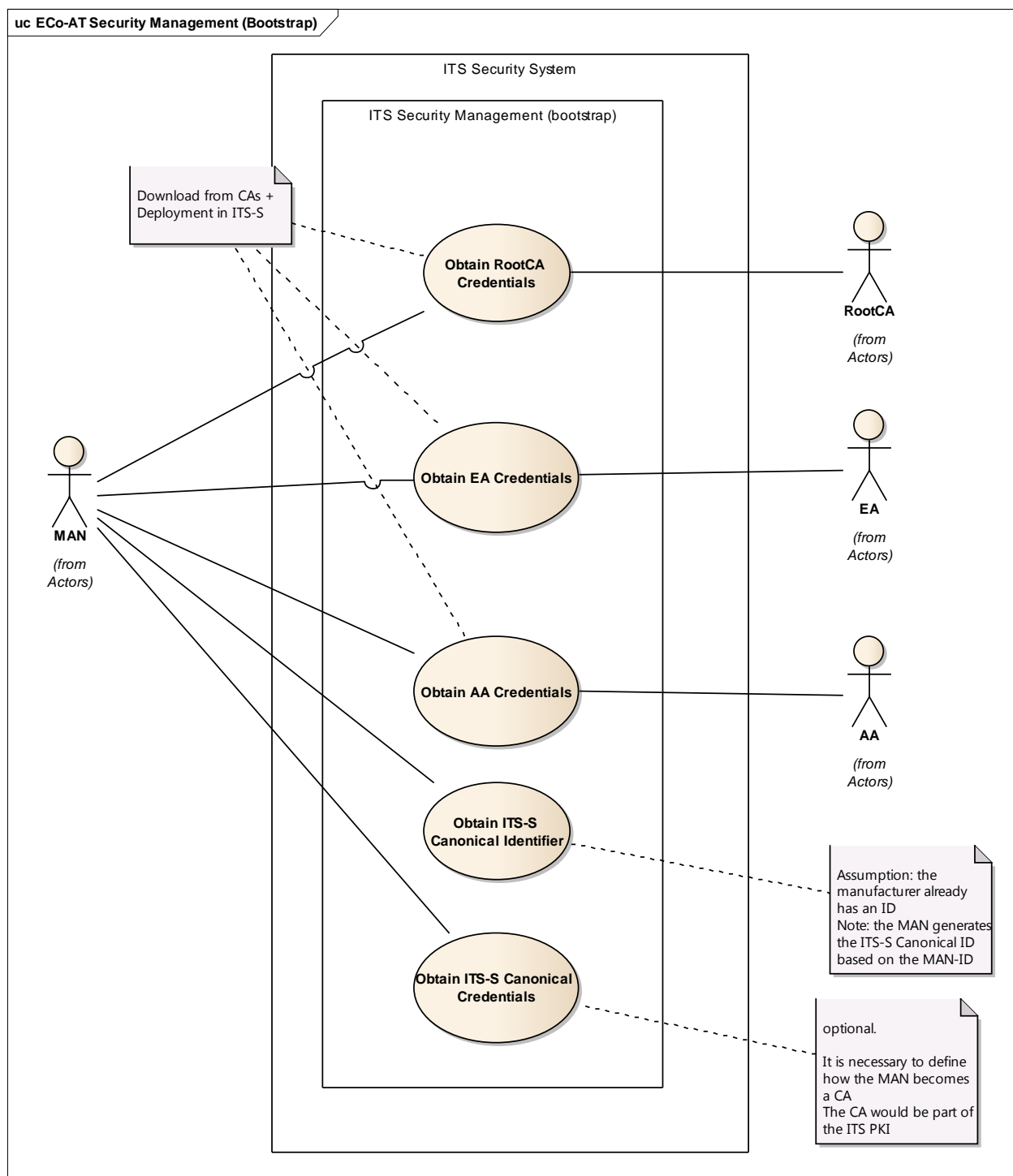


Figure 3 Use case model – ECo-AT Security Management (Bootstrap)

6.4.3 Enrolment of ITS Stations

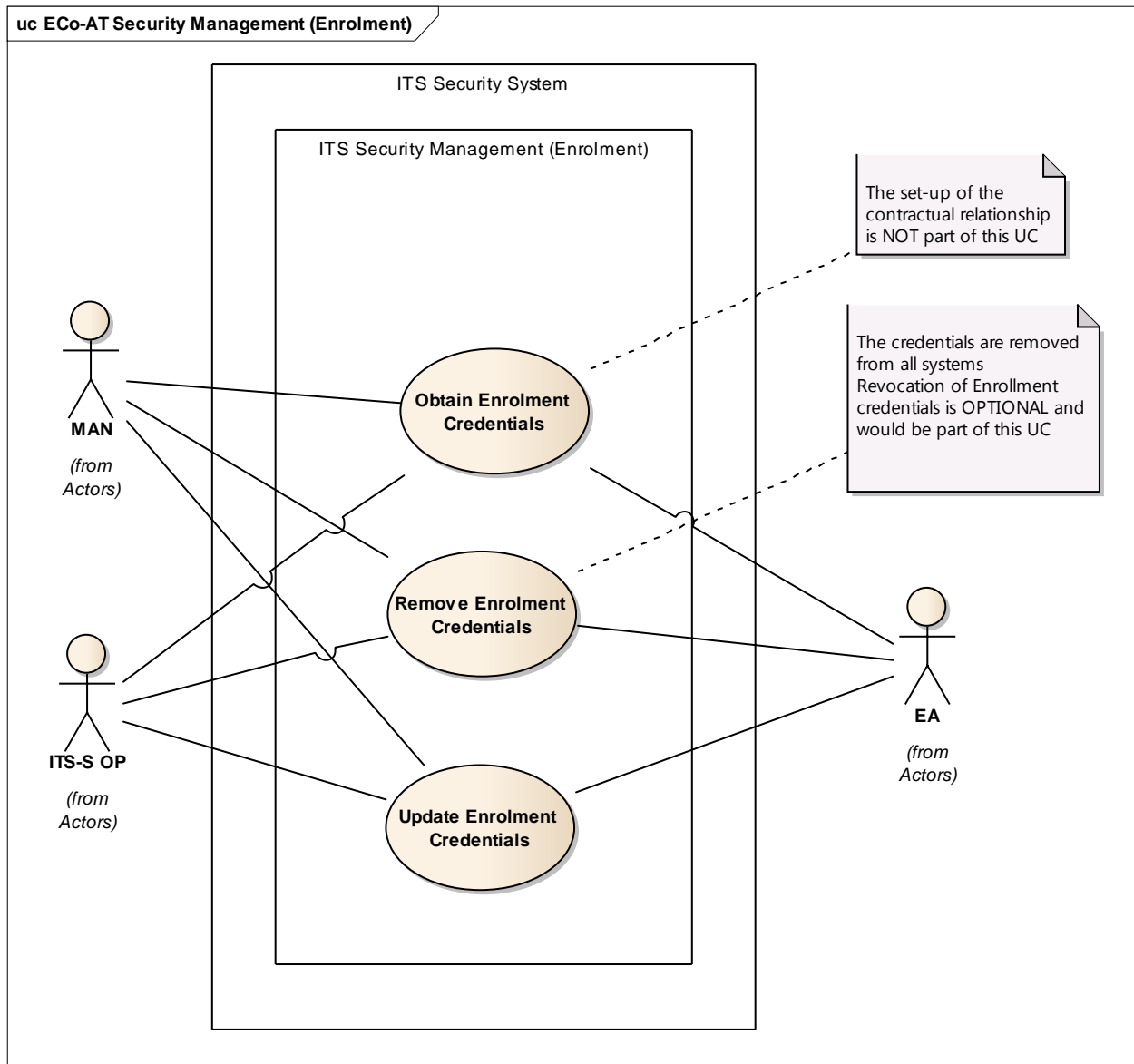


Figure 4 Use case model – ECo-AT Security Management (Enrolment)

6.4.4 Authorization of ITS Stations

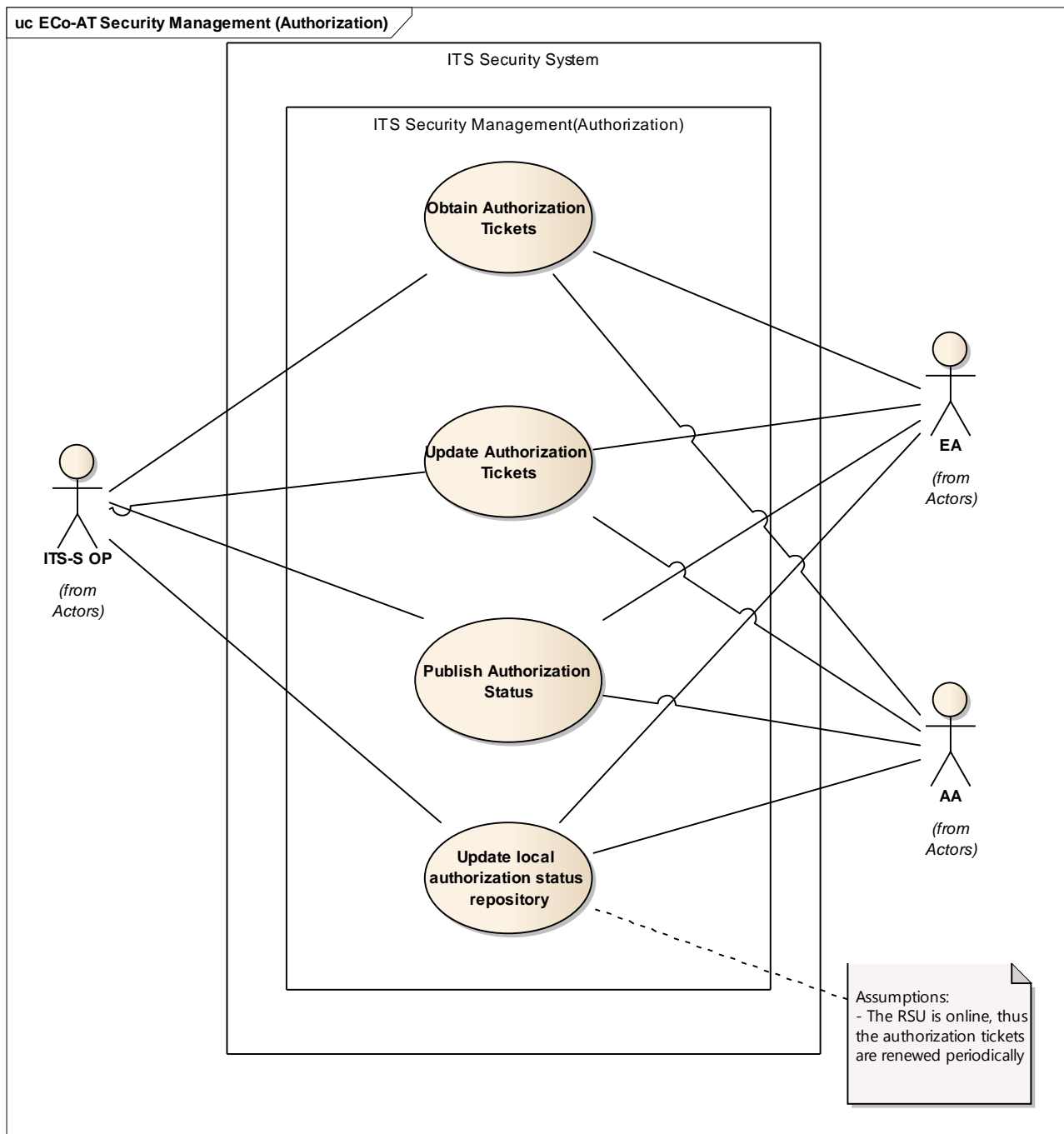


Figure 5 Use case model – ECo-AT Security Management (Authorization)

6.4.5 Security Associations between ITS Stations

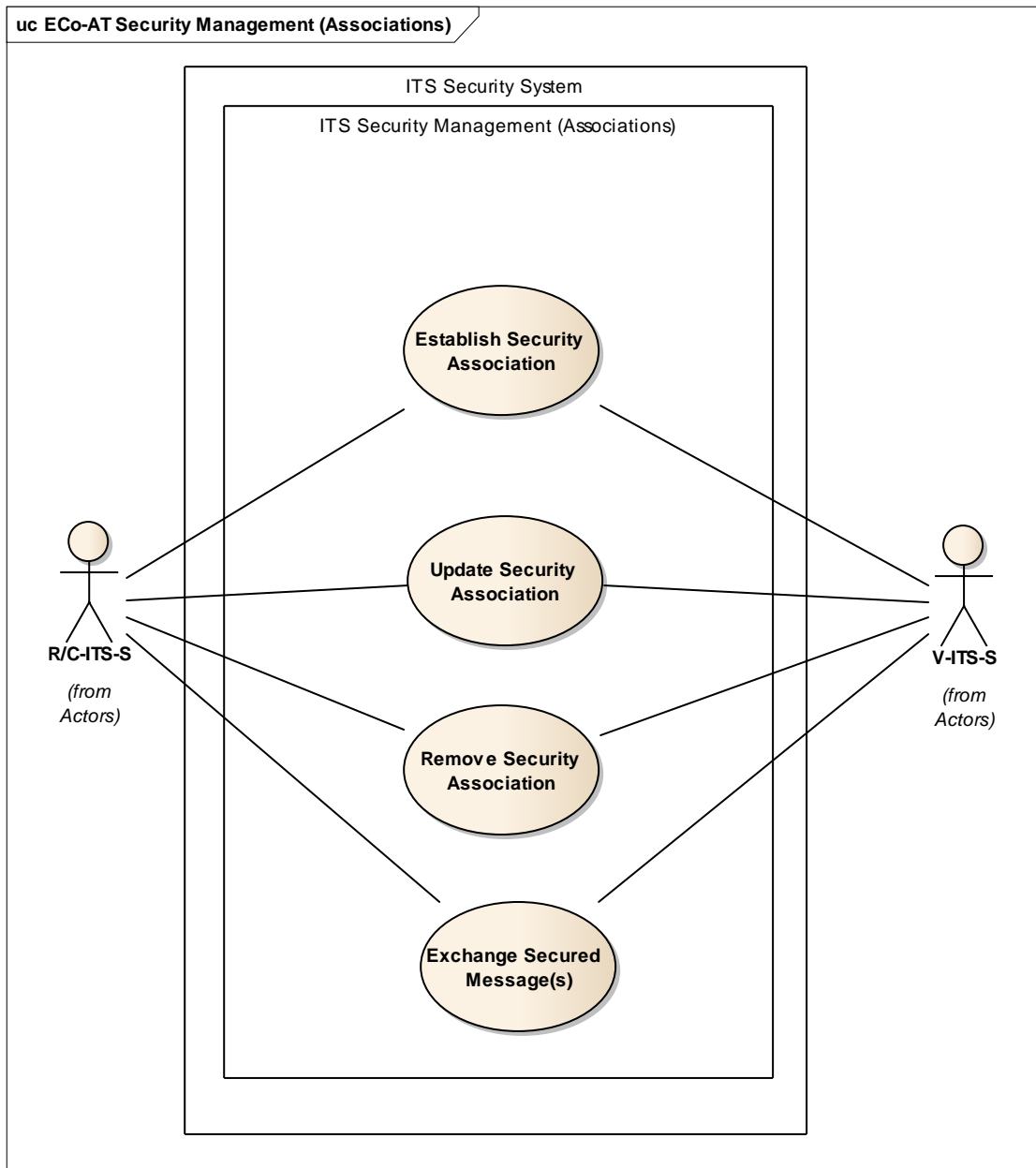


Figure 6 Use case model – ECo-AT Security Management (Associations)

6.5 IF3 (Internal Communication) Security

IF3 identifies both a communication interface (all 7 layers) as well as interfaces between application processes (application interfaces) on R-ITS-S and on C-ITS-S side. With regards to applications running at the Manufacturer, the C-ITS-S is logically acting as a proxy.

Refer to [ECo-AT SWP2.3 system overview] for overview of the interfaces between the identified application processes on R-ITS-S and C-ITS-S side.

6.5.1 IF3 Communication Security Requirements

IF3 shall protect the integrity and confidentiality of communications against attackers outside the system context.

IF3 shall ensure accountability of the C-ITS-S and the R-ITS-S actions with regards to the business use cases and the transferred business information.

For Operational Scenario 2 only, since the manufacturer needs reserved access to the C-ITS-S / R-ITS-S:

- IF3 shall provide access to the Manufacturer to the R-ITS-S it is allowed to manage.
- IF3 shall limit access to application interfaces intended for the Manufacturer only.
- IF3 shall provide accountability for the communications between the Manufacturer / C-ITS-S and the R-ITS-S.

6.5.2 IF3 Security Management

For Operational Scenario 2 only:

- IF3 shall support security management for the needed security objects (where applicable).

6.6 IF1 (TCC to C-ITS-S) Communication Security

We assume and from a security perspective demand that the TCC and the C-ITS-S productive system are located physically very closed in the same data center which is equipped with access control and other security attributes. There will be access control to the systems. If this requirement can be fulfilled by the productive system provider IF1 does not need to be secured.

6.7 IF6 & 7 (R-ITS-S to TLC&Trailer) Communication Security

Due to the legacy nature of those interfaces, no communication security can be provided other than physical protection of the connection.

7 ECo-AT Security Requirements Specification – Component Level

This section describes the security features related to the ECo-AT System components or sub-systems as processing platforms and application hosts against internal and external threats:

- protection of ITS applications from the actions of other applications;
- protection of shared and stored information;
- protection of shared processing and storing resources (software and hardware)

As baseline the Open Security Architecture (OSA) security controls have been selected. The controls are structured in categories. As the ECo-AT system needs to integrate in an existing system and operated by an enterprise or organization, not all categories are considered. ITS-specific controls have been added as needed.

Security controls are defined in a generic way and may provide options. For controls with multiple options, to fulfill one of the choices means to be compliant.

7.1 Central ITS Station Security Functionality

7.1.1 Baseline Controls

ID	Controls Name	Link to OSA Security Control Description
C-ITS-S_AC-03	Access Enforcement	AC-03 Access Enforcement
C-ITS-S_AC-09	Previous Logon Notification	AC-09 Previous Logon Notification
C-ITS-S_AC-10	Concurrent Session Control	AC-10 Concurrent Session Control
C-ITS-S_AC-11	Session Lock	AC-11 Session Lock
C-ITS-S_AC-12	Session Termination	AC-12 Session Termination
C-ITS-S_AU-10	Non-Repudiation	AU-10 Non-Repudiation
C-ITS-S_AU-11	Audit Record Retention	AU-11 Audit Record Retention
C-ITS-S_IA-07	Cryptographic Module Authentication	IA-07 Cryptographic Module Authentication
C-ITS-S_SC-04	Information Remnance	SC-04 Information Remnance

ID	Controls Name	Link to OSA Security Control Description
C-ITS-S_SC-06	Resource Priority	SC-06 Resource Priority
C-ITS-S_SC-11	Trusted Path	SC-11 Trusted Path
C-ITS-S_SC-12	Cryptographic Key Establishment And Management	SC-12 Cryptographic Key Establishment And Management
C-ITS-S_SC-13	Use Of Cryptography	SC-13 Use Of Cryptography
C-ITS-S_SC-17	Public Key Infrastructure Certificates	SC-17 Public Key Infrastructure Certificates
C-ITS-S_SC-24	Fail in Known State	SC-24
C-ITS-S_SC-39	Process Isolation	SC-39
C-ITS-S_SI-06	Security Functionality Verification	SI-06 Security Functionality Verification
C-ITS-S_SI-07	Software And Information Integrity	SI-07 Software And Information Integrity
C-ITS-S_AC-05	Separation Of Duties	AC-05 Separation Of Duties
C-ITS-S_AC-06	Least Privilege	AC-06 Least Privilege
C-ITS-S_AC-07	Unsuccessful Login Attempts	AC-07 Unsuccessful Login Attempts
C-ITS-S_AC-08	System Use Notification	AC-08 System Use Notification
C-ITS-S_AU-02	Auditable Events	AU-02 Auditable Events
C-ITS-S_AU-03	Content Of Audit Records	AU-03 Content Of Audit Records
C-ITS-S_AU-04	Audit Storage Capacity	AU-04 Audit Storage Capacity
C-ITS-S_AU-05	Response To Audit Processing Failures	AU-05 Response To Audit Processing Failures
C-ITS-S_AU-07	Audit Reduction And Report Generation	AU-07 Audit Reduction And Report Generation
C-ITS-S_AU-08	Time Stamps	AU-08 Time Stamps
C-ITS-S_AU-09	Protection Of Audit Information	AU-09 Protection Of Audit Information
C-ITS-S_CM-05	Access Restrictions For Change	CM-05 Access Restrictions For Change

ID	Controls Name	Link to OSA Security Control Description
C-ITS-S_CM-06	Configuration Settings	CM-06 Configuration Settings
C-ITS-S_CM-07	Least Functionality	CM-07 Least Functionality
C-ITS-S_CP-09	Information System Backup	CP-09 Information System Backup
C-ITS-S_CP-10	Information System Recovery And Reconstitution	CP-10 Information System Recovery And Reconstitution
C-ITS-S_IA-02	User Identification And Authentication	IA-02 User Identification And Authentication
C-ITS-S_IA-03	Device Identification And Authentication	IA-03 Device Identification And Authentication
C-ITS-S_IA-04	Identifier Management	IA-04 Identifier Management
C-ITS-S_IA-06	Authenticator Feedback	IA-06 Authenticator Feedback
C-ITS-S_MP-02	Media Access	MP-02 Media Access
C-ITS-S_SC-02	Application Partitioning	SC-02 Application Partitioning
C-ITS-S_SC-08	Transmission Integrity	SC-08 Transmission Integrity
C-ITS-S_SC-09	Transmission Confidentiality	SC-09 Transmission Confidentiality
C-ITS-S_SC-16	Transmission Of Security Parameters	SC-16 Transmission Of Security Parameters
C-ITS-S_SC-23	Session Authenticity	SC-23 Session Authenticity
C-ITS-S_SC-28	Protection Of Information At Rest	SC-28
C-ITS-S_SI-03	Malicious Code Protection	SI-03 Malicious Code Protection
C-ITS-S_SI-04	Information System Monitoring Tools And Techniques	SI-04 Information System Monitoring Tools And Techniques
C-ITS-S_SI-09	Information Input Restrictions	SI-09 Information Input Restrictions
C-ITS-S_SI-10	Information Accuracy, Completeness, Validity, And Authenticity	SI-10 Information Accuracy, Completeness, Validity, And Authenticity
C-ITS-S_SI-11	Error Handling	SI-11 Error Handling
C-ITS-S_SI-12	Information Output Handling And Retention	SI-12 Information Output Handling And Retention

Table 8 OSA controls relevant for C-ITS-S

7.1.2 Specific Controls

IF3 is assumed to physically fulfill the security requirements of 6.5.1 as operated by Asfinag for the fixed R-ITS-S installations.

IF3 is assumed to fulfill the security requirements of 6.5.1 as supplied by a mobile communications provider for the mobile R-ITS-S.

The accountability requirements of the Business Use Case interface of IF3 are fulfilled by the monitoring solution (see [ECo-AT SWP2.3 C-ITS monitoring]). No further security measures are specified here for the ECo-AT system.

For Operational Scenario 2 only:

- The C-ITS-S may manage the access control for the manufacturer application interfaces in a manufacturer specific way.
- In order to fulfil the accountability requirement, the C-ITS-S shall fulfill the following requirements:
 - provide remote access to the manufacturer to the R-ITS-S or C-ITS-S according to maintenance windows defined by the operator,
 - only provide access to the R-ITS-S that the manufacturer must maintain according to contract;
 - provide a method to the manufacturer to subscribe to detailed and/or aggregated status monitoring messages, which can be delivered to the manufacturer directly;
 - log all manufacturer's activities including the communication over IF3. The logs can be viewed by the C-ITS-S operator.

7.2 Roadside ITS Station Security Functionality

7.2.1 Baseline Controls

ID	Controls Name	Link to OSA Control Description
R-ITS-S_AC-03	Access Enforcement	AC-03 Access Enforcement
R-ITS-S_AC-09	Previous Logon Notification	AC-09 Previous Logon Notification
R-ITS-S_AC-10	Concurrent Session Control	AC-10 Concurrent Session Control
R-ITS-S_AC-12	Session Termination	AC-12 Session Termination

ID	Controls Name	Link to OSA Control Description
R-ITS-S_AU-10	Non-Repudiation	AU-10 Non-Repudiation
R-ITS-S_IA-07	Cryptographic Module Authentication	IA-07 Cryptographic Module Authentication
R-ITS-S_SC-03	Security Function Isolation	SC-03 Security Function Isolation
R-ITS-S_SC-04	Information Remnance	SC-04 Information Remnance
R-ITS-S_SC-06	Resource Priority	SC-06 Resource Priority
R-ITS-S_SC-11	Trusted Path	SC-11 Trusted Path
R-ITS-S_SC-12	Cryptographic Key Establishment And Management	SC-12 Cryptographic Key Establishment And Management
R-ITS-S_SC-13	Use Of Cryptography	SC-13 Use Of Cryptography
R-ITS-S_SC-17	Public Key Infrastructure Certificates	SC-17 Public Key Infrastructure Certificates
R-ITS-S_SC-24	Fail Known State	SC-24
R-ITS-S_SC-39	Process Isolation	SC-39
R-ITS-S_SI-06	Security Functionality Verification	SI-06 Security Functionality Verification
R-ITS-S_SI-07	Software And Information Integrity	SI-07 Software And Information Integrity
R-ITS-S_AC-05	Separation Of Duties	AC-05 Separation Of Duties
R-ITS-S_AC-06	Least Privilege	AC-06 Least Privilege
R-ITS-S_AC-07	Unsuccessful Login Attempts	AC-07 Unsuccessful Login Attempts
R-ITS-S_AC-08	System Use Notification	AC-08 System Use Notification
R-ITS-S_AU-02	Auditable Events	AU-02 Auditable Events
R-ITS-S_AU-03	Content Of Audit Records	AU-03 Content Of Audit Records
R-ITS-S_AU-04	Audit Storage Capacity	AU-04 Audit Storage Capacity
R-ITS-S_AU-05	Response To Audit Processing Failures	AU-05 Response To Audit Processing Failures

ID	Controls Name	Link to OSA Control Description
R-ITS-S_AU-08	Time Stamps	AU-08 Time Stamps
R-ITS-S_AU-09	Protection Of Audit Information	AU-09 Protection Of Audit Information
R-ITS-S_CM-05	Access Restrictions For Change	CM-05 Access Restrictions For Change
R-ITS-S_CM-06	Configuration Settings	CM-06 Configuration Settings
R-ITS-S_CM-07	Least Functionality	CM-07 Least Functionality
R-ITS-S_CP-10	Information System Recovery And Reconstitution	CP-10 Information System Recovery And Reconstitution
R-ITS-S_IA-02	User Identification And Authentication	IA-02 User Identification And Authentication
R-ITS-S_IA-04	Identifier Management	IA-04 Identifier Management
R-ITS-S_IA-06	Authenticator Feedback	IA-06 Authenticator Feedback
R-ITS-S_SC-08	Transmission Integrity	SC-08 Transmission Integrity
R-ITS-S_SC-09	Transmission Confidentiality	SC-09 Transmission Confidentiality
R-ITS-S_SC-16	Transmission Of Security Parameters	SC-16 Transmission Of Security Parameters
R-ITS-S_SC-23	Session Authenticity	SC-23 Session Authenticity
R-ITS-S_SC-28	Protection Of Information At Rest	SC-28
R-ITS-S_SI-09	Information Input Restrictions	SI-09 Information Input Restrictions
R-ITS-S_SI-10	Information Accuracy, Completeness, Validity, And Authenticity	SI-10 Information Accuracy, Completeness, Validity, And Authenticity
R-ITS-S_SI-11	Error Handling	SI-11 Error Handling

Table 9 OSA controls relevant for R-ITS-S

7.2.2 Specific Controls

The R-ITS-S shall provide manufacturers a direct and local access to the R-ITS-S for installation and programmed or requested repairs. Direct access by maintenance personnel may be logged manually according to applicable security policies.

For Operational Scenario 2 only:

- The R-ITS-S shall provide manufacturers a direct and local access to the R-ITS-S for maintenance. Direct access by maintenance personnel may be logged manually according to applicable security policies.
- The R-ITS-S may manage the access control for the manufacturer application interfaces in a manufacturer specific way.

7.3 Central ITS Station Security Management Functionality

This section describes functionality necessary to enable and maintain the security features defined in chapter 6.4 and 6.5.

7.3.1 IF3 (Internal Communication) Security Management Functionality

There are no requirements to security management for communication security.

The C-ITS-S may manage the security objects for the manufacturer application interfaces in a manufacturer specific way.

The C-ITS-S operator shall manage the security objects for remote manufacturer's access in a defined way.

7.3.2 IF4 (ITS-G5) Security Management Functionality support

Important Note: The interface to the PKI will be left open. A decision needs to be taken which security concept will be chosen by the operator and if the concept is chosen, a PKI provider needs to be selected. At the moment there are quite fundamental discussions in the EC about the infrastructure security concepts. As soon as there is an agreement and clarity about the future concept, an interface of a PKI provider with an appropriate security policy can be referenced.

7.4 Roadside ITS Station Security Management Functionality

This section describes functionality necessary to enable and maintain the security features defined in chapter 6.4 and 6.5.

7.4.1 IF3 (Internal Communication) Security Management Functionality

There are no requirements to security management for communication security. The R-ITS-S may manage the security objects for the manufacturer application interfaces in a manufacturer specific way.

7.4.2 IF4 (ITS-G5) Security Management Functionality

Important Note: The interface to the PKI will be left open. A decision needs to be taken which security concept will be chosen by the operator and if the concept is chosen, a PKI provider needs to be selected. At the moment there are quite fundamental discussions in the EC about the infrastructure security concepts. As soon as there is an agreement and clarity about the future concept, an interface of a PKI provider with an appropriate security policy can be referenced.

8 ECo-AT Security Design - Logical ITS Security Architecture

This chapter describes the whole technical architecture that satisfies the requirements from the previous chapter 6, thus, it is the design of the ECo-AT ITS security system. The technical architecture has a logical view, that shows the functional entities and their communication points, and a physical view, that illustrates the software and hardware components and how they are interconnected distributed over the different physical locations. This chapter presents the logical view.

SYSTEM CONTEXT: SYSTEM and ENVIRONMENT (Logical View) - During Operations

Eco-AT SYSTEM ENVIRONMENT

Eco-AT System

TCC

Roadside Operator SYSTEM
(e.g. ASFINAG)

C-ITS-S

ITS functionality
ITS Security Services
ITS Security Management Services

R-ITS-S

ITS functionality
ITS Security Services
ITS Security Management Services

V-ITS-S

PVD
ITS functionality
ITS Security Services
ITS Security Management Services

TLC (5)

ITS functionality

RWW Trailer

ITS functionality

ITS PKI

RootCA System

ITS Security Management Services
PKI Management Services

EA System

ITS Security Management Services
PKI Management Services

AA System

ITS Security Management Services
PKI Management Services

ITS Security Management SYSTEM

Note A: the services can be provided/implemented via IT-services (software) and/or via operational processes

Note B: This diagram shows only the logical blocks of the system architecture that provide any functionality. It should be seen together with a physical view (TBD)

Title:
Area/Section/Topic:
Project:
Workpackage:
Date:
Status:
Author:

System Context Diagram – Logical view for operations phase
Security System Architecture
Eco-AT
WP2.4 Security Architecture
11-02-2015
V2.0
Eco-AT SWP2.4 group

Note (4): These interfaces are defined by C2C-CC PKI Specification. It is necessary that the specification of the C2C-CC is available to ECo-AT project members.

Note (5): the traffic light controller (TLC) is located in the same physical location as the R-ITS-S, i.e. a closed cabinet. It is assumed that the R-ITS-S can trust the TLC. No signing of messages is foreseen.

8.1.1 ITS Functionality

ITS functionality is the SW functionality that realizes/implements the ECo-AT (Cooperative ITS) business use cases.

The combination of all the instances of ITS Functionality is the **ITS Functional System**.

For more information refer to SWP 2.3 documentation.

8.1.2 ITS Security Services

ITS Security Services are those IT services or SW functionality that provide the security functionality, such as encryption of transmitted data, encryption of stored data, digitally signature of data, accounting of actions, access control to specific functionality, access control to specific data, implementation of a specific role concept (authentication + authorization), etc. The ITS functionality uses and relies on the ITS Security Services in order to achieve the security objectives. The ITS Security Services realize the security measures at SW layer required to achieve the ECo-AT security objectives, as specified in chapter 7.

The ITS Security Services are just protecting the C-ITS functionality. The operating system or other applications running on the same hardware are not protected by the ITS Security Services.

The ITS Security Services do not directly communicate with each other, but via the ITS functionality. They run on ITS Stations (C-ITS-S, R-ITS-S and V-ITS-S).

The combination of all the instances of ITS Security Services is the ECo-AT **ITS Security System**.

As the most important interface is the ITS-G5 link, which connects the vehicles and the infrastructure the main focus in the service catalogue is placed on the provided ITS-G5 security services.

8.1.3 ITS Security Management Services

ITS Security Management Services (ITS SecMS) are those IT services, SW functionality or non-SW processes that ensures that the ITS Security Services work properly. This means that the necessary information (such as cryptographic objects, credentials, lists of Canonical IDs, etc.) required by the entities and the ITS Security Services are in place.

The ITS SecMS run on or are provided by the following ECo-AT sub-systems/components: C-ITS-S, R-ITS-S, RootCA¹ System, Enrollment Authority System and Authorization Authority System. The V-ITS-S also provides these services. The instances of these ITS SecMS are logically connected in the following ways:

- The ITS SecMS at C-ITS-S with those at R-ITS-S, EA System, AA System and RootCA System
- The ITS SecMS at R-ITS-S with those at C-ITS-S and V-ITS-S.
Note: to be defined if direct connection from R-ITS-S to EA System, AA System are allowed/needed.
- The ITS SecMS at EA-ITS-S with those at C-ITS-S, AA System, RootCA System and the PKI Management Services
- The ITS SecMS at AA-ITS-S with those at C-ITS-S, EA System, RootCA System and the PKI Management Services
- The ITS SecMS at RootCA System with those at C-ITS-S, AA System, EA-ITS-S and the PKI Management Services.

The combination of all the instances of ITS SecMS is the **ITS Security Management System**.

Some examples of the functionality provided by the ITS SecMS at different locations:

- Generation of Certificate Signing Requests (CSR) at the ITS-S
- Processing of CSR at the Certificate Authorities -CA - (RootCA, EA and/or AA)
- Exchanging ITS-S lists between the entities (via e.g. email)
- Issuing of CA Certificates at the RootCA System
- Issuing of Enrolment Credentials at the EA System
- Issuing of Authorization Credentials at the AA System
- Distribution of Certificates from the CA (EA and/or AA) to the C-ITS-S
- Distribution of Certificates from the C-ITS-S to the R-ITS-S
- Establishment of Security Associations
- Distribution/Update of access control policies (role concept)
- Distribution/Update of accounting/logging policies

Note: Certificates is the common term for Enrolment Credentials and Authorization Credentials

Note: for a complete list of the provided ITS SecMS, refer to the chapter 8.4.

8.1.4 PKI Management Services

The PKI Management Services consist of SW/HW functionality and operational processes provided and performed by any of the subsystem of a PKI. These services and processes are common PKI services and not specific to C-ITS. Examples are:

- Maintenance of an Incident Management System

¹ The RootCA might not need to have the ITS Security Management Services.

- Maintenance of a Business Continuity Strategy
- Implementation of security controls for Personal Identifiable Information (Privacy)
- Maintenance of the security controls for protecting the cryptographic material
- Performance of Security Audits
- Publication of CA CRLs
- Publication of the CA certificates
- Any other activities contained in a Certificate Policy that is not C-ITS specific

The combination of all the instances of PKI Management Services is the **ITS PKI Management System**.

8.1.5 ITS-G5 Public Key Infrastructure

The ITS-G5 PKI consists of the following systems: Enrollment Authority System, ITS-G5 RootCA System and Authorization Authority System. They are Certification Authorities (CAs) with different purposes. Each of these CAs has an instance of ITS Management Services and an instance of PKI Management Services.

8.1.6 Traffic Control Center (TCC)

The TCC has a logical connection with the ITS Functionality and the ITS SecMS. For more information refer to SWP 2.3 documentation.

8.1.7 Roadside Operator System

This system is made of at least one instance of C-ITS-S, at least one instance of R-ITS-S and the TCC.

8.1.8 Traffic Light Controller (TLC)

Traffic signals are controlled by a traffic light controller. A traffic controller interfaces detectors on the road. A controller is mounted inside a cabinet and mounted on a concrete pad. The Traffic Light Controller predicts the future phases of the signals. The information of the prediction of the phases is forwarded to the R-ITS-S.

8.1.9 RWW trailer

RWW trailers need to reliably warn all road user about ongoing road works. They are mainly used on motorways. They are equipped with variable message signs. The mobile ITS-G5 R-ITS-S interfaces the information about the configured message sign via a propriety interface. The mobile R-ITS-S communicates via cellular interface with the C-ITS-S.

8.1.10 PVD

The "PVD" element represents both the PVD functionality and the PVD message type. This is currently out-of-scope of ECo_AT

8.2.1 Manufacturer System

The Manufacturer System has an instance of ITS SecMS that are logically connected with the instances of ITS SecMS at C-ITS-S and at R-ITS-S and with those at the CAs of the ITS PKI.

8.3 IF4 (ITS-G5) Communication Security Services Catalogue

Service Category	Security service	Relevant for ECo-AT
Single message services	Authorize Single Message	yes - prio 1
	Validate Authorization on Single Message	yes - prio 1
	Encrypt Single Message	out of scope in day-1
	Decrypt Single Message	out of scope in day-1
Integrity services	Calculate Check Value	yes
	Validate Check Value	out of scope
	Insert Check Value	out of scope
Replay Protection services	Replay Protection Based on Timestamp	yes - prio 1
	Replay Protection Based on Sequence Number	out of scope in day-1
Accountability services	Record Incoming Message in Audit Log	yes - only for debug
	Record outgoing message in Audit Log	yes - only for debug
Plausibility validation	Validate Data Plausibility	out of scope

Table 10: G5 Communication Security Service Catalogue

8.4 IF4 (ITS-G5) Security Management Services Catalogue

Service category	Security service	Relevant for ECo-AT
Bootstrap	Obtain Root Credentials	yes - prio 1
	Obtain CAs' Credentials	yes - prio 1
	Obtain ITS-S Canonical Identifier	yes - prio 1
	Obtain ITS-S Canonical Credentials	out of scope in day-1
Remote management	Remote Activate Transmission	out of scope in day-1

Service category	Security service	Relevant for ECo-AT
	Deactivate ITS transmission	out of scope in day-1
Report Misbehaving ITS-S	Report misbehavior	out of scope in day-1
Enrolment (C2CC long Term)	Obtain Enrolment Credentials	yes - prio 1
	Update Enrolment Credentials	yes - prio 1
	Remove Enrolment Credentials	yes - prio 1
Authorization (C2CC Pseudonym)	Obtain Authorization Tickets	yes - prio 1
	Update Authorization Tickets	yes - prio 1
	Publish Authorization Status	out of scope in day-1
	Update Local Authorization Status Repository	out of scope in day-1
Security Association Management	Establish Security Association	yes - prio 1
	Update security association	yes - prio 1
	Remove security association (check if necessary)	not needed
	Send Secured Message (signed and encrypted)	out of scope in day-1
	Receive Secured Message (signed and encrypted)	out of scope in day-1
ITS-S Crypto Services	Generation of Key Pair	yes - prio 1
	Generation of Certificate Signing Request	yes - prio 1

Table 11: G5 Security Management Service Catalogue

8.5 IF4 (ITS-G5) PKI Management Services Catalogue

Service category	Security service	Relevant for ECo-AT
Manage PKI	Manufacture joins PKI (opt)	out of scope in day-1
	Joining of Authorities (EA/AA) to PKI	yes - prio 1
	Cross-certification of root CAs	out of scope in day-1
	Revocation of CAs	yes - prio 1
	Renew of CAs' credentials	

Table 12: G5 PKI Management Services Catalogue

9 ECo-AT Security Design - Physical ITS Security Architecture

This represents the security management part of the ECo-AT Security architecture at technical/physical level: i.e. the specification of security-related data objects and their processing by security applications instantiated in dedicated hardware and software.

9.1 IF4 (ITS-G5) Security

9.1.1 Communication Security Specification

IF4 transmitter-side communication security is according to [ETSI 103 097] and with additional specifications in:

- [ETSI 103 301] for SPAT/MAP, IVI and DENM (I2V);
- [ETSI 302 637-2] for CAM (V2I);
- [ETSI 302 637-3] for DENM (V2I).

Note: receiver-side behavior shall be defined in the applicable security policy.

9.1.2 Security Management Specification

The PKI for the ITS-G5 communication is needed to grant reliable verification of road users using G5 communication, for instance vehicles, roadside units, pedestrians.

At the moment no productive ITS-G5 PKI is available. The C2C-CC deployed a Demo PKI for tests but we expect in the near future with the distribution of ITS-G5 communication systems and the final release of standards multiple providers for certificate authorities will be available. At the moment there is no stable standard published for an interface like IF4 (to a certificate authority for ITS-G5 certificates). Which means every provider is free to offer its own interface which can differ to that one proposed by the C2C-CC Demo PKI.

IF2 Definition: Make a reference to C2C-CC Documents and/or [ETSI 102 941].

9.2 IF3 (Internal Communication) Security

9.2.1 Communication Security Specification

No measures for communication security are specified.

For Operational Scenario 2:

- Access control specifications for the manufacturer application interfaces are manufacturer specific and not defined here.

9.2.2 Security Management Specification

For Operational Scenario 2:

- The management of the security objects that regulate the manufacturer's access shall be defined by the C-ITS-S operator according to common practices.
- Security management specifications for the manufacturer application interfaces are manufacturer specific and not defined here.

9.3 ITS Station security

<p>Important Note: The decision is dependent on chapter 3.5 which is an open issue. The decision is dependent on the policy of the infrastructure security policy..</p>
--

Annex A - High level information security Policy (Strategy)

Introduction

In this document the corporate management expresses its commitment and set out the high level rules for information security and information security risk management.

This document should be aligned with the security policies of the corporate group to which the operating company belongs.

Scope

The area of validity of this information security policy includes all core areas of the *operating company*.

Core areas needs to be defined by the operating company but should include the main business processes

The area of validity of this information security policy is determined by a clear demarcation of the technical interface with other technical systems.

The area of validity of this information security policy is determined by a clear demarcation and definition of the intersections with adjoining service units by means of service level agreements (SLAs).

The area of validity of this information security policy is determined by a clear demarcation and definition of the intersections with external companies providing IT services by means of underpinning contracts

Audience

The audience of this policy is the top-management of the *operating company*. It provides a tool to manage information security from a high level perspective.

Referenced documents

References to laws, regulations

References to other documents of the security policy framework, such as an information security handbook containing detailed policies.

Policy Directives

Mission

The mission of the operating company is to set up a holistic approach to manage information security in order to select adequate and proportionate security controls that protect assets and give confidence to interested parties about the business processes.

The targets of information security in the operating company are:

- Compliance with all laws and regulations
- Correctness, completeness, authenticity, confidentiality and availability of information
- Maintaining trust of user of the provided services

Goals

In the context the services provided by the *operating company*, which are additional best effort traffic information services that do not substitute the legal signage on the road, the high level goals are to guarantee:

- Confidentiality: ensuring that the business information is accessible only to those authorized to access it.
- Integrity: ensuring that the information is accurate in accordance with the traffic situation and complete and that the information is not modified without authorization.
- Availability: ensuring that the information is accessible to authorized users when required.

Additional goals are:

- Privacy, i.e. confidentiality of personal data, as far as such is collected
- Authenticity of users and generated information
- Accountability of actions and events that happen within the information system

Strategy

The information security strategies of the *operating company* are:

- to protect and manage information based on a systematic business risk management approach
- to establish, implement, operate, monitor, review, maintain, and improve information security management (*optional – according [ISO 27001] approach*),
- to establish and improve an information risk management system, where risks from the use of information systems are assessed in a traceable manner (*optional – according [ISO 27005] approach*),
- to establish guidelines, regulations and procedures to support this policy,
- to train all personal on information security and to create awareness of the,
- to formalize responsibilities in roles and allocate them correctly to employees,

- to maintain compliance with the applicable international regulations and standards,
- to maintain a performance indicator system for the measurement of information security.

Complete as applicable to the operating company

Context and Security Architecture

Information security for cooperative ITS is not a stand-alone aspect but is based on the interaction with service provider roles technically implemented in ITS Stations, and is based on the ETSI communication security architecture.

The *operating company* provides its services within this context but with a clear demarcation of its responsibility in technical terms. Its architecture defines on logical level which is the functions and data provided by the company.

The *operating company* receives its security objects² from a Public Key Infrastructure and relies on its operation.

The technical system has been therefore designed based on those constraints and considering best practices in information security. This is the basis for the continuous evolution of information security in the *operating company*.

Roles and Responsibilities

The general management is accountable for information security but can delegate the responsibility for the implementation of information security and risk management to an information security Manager / Officer.

Roles and responsibilities shall be clearly assigned to employees so that they are accountable for their duties.

Information and / or process owners are responsible for information used in their business processes. They are responsible for the determination of protection goals.

Users are responsible for a suitable safe usage of IT systems as well as using the necessary security rules.

Consequences of violations

Cases of a failure to comply with agreements, standards and laws relating to information security which are in place across the operating company shall be deemed substantial violations of employment duties.

² Security object is used in this document as an umbrella term that covers all kinds of digital certificates used in cooperative ITS, i.e. among others, for enrolment and for authorization

A reporting and sanctioning system shall be set up.

Annex B - Security Attributes and Impact classes

The categorization of the information should be done following the criteria in the table below:

Security attribute	IMPACT		
	Low	Medium	High
<p>Confidentiality</p> <p>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.</p>	<p>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</p>
<p>Integrity</p> <p>Guarding against improper information modification or destruction</p>	<p>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>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.</p>
<p>Availability</p> <p>Ensuring timely and reliable access to and use of information.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a limited adverse</p>	<p>The disruption of access to or use of information or an information system could be expected to have a serious</p>	<p>The disruption of access to or use of information or an information system could be expected to have a severe or</p>

Security attribute	IMPACT		
	Low	Medium	High
	effect on organizational operations, organizational assets, or individuals.	adverse effect on organizational operations, organizational assets, or individuals.	catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Authenticity Ensuring that the information has not been modified and enabling that it can be verified that the information is genuine (authentic)	The lack of means to prove the authenticity of the information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The lack of means to prove the authenticity of the information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The lack of means to prove the authenticity of the information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Accountability			

Table 13 Security attributes and impact classes

Annex C : Threat Analysis

Methodology

According to [ETSI 102 893] chapter 4, the TVRA method involves the following steps.

- 1) Identify security objectives.
- 2) Identify security requirements.
- 3) Produce an inventory of system assets.
- 4) Classify system vulnerabilities and threats.
- 5) Quantify the likelihood and impact of attack.
- 6) Determine the risks involved.
- 7) Specify detailed security requirements (security controls)

Security objectives and protection level

See Chapter5, Section 1 in [ECo-AT SWP3.4 security]

Security requirements

See Chapter 6, 7 in [ECo-AT SWP3.4 security]

Assets to be protected

See Chapter 4 in [ECo-AT SWP3.4 security]

Target of evaluation

Refer to Figure 1 in [ECo-AT SWP3.4 security]

R-ITS-S and C-ITS-S as part of the ECo-AT system, and their interface: IF3

Note: IF4 was analyzed by ETSI TVRA [ETSI 102 893] and therefore does not represent a scope for this document;

Note: out of scope are following: IF 6 & 7 see chapter 6.7, IF1 see chapter 6.6, IF2 – not specified until yet, IF5 not specified in WP3

Thread, vulnerability and risk analysis

The increasing professionalization of attackers and attack methods furthermore causes a dynamic threat scenario and a permanent competition between cyber attacks and cyber defense. Therefore, within Eco-AT it has been chosen to adopt as a reference for the TVRA the IT-Grundschutz Elementary Threats Catalogue, due to its frequent updates and adaptations to the latest state of the art. The above reference is suggested also by OSA.

The TVRA has been carried for the Eco-AT system, considering its components (C-ITS-S and for the R-ITS-S.) and their interfaces.

For every analyzed threat there have been indicated:

- ID according to the IT Grundschutz Catalogue
- Threat name
- Relevant security attributes in relation to the respective threat and following annotations have been performed: Confidentiality (C), Integrity (including Authenticity plus Accountability) (I) and Availability (A)
- One or more examples as threat description in relation to the ECo-AT system
- The threat interface
- Frequency class representing the probability for the event to occur. Three levels of frequency values have been defined for each threat: low (L), medium (M) and high (H).
- Impact class – three levels of values have been defined in relation with the impact, in consistence with the descriptions in Annex B: low (L), medium (M) and high (H)
- Risk class derived from the combination of the Frequency Class and Impact class values, as shown in the table below. Five values have been defined for the Risk class: very low (VL), low (L), medium (M), high (H), very high (VH)

The figure below briefly describes the methodology adopted for the Risk class determination following the classical approach where the Risk represents a product derived from frequency/probability and impact/magnitude. The matrix contains all possible combinations of Impact class and Frequency class (as described in the paragraph above) indicating for each combination the resulting Risk class to be considered.

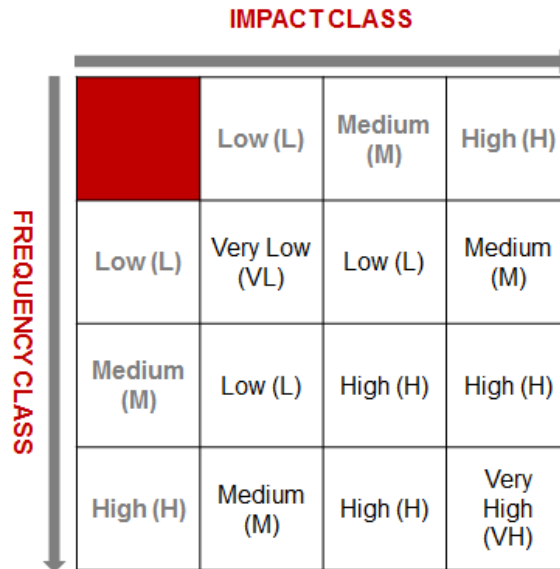


Figure 9 ECo-AT Risk Assessment Matrix

C-ITS-S

ID	Threat	Related ITS-S Security Params.	Examples of caused system weaknesses	Threat IFs	Freq. class	Impact class	Risk class	OSA Controls to be applied in order to reduce risk
T 0.14	Interception of Information / Espionage	C,I,A	Interception of CAM messages	IF3	H	M	H	C-ITS-S_IA-07 C-ITS-S_SC-11 C-ITS-S_SC-12 C-ITS-S_SC-13 C-ITS-S_IA-02 C-ITS-S_IA-03 C-ITS-S_SI-03 C-ITS-S_SC-16 C-ITS-S_SC-23
T 0.15	Eavesdropping	C,I,A	Interception of CAM messages	IF3	H	M	H	C-ITS-S_IA-07 C-ITS-S_SC-11 C-ITS-S_SC-12 C-ITS-S_SC-13 C-ITS-S_IA-02 C-ITS-S_IA-03

								C-ITS-S_SI-03
T 0.20	Information or Products from an Unreliable Source.	C,I,A	Delivery of unreliable IVS data; Receiving fake DENMs from the vehicles	IF3	L	H	M	C-ITS-S_IA-07 C-ITS-S_SC-17 C-ITS-S_IA-02 C-ITS-S_IA-03 C-ITS-S_IA-04
T 0.21	Manipulation of Hardware or Software	C,I,A	Malicious software installation	C-ITS-S	L	H	M	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-03
T 0.22	Manipulation of Information	I	Transmission of erroneous IVI messages	IF3	L	H	M	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09

								C-ITS-S_CM-05 C-ITS-S_SI-09 C-ITS-S_SI-10
T 0.23	Unauthorised Access to IT Systems	C,I	Unauthoriz ed access to the system	C-ITS- S	L	H	M	C-ITS-S_AC-03 C-ITS-S_AC-09 C-ITS-S_AC-07 C-ITS-S_AC-08 C-ITS-S_CM-05 C-ITS-S_CM-06 C-ITS-S_IA-02 C-ITS-S_IA-03 C-ITS-S_IA-04 C-ITS-S_IA-06
T 0.25	Failure of Devices or Systems	A	Failure of devices in an unknown state that produce the blocking of the service	C-ITS- S	M	M	H	C-ITS-S_SC-06 C-ITS-S_SC-24 C-ITS-S_SC-39 C-ITS-S_CM-07 C-ITS-S_CP-09 C-ITS-S_CP-10 C-ITS-S_SI-04 C-ITS-S_SI-11 C-ITS-S_SI-12 C-ITS-S_SC-06
T 0.26	Malfunction of Devices or Systems	I,A	Unavailabil ity of the service	C-ITS- S	M	M	H	C-ITS-S_SC-06 C-ITS-S_SC-24 C-ITS-S_SC-39 C-ITS-S_CM-07 C-ITS-S_CP-09 C-ITS-S_CP-10 C-ITS-S_SI-04 C-ITS-S_SI-11 C-ITS-S_SI-12 C-ITS-S_SC-06
T 0.27	Lack of Resources	A	Overflow of storage capacity	C-ITS- S	L	M	L	C-ITS-S_AU-04 C-ITS-S_CM-06 C-ITS-S_CM-07 C-ITS-S_SC-02 C-ITS-S_SC-06
T	Software	C,I,A	Wrong	C-ITS-	L	M	L	C-ITS-S_AU-04

0.28	Vulnerabilities or Errors		process prioritization	S				C-ITS-S_CM-06 C-ITS-S_CM-07 C-ITS-S_SC-02 C-ITS-S_SC-06 C-ITS-S_SI-11
T 0.30	Unauthorised Use or Administration of Devices and Systems	C,I,A	System accessed by unauthorized personnel	IF3	L	H	M	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-03
T 0.31	Incorrect Use or Administration of Devices and Systems	C,I,A	Human error in system management	IF3	L	M	L	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-03
T 0.36	Identity Theft	C,I,A	IP Spoofing of the C-ITS-S	C-ITS-S	L	H	M	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10

								C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-09 C-ITS-S_SI-10
T 0.39	Malicious Software	C,I,A	Virus on C-ITS-S	C-ITS-S	M	M	H	C-ITS-S_SI-03
T 0.40	Denial of Service	A	No IVS messages being delivered	IF3	M	H	H	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03 C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-03
T 0.43	Replaying Messages	I	Old update of red/green transition being replayed	IF3	M	H	H	C-ITS-S_AC-10 C-ITS-S_AC-11 C-ITS-S_AC-12 C-ITS-S_AU-10 C-ITS-S_AU-11 C-ITS-S_AC-05 C-ITS-S_AC-06 C-ITS-S_AU-02 C-ITS-S_AU-03

								C-ITS-S_AU-04 C-ITS-S_AU-05 C-ITS-S_AU-07 C-ITS-S_AU-08 C-ITS-S_AU-09 C-ITS-S_CM-05 C-ITS-S_SI-03
T 0.45	Data Loss	A	Loss of DENM messages due to deletion or malfunctioning	C-ITS-S	L	L	VL	Inconsiderable

R-ITS-S

ID	Threat	Related ITS-S Security Params.	Examples of caused system weaknesses	Threat IFs	Freq. class	Impact class	Risk class	OSA Controls to be applied in order to reduce risk
T 0.14	Interception of Information / Espionage	C,I,A	Interception of CAM messages	IF3	H	M	H	R-ITS-S_IA-07 R-ITS-S_SC-11 R-ITS-S_SC-12 R-ITS-S_SC-13 R-ITS-S_IA-02 R-ITS-S_IA-04 R-ITS-S_SC-16 R-ITS-S_SC-23
T 0.15	Eavesdropping	C,I,A	Interception of CAM messages	IF3	H	M	H	R-ITS-S_IA-07 R-ITS-S_SC-11 R-ITS-S_SC-12 R-ITS-S_SC-13 R-ITS-S_IA-02 R-ITS-S_IA-04
T 0.19	Disclosure of Sensitive Information	C	Vehicle identification shared; Bad password	IF3	L	M	L	R-ITS-S_AC-03 R-ITS-S_SC-04 R-ITS-S_AC-06

			manageme nt by the system operators					
T 0.20	Information or Products from an Unreliable Source.	C,I,A	Delivery of unreliable IVS data; Receiving fake DENMs from the vehicles	IF3	L	H	M	R-ITS-S_IA-07 R-ITS-S_SC-17 R-ITS-S_IA-02 R-ITS-S_IA-04 R-ITS-S_IA-06
T 0.21	Manipulation of Hardware or Software	C,I,A	Malicious software installation	R-ITS- S	M	H	H	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05
T 0.22	Manipulation of Information	I	Transmissi on of erroneous IVI messages	IF3	M	H	H	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05 R-ITS-S_SI-09 R-ITS-S_SI-10
T 0.23	Unauthorised Access to IT Systems	C,I	Unauthoriz ed access to the	R-ITS- S	M	H	H	R-ITS-S_AC-03 R-ITS-S_AC-09 R-ITS-S_AC-07

			system					R-ITS-S_AC-08 R-ITS-S_CM-05 R-ITS-S_CM-06 R-ITS-S_IA-02 R-ITS-S_IA-04 R-ITS-S_IA-06
T 0.25	Failure of Devices or Systems	A	Failure of devices in an unknown state that produce the blocking of the service	R-ITS- S	M	M	H	R-ITS-S_SC-24 R-ITS-S_SC-39 R-ITS-S_CM-07 R-ITS-S_CP-10 R-ITS-S_SI-11
T 0.26	Malfunction of Devices or Systems	I,A	Unavailabil ity of the service	R-ITS- S	M	M	H	R-ITS-S_SC-24 R-ITS-S_SC-39 R-ITS-S_CM-07 R-ITS-S_CP-10 R-ITS-S_SI-11
T 0.27	Lack of Resources	A	Overflow of storage capacity	R-ITS- S	L	M	L	R-ITS-S_AU-04 R-ITS-S_CM-06 R-ITS-S_CM-07 R-ITS-S_SC-06
T 0.28	Software Vulnerabilities or Errors	C,I,A	Wrong process prioritizatio n	R-ITS- S	M	M	H	R-ITS-S_AU-04 R-ITS-S_CM-06 R-ITS-S_CM-07 R-ITS-S_SC-06 R-ITS-S_SI-11
T 0.30	Unauthorised Use or Administration of Devices and Systems	C,I,A	System accessed by unauthoriz ed personnel	IF3	M	H	H	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05

T 0.31	Incorrect Use or Administration of Devices and Systems	C,I,A	Human error in system manageme nt	IF3	L	M	L	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05
T 0.36	Identity Theft	C,I,A	IP Spoofing of the C-ITS- S	R-ITS- S	L	H	M	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05 R-ITS-S_SI-09 R-ITS-S_SI-10
T 0.40	Denial of Service	A	No IVS messages being delivered	R-ITS- S	M	H	H	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10 R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05
T 0.43	Replaying Messages	I	Old update of red/green	IF3	M	H	H	R-ITS-S_AC-10 R-ITS-S_AC-12 R-ITS-S_AU-10

			transition being replayed					R-ITS-S_AC-05 R-ITS-S_AC-06 R-ITS-S_AU-02 R-ITS-S_AU-03 R-ITS-S_AU-04 R-ITS-S_AU-05 R-ITS-S_AU-08 R-ITS-S_AU-09 R-ITS-S_CM-05
T 0.46	Loss of Integrity of Sensitive Information	I		IF3	L	M	L	R-ITS-S_SC-08