SECREDAS

Product **Se**curity for **Cr**oss Domain R**e**liable **D**ependable **A**utomated **S**ystems

DELIVERABLE REPORT
"D5.1: Initial ITS station architecture with functional security features"

Document Type	Deliverable
Document Number	D5.1
Primary Author(s)	Thierry Ernst
Document Date	18 June 2019
Document Version / Status	v1.0
Distribution Level	Public
Reference DoA	30 April 2018

Project Coordinator	Patrick Pype, NXP Semiconductors, patrick.pype@nxp.com
Project Website	www.secredas.eu (in progress)
JU Grant Agreement Number	783119

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

European Commission
Horizon 2020
European Union funding
for Research & Innovation

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis

CONTRIBUTORS

Name	Organization	Name	Organization
Lead editors	YoGoKo & Commsignia		

FORMAL REVIEWERS

Name	Organization	Date
Roy Pennings	NXP	09.06.2019 / 16.06.2019
SECREDAS Project Steering Board	N/A	18.06.2019

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.5	06/06/2019	T. Ernst / YoGoKo	Version submitted for review
1.0	11/06/2019	T. Ernst / YoGoKo	Final draft version

Executive summary

The vehicle of tomorrow will be connected to remote platforms providing services (navigation, software update, telematics, electric vehicle charging, …). It will also cooperate with its surrounding environment (other vehicles, other road users, roadside and urban infrastructure) in order to improve road safety (crash avoidance, obstacle detection, emergency call, …) and traffic efficiency (green wave, lane access control, contextual speed limits, variable message signs, …). All these services require a common approach to the way communications are handled, and in a secure way. Cooperative Intelligent Transportation Systems (C-ITS) standards have been developed to allow the exchange of information between vehicles (cars, trucks, buses, ...), other road users (pedestrians, cyclists, …), the roadside and urban infrastructure (traffic lights, road tolls, ...), and control and services centres in the cloud (traffic control centre, service providers, map providers, …).

In order to ensure interoperability between the potentially unlimited Cooperative ITS services, a functional communication architecture ("*the ITS station communication architecture*") has been specified and is used as a reference for a complete set of standards developed by the International Organization for Standardization (ISO), the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI). This effort is conducted in Technical Committees dedicated to Intelligent Transport Systems (ITS): ISO TC 204, CEN TC278 and ETSI TC ITS. The standards have been developed mainly in Europe with the support of the European Commission from 2006 to 2013 (FP6 & FP7 collaborative projects and Standardization Mandate M/453 on C-ITS given to CEN TC278 and ETSI TC ITS). A first wave of Cooperative ITS services is currently under pilot deployment all over Europe (C-Roads, InterCor). Cooperative ITS services are set to be widely deployed following the adoption of the Delegated Act under final approval within the European Commission.

The objective of Work Package 5 (WP5) is to improve the security of communications involving access to vehicle data through external devices (other vehicles, roadside equipment, carried-on devices, sensors, servers, etc.) by means of wireless communication technologies (localized V2X communications and cloud connectivity). To address this objective, WP5 will pursue the development of secure communication solutions complying as much as possible with Cooperative ITS standards. More particularly WP5 will look into integrating software and hardware security mechanisms developed by SECREDAS partners into selected communication platforms. These platforms are developed or made available by SECREDAS partners. They are complying with existing Cooperative ITS standards and will be extended beyond the capabilities of existing solutions on the market. .

The objective of T5.1 is to analyse how SECREDAS security elements can fit into the functional ITS station communication architecture used as the reference for the deployment of Cooperative ITS services in Europe. T5.1 started at month 07 and will last until around the end of the project at month 33. Its first output is D5.1 "*Initial ITS*

station architecture with functional security features" at month 12, and its final output is D5.12 "*Final ITS station architecture with functional security features*" at month 33.

D5.1 is structured as follows: first, an introduction explains the objectives of WP5 "Connectivity", the objective and the process of the present deliverable D5.1 and its relationship with other SECREDAS WPs. The following section provides an overview of the development of Cooperative ITS services, from research to deployment through standardization. Then, the functional ITS station communication architecture used as a reference for all deployments of Cooperative ITS services in Europe is described in detail. The section on "hybrid communications" provides an insight towards the development of standards beyond the current State of The Art, while the last section before the conclusion describes the current status of the functional security elements already included in the ITS station communication architecture.

Table of Contents

Acronyms

AA	Authorization Authority
ADU	Application Data Unit
API	Application Programming Interface
AT	Authorization Ticket
BTP	Basic Transport Protocol
CAN	Controller Area Network
CA	Certificate Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
C-ITS-S	Central ITS Station (ISO 21217)
CPOC	C-ITS Point-of-Contact
C-V2X	Cellular V2X
C2C-CC	Car-to-Car Communication Consortium
CN	Correspondent Node (RFC 4885)
CRL	Certificate Revocation List
CEN	European Committee for Standardization
CoA	Care-of Address (RFC 4885)
DC	Distribution Centre
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short Range Communication
EA	Enrolment Authority
EC	Enrolment Credentials
ECTL	European Certificate Trust List
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GN	GeoNetworking
HA	Home Agent (RFC 4885)
HoA	Home Address (RFC 4885)
HSM	Hardware Security Module
IPv6	Internet Protocol Version 6
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITS-S	ITS station (ISO 21217)
ITS-AP	ITS station application process (ISO 21217)
ITS-G5	vehicular WiFi in 5.9 GHz frequency range
ITS-SCU	ITS station communication unit (ISO 21217)
ITS-SU	ITS station unit (ISO 21217)
LTE	Long Term Evolution (4G cellular)
MAC	Media Access Control
MCoA	Multiple Care-of Addresses Registration (RFC 5648)
MNN	Mobile Network Node (RFC 4885)
MR	Mobile Router (RFC 4885)
NEMO	Network Mobility Support (RFC 3963)
OBU	On-Board Unit
P-ITS-S	Personal ITS Station (ISO 21217)
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
PVT	Positioning, Velocity and Time
R-ITS-S	Roadside ITS Station (ISO 21217)
RSU	Road Side Unit
SPAT	Signal Phase & Timing
TLM	Trust List Manager
V-ITS-S	Vehicle ITS Station (ISO 21217)
V2X	Localized communications
WAVE	Wireless Access in Vehicular Environments
WG	Working Group

1. Introduction

1.1 WP5 objective and approach

The objective of Work Package 5 (WP5) is to improve the security of communications involving access to vehicle data through external devices (other vehicles, roadside equipment, carried-on devices, sensors, servers, etc.) by means of wireless communication technologies (localized V2X communications and cloud connectivity).

To address this objective, WP5 will pursue the development of secure communication solutions complying as much as possible with Cooperative ITS standards. More particularly, WP5 will look into integrating software and hardware security mechanisms developed by SECREDAS partners into selected communication platforms. These platforms are developed or made available by SECREDAS partners and comply with existing Cooperative ITS standards. They will be extended beyond the capabilities of existing solutions on the market.

As indicated in the Description of Work, WP5 has started its work with the analysis of existing standards and communication technologies for connected and cooperative mobility, i.e. the set of standards developed within ISO TC204, CEN TC278 and ETSI TC ITS for Cooperative ITS services. This analysis will direct technical development realized in WP5 tasks T5.2 to T5.6. However, WP5 technical development will principally seek to meet WP9 demonstration requirements according to WP1 Use Cases (UCs).

1.2 Task 5.1

D5.1 is an output of Task 5.1 which objective is, as it is originally written in the SECREDAS description of work to *"Specify in details how high security features designed in WP3 will be mapped into the ITS station reference architecture for V2X communication, Internet connectivity, IoT devices and radar 5G. Taking as an input the high level Secure architecture for Automated Systems defined in WP2, WP5 will map it to existing ITS communication standards defined for Cooperative ITS (primarily V2X standards developed around ITS-G5 by ETSI / CEN / ISO for the European market, but also IEEE / WAVE standards developed for the USA and other regional markets) and Internet connectivity (ISO TC22 and TC204 standards based on IPv6 and the TCP/IP family set of protocols specified by the IETF). Various access technologies will be considered, with a focus on vehicular WiFi (ITS-G5), regular WiFi (IEEE 802.11 n / ac), cellular (legacy 3G and 4G, and more importantly 4G direct device-to-device and 5G) and sensor networks (IEEE 802.15.4, ...). To this end, security features identified in the high-level Secure architecture for Automated Systems and missing in the ITS station reference communication architecture (ISO 21217 / ETSI 302 665) will be clearly identified and integrated into relevant parts of the ITS station reference architecture. The results of this task may lead into improving the specification of existing ITS standards. Results will be fed to ISO, CEN and ETSI through WP10."*.

T5.1 started at month 07 and will last until around the end of the project at month 33. Its first output is D5.1 "*Initial ITS station architecture with functional security features*" at month 12, and its final output is D5.12 "*Final ITS station architecture with functional security features*" at month 33.

1.3 Deliverable D5.1

The work on deliverable D5.1 "*Initial ITS station architecture with functional security features*" started with the kick-off of T5.1 in month 7. This deliverable provides an analysis of the functional ITS station communication architecture and related Cooperative ITS standards applicable to SECREDAS. It addresses the subset of the objectives of SECREDAS indicated in

Table 01 below.

Table 01: SECREDAS Objectives applicable to this deliverable

SECREDAS objective number (DoA)	SECREDAS objective title	SECREDAS expected outcome
7	Develop & validate a next level of secured and privacy-protecting external communication technologies (V2X, 5G)	• Integration of security building blocks necessary to protect the external interfaces linking the vehicle to the external environment • Protection of the vehicle against security breaches using communication with other vehicles, roadside infrastructure (V2X), IoT, and sensor devices interacting with the vehicle • Performance assessment of the security building blocks and their ability to provide an efficient protection against various types of attacks
12	Take an active role in international standardization	• Analyse the applicability of current security and safety standards, and initiatives, for the automotive domain • Contribution to standards in ISO TC204, CEN TC278, ETSI TC ITS

D5.1 first provides an overview of the development of Cooperative ITS services, from research to deployment through standardization. Then, the functional ITS station communication architecture used as a reference for all deployments of Cooperative ITS services in Europe is described in detail. The section on "hybrid communications" provides an insight towards the development of standards beyond the current State of The Art, while the last section before the conclusion describes the current status of the functional security elements already included in the ITS station communication architecture.

As its title stands for, D5.1 "*Initial ITS station architecture with functional security features*" is the initial output of T5.1 turning around the standardized ITS station communication architecture. It will be continuously revised during the course of SECREDAS into a finalized deliverable (D5.12 "*Final ITS station architecture with functional security features*") which will provide the final analysis. The first purpose of the initial analysis presented in D5.1 is to shed light on the existing functional ITS station communication architecture and related Cooperative ITS standards and to share this knowledge internally within SECREDAS.

At first, it will serve within SECREDAS as the reference document guiding WP1 Use Case definitions, WP5 development,

WP9 demonstrations and WP10 contributions related to Cooperative ITS standards. It will serve as the main input from WP5 to analyse how SECREDAS secure elements developed in WP3 can fit into the functional ITS station communication architecture, and how the security of communications can be improved in compliancy with functional ITS station communication architecture. Transforming D5.1 to D5.12 will thus be an iterative process.

For WP9, D5.1 in its final state at M12 will help to ensure interoperability between SECREDAS partners (i.e. all having communication systems used in WP4, WP5, WP6 and WP9 complying to the same communication standards, thus ensuring interoperability between WPs and also at test sites with third parties).

Findings of this analysis and proposed additions functional elements of the ITS station communication architecture or modifications of the functional ITS station communication architecture will be communicated through WP10 continuously to SDOs (ISO, CEN and ETSI) in charge of the related standardization effort.

1.4 Relation with other WPs

At this stage of the SECREDAS project, D5.1 doesn't intend to relate its content directly to the work conducted in other WPs, besides WP10. However, this deliverable will impact upon the work conducted in other WPs. D5.1 follows the holistic objective of sharing within SECREDAS the knowledge WP5 participants have acquired on the standards and communication technologies currently developed for connected and cooperative mobility. This deliverable will thus serve within SECREDAS as the reference document guiding WP1 UC definitions, WP5 development, WP9 demonstrations and WP10 contribution related to Cooperative ITS standards.

1.5 Next steps

The revision of this deliverable into deliverable D5.12 "*Final ITS station architecture with functional security features*" will provide an analysis of the output of WP1, WP2 and WP3 and propose necessary adaptations to the reference communication architecture in order to fulfil use cases identified in WP1 which may not yet be supported using existing standards or not feasible with an acceptable level of security.

Standards developed by organizations other than ISO TC204, CEN TC 278 and ETSI TC ITS for other regional markets (e.g. IEEEE P1609 for the V2X communications in North America) or specific services (e.g. Electric Vehicle Charging developed by ISO TC 22) might also be investigated during the course of SECREDAS, with less effort, and with no intend for technical development nor integration within SECREDAS.

2. Cooperative ITS services & standards

2.1 Connected & cooperative mobility

The vehicle of tomorrow will be connected to remote platforms providing services (navigation, software update, telematics, electric vehicle charging, …). It will also cooperate with its surrounding environment (other vehicles, other road users, roadside and urban infrastructure) in order to improve road safety (crash avoidance, obstacle detection, emergency call, …) and traffic efficiency (green wave, lane access control, contextual speed limits, variable message signs, …). All these services require a common approach to the way communications are handled.

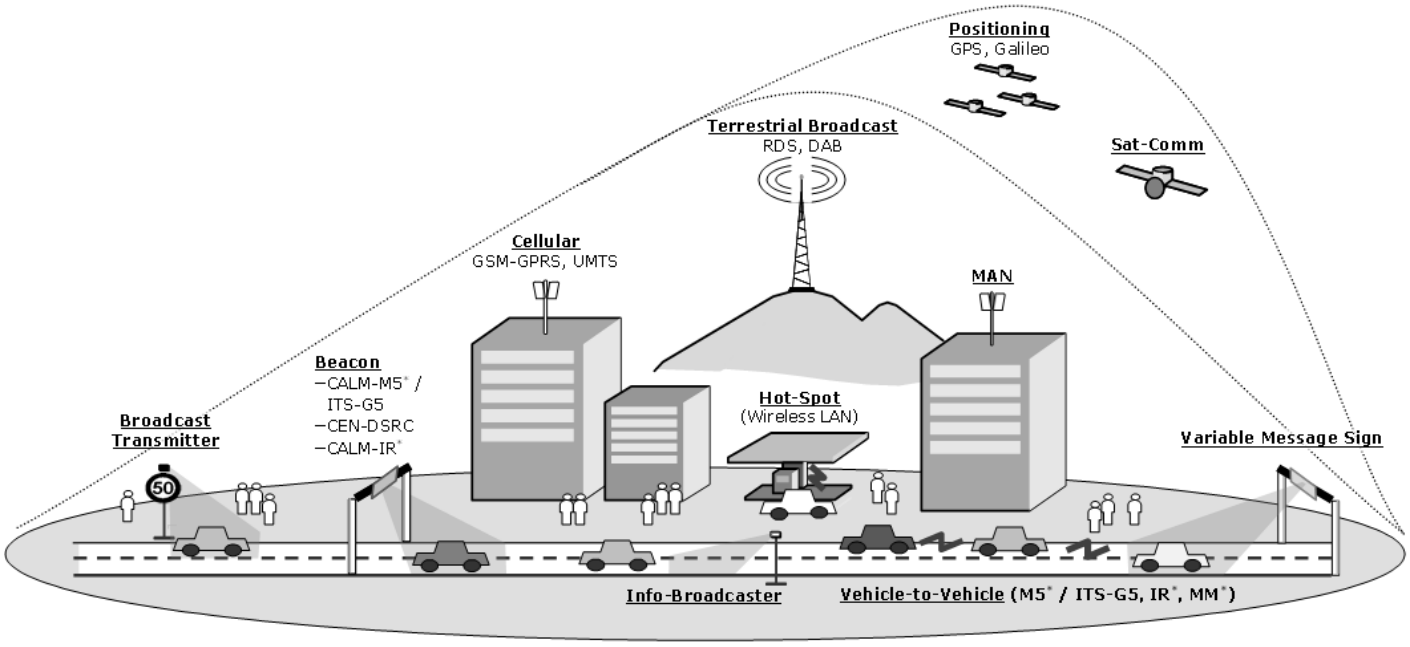

Figure 01: Connected & Cooperative Mobility (ISO 21217)

2.2 Cooperative ITS standards

Cooperative Intelligent Transportation Systems (C-ITS) are Intelligent Transportation Systems (ITS) in which information is exchanged between vehicles (cars, trucks, buses, ...) and other road users (pedestrians, cyclists, …), the roadside and urban infrastructure (traffic lights, road tolls, ...) and control and services centres in the cloud (traffic control centre, service providers, map providers, …). C-ITS services are traditionally ranged into “road traffic safety”, “traffic efficiency” and “other” (infotainment, value added services, etc.).

In order to ensure interoperability between (potentially unlimited) C-ITS services, reference communication architecture and related standards have been developed by the International Organization for Standardization (ISO), the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI).

This effort is conducted in Technical Committees dedicated to Intelligent Transport Systems (ITS): ISO TC 204, CEN TC278 and ETSI TC ITS.

Most relevant activities are conducted by ISO TC204 in WG16 (communications), WG17 (personal devices), WG18 (Cooperative ITS), by CEN TC278 in WG16 (Cooperative ITS) and WG17 (urban ITS) and all ETSI TC ITS WGs. All these standards are based on a common ITS communication architecture (ITS station reference architecture) specified by ISO [ISO 21217] and ETSI [ETSI 302 665].

2.3 Localized communications (V2X)

One of the main pillars of Cooperative ITS is "localized communications", i.e. V2X communication between the vehicle and its surrounding environment (other vehicles, other road users, roadside infrastructure, urban infrastructure).

The term ***localized communications*** refers to communication technologies used for the exchange of data between neighbouring vehicles (**vehicle-to-vehicle** or **V2V**) and between the vehicle and the roadside infrastructure (**vehicle-roadside**). Vehicle-to-roadside communications are often referred to as V2I (vehicle-to-roadside infrastructure) but this term is confusing and may also refer to vehicle-to-(telecommunication)infrastructure, so it should be used. It is sufficient to use the term **V2X** as there is no difference between localized communications involving only vehicles from localized communications involving both vehicles and roadside infrastructure.

In the literature, V2X is sometimes used with the meaning "vehicle-to-everything" i.e. communication system that incorporate specific types of communication as V2I (vehicle-to-(roadside)infrastructure), V2N (vehicle-to-network), V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), etc.[1]. However, "vehicle-to-everything" is also confusing as it may imply that all types of communications technologies involving the vehicle, including cloud-based communications over the cellular network or the satellite network are included, which would dismiss any meaning for V2X. In this document we will therefore stick strictly to *localized communications* and we will focus mostly on short-range communications around a few hundred meters (so, ultra short-range sensor-based communications are addressed separately from V2X).

In general, V2X is considered as the means of communication when it comes down to **road traffic safety** and **road traffic efficiency** services that require real time transmission delays. As it is involving safety aspects, V2X is usually supported by some form of regulation in all regions, by e.g. having dedicated frequency band(s) in most regions and continuously being harmonized at the global level.

[1] https://en.wikipedia.org/wiki/Vehicle-to-everything

The most mature V2X technology is vehicular WiFi, i.e. a variant of the 802.11 WiFi technology specifically designed for ad-hoc communications for fast-moving vehicles. This WiFi variant for vehicular communications is specified as IEEE 802.11p, now part of IEEE 802.11-2016, and integrated in the ITS station reference architecture (see Section 3

In Europe, IEEE 802.11p vehicular communications are known as ITS-G5 while in the US it is known as DSRC (Dedicated Short-Range Communications), which is also misleading as in Europe DSRC is standing for another short-range communication technology used for tolling (CEN DSRC).

In Europe, the physical access (radio) layer (including media congestion control) and frequency regulation is specified as part of ITS-G5 [ETSI EN 302 663] according to the European Directive (2010/40/EU) which instruments the coordinated implementation of ITS in Europe[2]. The directive facilitated the development of Cooperative ITS standards based on a common communication architecture.

The term V2X usually covers specifications and standards from the physical layer up throughout network and security layers to applications. V2X standards for communications between vehicles and the road infrastructure in the 5.9 GHz frequency band (ITS G5, GeoNetworking, CAM, DENM) have been developed principally within ETSI while ISO and CEN have been concentrating on the applicability of V2X communications using a wider panel of access technologies, including ITS-G5 and LTE-V2X [ISO 17515-3]. These V2X standards are based on earlier work initially developed in European Projects (CVIS, GeoNet, SafeSpot, DriveC2X, FOTsis, SeVeCoM, PRESERVE, ITSSv6) and the Car2CarCommunication Consortium (C2C-CC), later tested in V2X FOTs (DriveC2X, SCORE@F) and now further validated in large scale pilots (C-ITS Corridor, SCOOP@F).

Currently, ETSI as well as the C2C-CC are working on a set of test suites to ensure standard conformance, interoperability and security for the Day One deployment of ITS-G5 technology. These test suites include physical layer tests, protocol layer tests as well as application layer tests which are only partially automated. A close cooperation between ETSI TC ITS and C2C-CC will ensure that SECREDAS results will match C-ITS standardization and compliance assessment requirements.

In recent years C-V2X (cellular-V2X) has emerged as an alternative solution to ITS-G5. Although C-V2X is part of release 14 by 3GPP, it is not yet integrated in the V2X family of standards. In order to become a real alternative, C-V2X will have to go through all the development cycle. C-V2X must first be integrated in the ITS station reference architecture as an access technology (this is undergoing at both ETSI and ISO); conformance tests must be specified, and interoperability tests must be organized. In addition, a frequency band must be allocated.

[2] https://ec.europa.eu/transport/themes/its/road/action_plan_en

2.4 Cooperative ITS services deployments

Europe has been a frontrunner in Cooperative ITS with field operational tests running as early as CVIS in 2006[3]. The scope of the European initiating Directive 2010/40/EU was to reach deployment. The initial deployment, also referred to as "Day 1 services" are mostly based on ETSI's Basic Set of Applications [ETSI 102 637] and ETSI's Release 1 [ETSI 101 607] also from ETSI. The first document aims at specifying the scope and underlying assumptions, while the second provides a complete list of standards available for the first generation of the ecosystem covering all layers. Pilot deployments of Cooperative ITS services complying with "Day 1" standards are undergoing everywhere in Europe under the framework of C-Roads and InterCor European platforms.

Apart from the underlying standards, two major industrial harmonized specifications of the deployed systems exist. The Basic System Profile version 1.3[4] by the Car2Car Communication Consortium (industrial group of automotive OEMs and their suppliers having activities in Europe), which specifies the vehicular profile for the initial deployment, while the C-Roads (European national road operators and respective suppliers) Harmonized Communication Profile[5] defines the agreed specifications by the roadside infrastructure stakeholders.

A third source of reference specification for European deployment is delivered by the European Commission's C-Platform phase I and II [C-ITS Platform 1, C-ITS Platform 2]. Especially important for SECREDAS, the Platform developed recommendations as well as policies that are partially enforced on a European regulatory level. Such policies are e.g. the Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) and the Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems[6]. It is important to note that currently a Delegated Act is being prepared by the Commission covering specifications for the Release 1 introduced above. The pending adoption of the Delegated Act under final approval within the European Commission is likely to boost wide adoption from the automotive industry and roadside equipment providers and to stem development of innovative Cooperative ITS services in new application domains (connected & cooperative autonomous vehicles, public transport, freight and logistics, etc.).

2.5 Next steps in European deployments

The ongoing pilots are set to be further extended in the next two years. They will particularly focus on the interoperability of the standalone pilots undergoing in different countries and will consider a combination of

[3] https://trimis.ec.europa.eu/project/cooperative-vehicle-infrastructure-systems
[4] https://www.car-2-car.org/documents/basic-system-profile/
[5] https://www.c-roads.eu/platform/get-in-touch.html
[6] https://ec.europa.eu/transport/themes/its/c-its_en

technologies (ITS-G5 and cellular) to achieve a better penetration of the C-ITS services (see “hybrid communications” in Section 4).

Looking forward, the deployment of Cooperative ITS services will go through several phases of deployments. While ongoing pilot deployments focuses to a limited set of services (Day 1) and technologies (ITS-G5 and 3G/4G cellular), new Cooperative ITS services which apply to new deployment context (urban areas, rural areas, vulnerable road users, autonomous vehicles, …) will require the deployment of new access technologies (5G, cellular V2X, optical communications, …) and new facilities (precise positioning, generic messaging, secure sessions, secure access to data, …). At some point in time, pilot deployment of C-ITS services will meet pilot deployment of connected and cooperative autonomous vehicle (CCAM) so new standards currently under development will be integrated.

Emerging standards and services which represent a certain interest to SECREDAS include the following:

- Standards in support of hybrid communications.
- Standards in support of precise positioning.
- Standards in support of vulnerable road users.
- Standards in support of automated driving (Cooperative Adaptive Cruise Control and Platooning services, Collective Perception Service, Encrypted V2X messages for platooning).

3. The ITS station reference architecture

3.1 ITS station architecture background

A functional communication architecture known as the *ITS station reference architecture* is the result of a harmonization effort conducting after the original development by ISO TC204 started in 2002 of a standard communication architecture combining a variety of access technologies and protocols and suitable for a variety of ITS needs. This harmonization effort was initiated within COMeSafety, a specific support action in which participated representatives from various organizations. The most significant contributors were representatives from European Projects CVIS (Cooperative Vehicle-Infrastructure Systems), Coopers (Co-operative Systems for Intelligent Road Safety), SafeSpot (Cooperative vehicles and road infrastructure for road safety), GeoNet (IPv6 GeoNetworking), SeVeCom (Secure Vehicular Communications) and the Car-to-Car Communication Consortium (C2C-CC), and several European Projects. Their work considered earlier architecture work performed within ISO TC204 WG16, also known as CALM (Communications Access for Land Mobiles) and established at ISO in 2000. This group is the birthplace of many of the concepts behind the communication architecture before it was harmonized by COMeSafety.

This harmonization work resulted in the specification of a common communication architecture which was then formally specified by ISO TC204 [ISO 21217] and ETSI TC ITS [ETSI 302-665]. This architecture is outlined in Figure 3-1.

3.2 ITS station layered architecture

The design principle of this communication architecture is to support simultaneously a diversity of applications of various categories (road safety, traffic efficiency and comfort / infotainment) and to offer them a diversity of access technologies with distinct characteristics (show, medium and long range wireless communications), for a variety of communication modes (localized and cloud-based communication, wired and wireless communications, broadcast and point-to-point communications, mobile and fixed stations, …). The necessary functionalities can vary according to many factors: the type of ITS station, the services it provides, system architecture design choices, regulation, etc.

In order to support this view, the ITS station reference architecture, shown on Figure 3-1, is defined into layers.

The adopted layered architecture differs from conventional 7-layer OSI architecture with the addition of vertical entities (the *ITS station management entity* and the *ITS station security entity*) providing cross-layer management and security functions. A middle layer (*ITS station facilities layer*) provides common services to the applications (message handling, service discovery, selection of the communication stack, maps, positioning, time stamping, etc.). Network and transport protocols are grouped within a single *ITS station networking & transport layer* while the *ITS station access technologies layer* can support any existing and forthcoming access technologies, including vehicular WiFi (IEEE 802.11p also known

as ETSI ITS-G5 in Europe), urban WiFi (IEEE 802.11n), cellular (2G/3G, LTE, LTE-D2D, LTE-V2X, 5G), infra-red, satellite, IEEE 802.15.4 (6LoWPAN), 60 GHz millimetre-wave, optical communications, and possibly others.

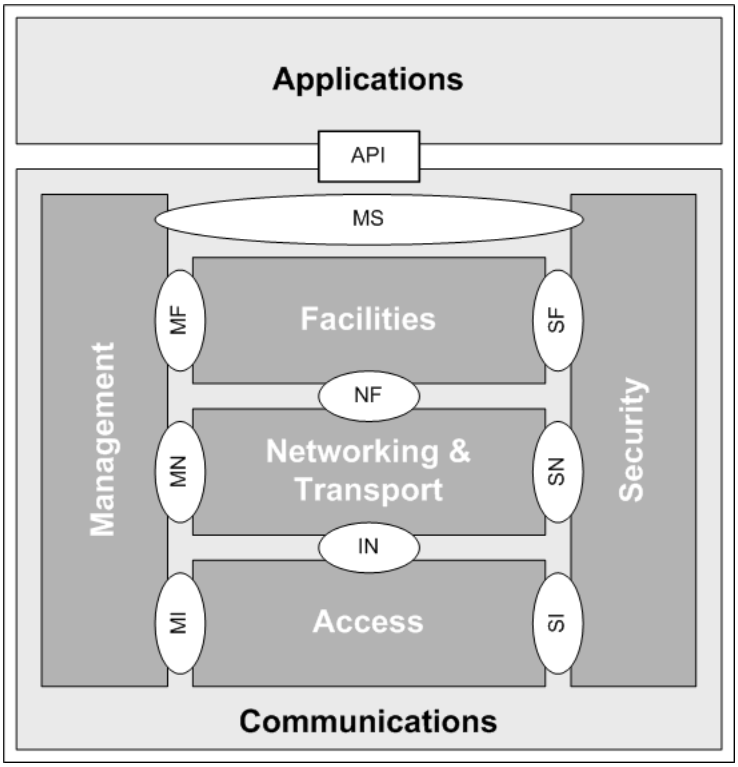

Figure 02: Simplified ITS Station (ITS-S) Reference Architecture (ISO 21217)

A fundamental advantage of this design concept over currently deployed systems is that applications are abstracted from the access technologies and the networks that transport the information from the source to the destination(s). This means that ITS stations applications are not limited to the availability and characteristics of a single access technology and protocol stack. Communication management functions make optimal use of all these resources transparently to the applications.

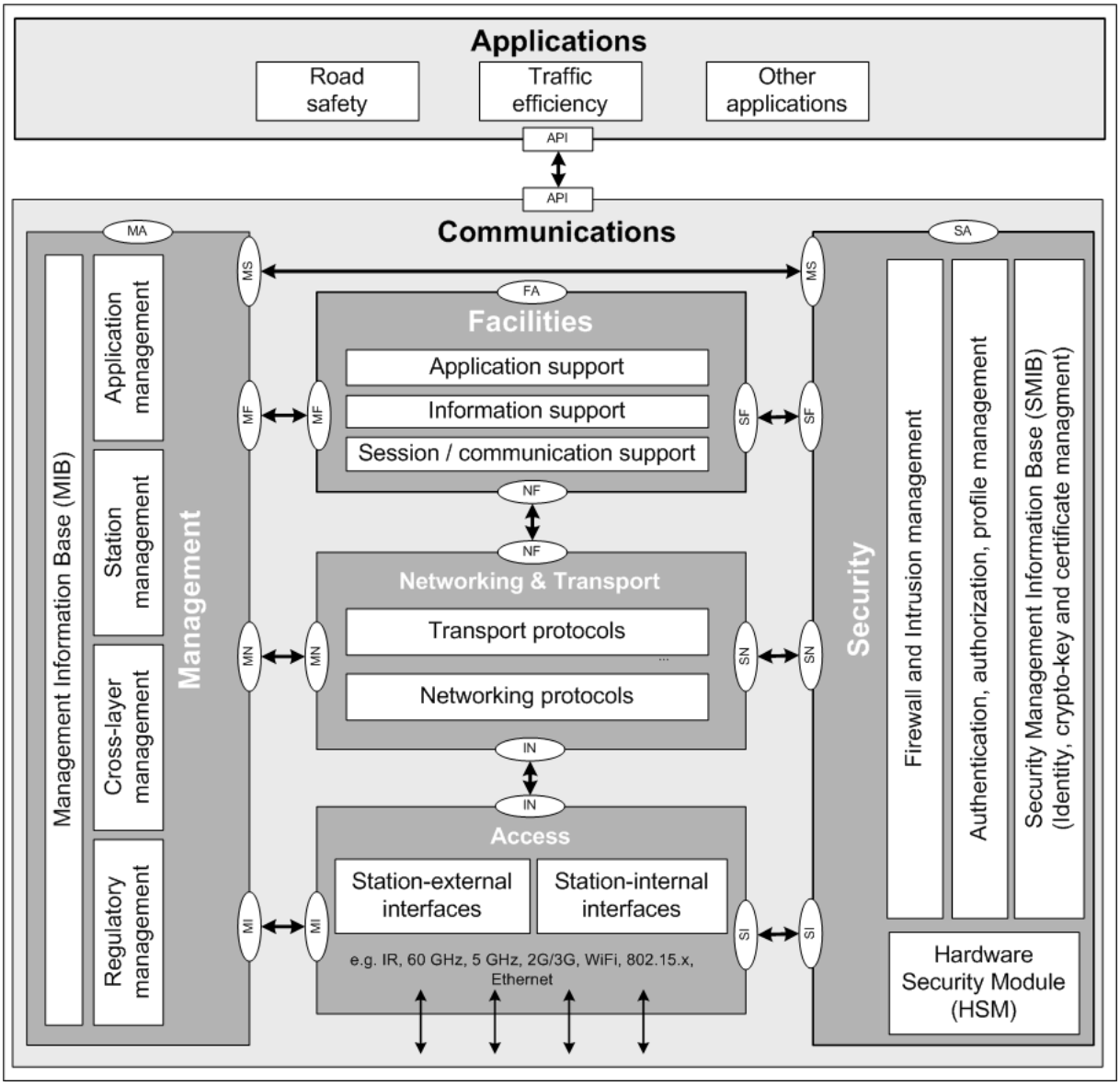

Figure 03: Detailed ITS Station (ITS-S) Reference Architecture

Thanks to this diversity of protocols and access technologies that can be combined simultaneously, the ITS station reference architecture is able to support a variety of communication scenarios (vehicle-based, roadside-based and Internet-based) for a variety of application types (road safety, traffic efficiency and comfort / infotainment). The particular novelty from a design viewpoint, compared to a typical OSI 7-layer architecture, are the two vertical entities, i.e. the ITS station management entity and the ITS station security entity performing a number of cross-layer functions. Cross-layer functions are not new in the literature (ITS no less than other UCs), but it is the first time this is explicitly shown on architecture diagrams.

The ITS station reference architecture is defined in [ISO 21217] and [ETSI 302 665]. The main difference between ETSI and ISO documents lies in the specification of the ITS station management entity. So far, ISO CALM has concentrated its effort on the cross-layer functions to ensure a given communication flow is matched to a particular communication

interface (CI) according to application needs and current network conditions. ETSI is not too much concerned about this issue, because ETSI TC ITS standards are largely focused on the use of the 802.11p access technology (ITS-G5) solely, whereas the focus of the ISO work has always been the simultaneous support of a variety of access technologies. For an up-to-date understanding of the terminology and underlying design principles, the reader is advised to refer to [ISO 21217) (last revision 2015, new revision pending) rather than [ETSI 302 665; first publication in 2010 and no revision since then).

3.3 ITS station unit types

Defined in [ISO-21217], an ITS station unit (ITS-SU) is a functional entity comprised of an ITS-S facilities layer, ITS-S networking and transport layer, ITS-S access layer, ITS-S management entity, ITS-S security entity and ITS-S applications entity providing ITS services. From an abstract point of view, the term "ITS station" refers to a set of functionalities. The term ITS-S is often used to refer to an instantiation of these functionalities in a physical unit. Often, the appropriate interpretation is obvious from the context. The proper name of the physical instantiation of an ITS-S is ITS station unit (ITS-SU).

Historically, the terms On-Board Unit (OBU), Roadside Unit (RSU) and Application Unit (AU) are used in the automotive industry. However, these terms were not defined with a networking view in mind and have therefore become obsolete in the context of Cooperative ITS services. In addition, the ITS station reference architecture does not use these terms either because they were confusing the discussion. This led to the definition of the generic term *ITS station* unit (ITS-SU) and a distinction of the supported functions according to the type of environment or network where it is be located. As such, four types of ITS station units are currently defined in the ITS station reference architecture, as described on Figure 3-3:

- **vehicle ITS station** (V-ITSS): ITS station unit located in a vehicle;
- **roadside ITS station** (R-ITSS): ITS station unit located in the roadside infrastructure;
- **central ITS station** (C-ITSS): ITS station unit located in the central infrastructure;
- **personal ITS station** (P-ITSS): ITS station unit located in a hand-held device.

More ITS station types may be added in the future, if needed (e.g. for buses, trains, emergency vehicles, tramways, bicycles, motorbikes, truck, ...).

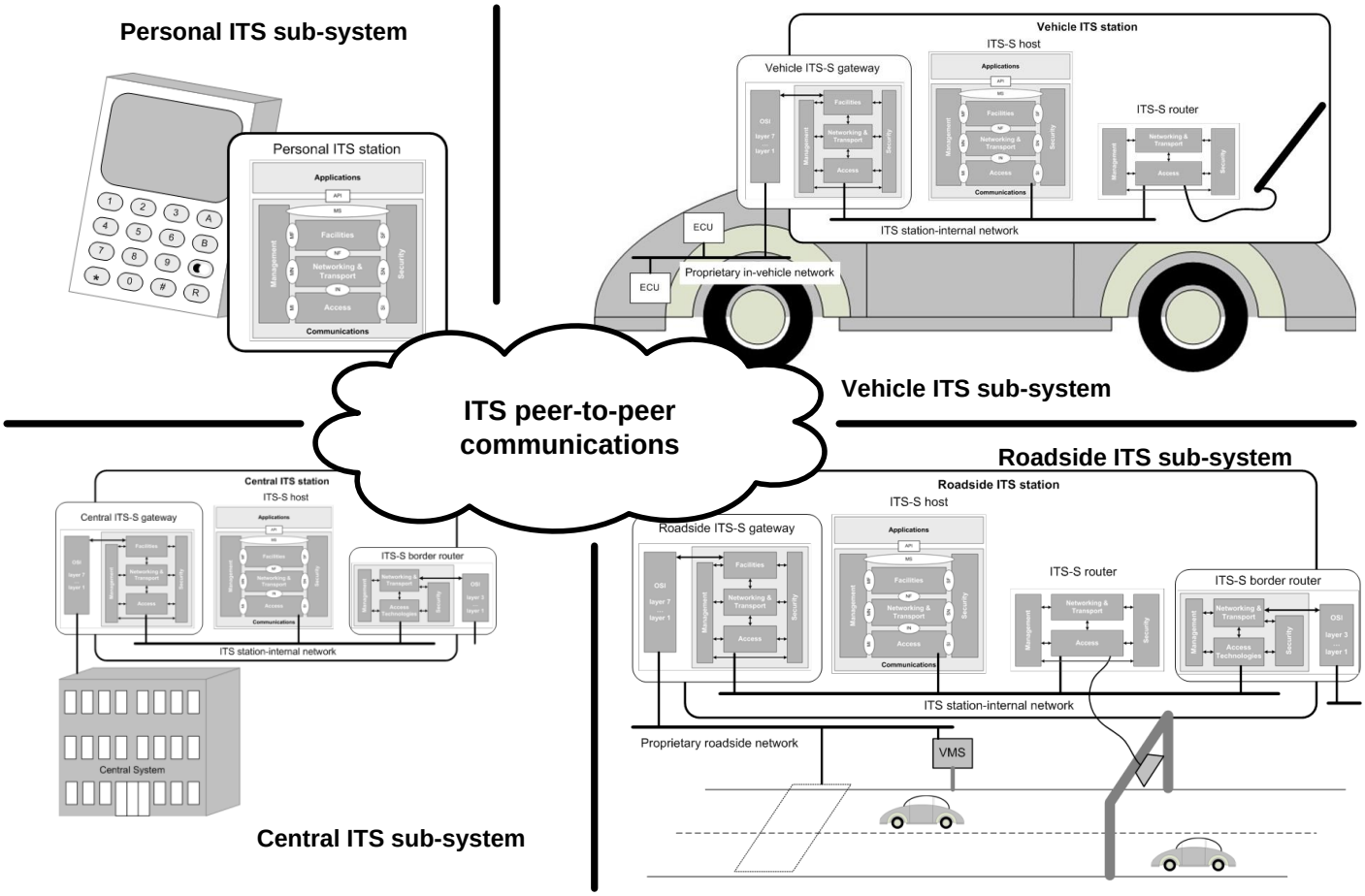

Figure 04: ITS Station unit (ITS-SU) types

3.4 ITS station communication unit

The physical implementations of an ITS station functionality are ITS station unit (ITS-SU). An ITS-SU can be composed of one or several ITS-S communication units (ITS-SCU) interconnected via an ITS station internal network, as illustrated on Figure 3-4 (vehicle ITS station unit view) and Figure 3-5 (roadside ITS station unit view).

In the most general case, the functions of an ITS station (ITS-S) are split into a router (ITS-S router) and hosts (ITS-S host) attached to the ITS-S router via some ITS station internal network. The router and hosts functions may also be merged into a single entity.

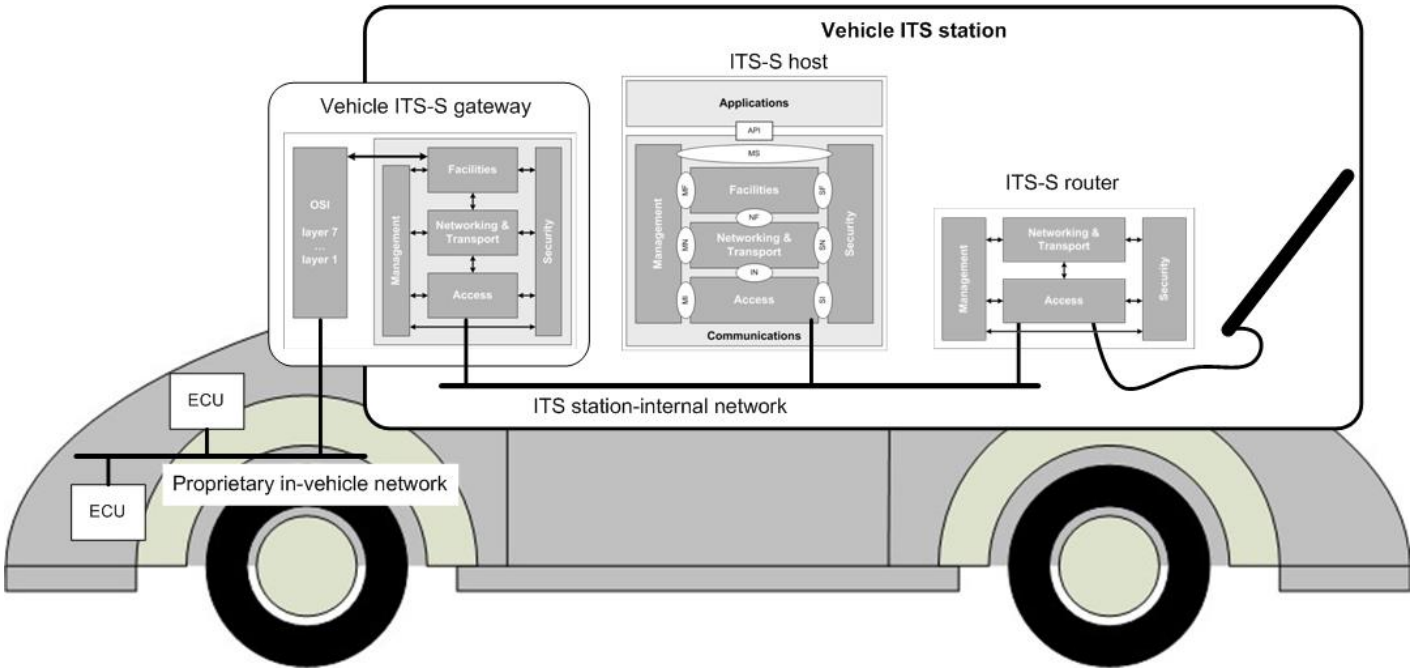

Figure 05: Example of a vehicle ITS station unit (ISO 21217)

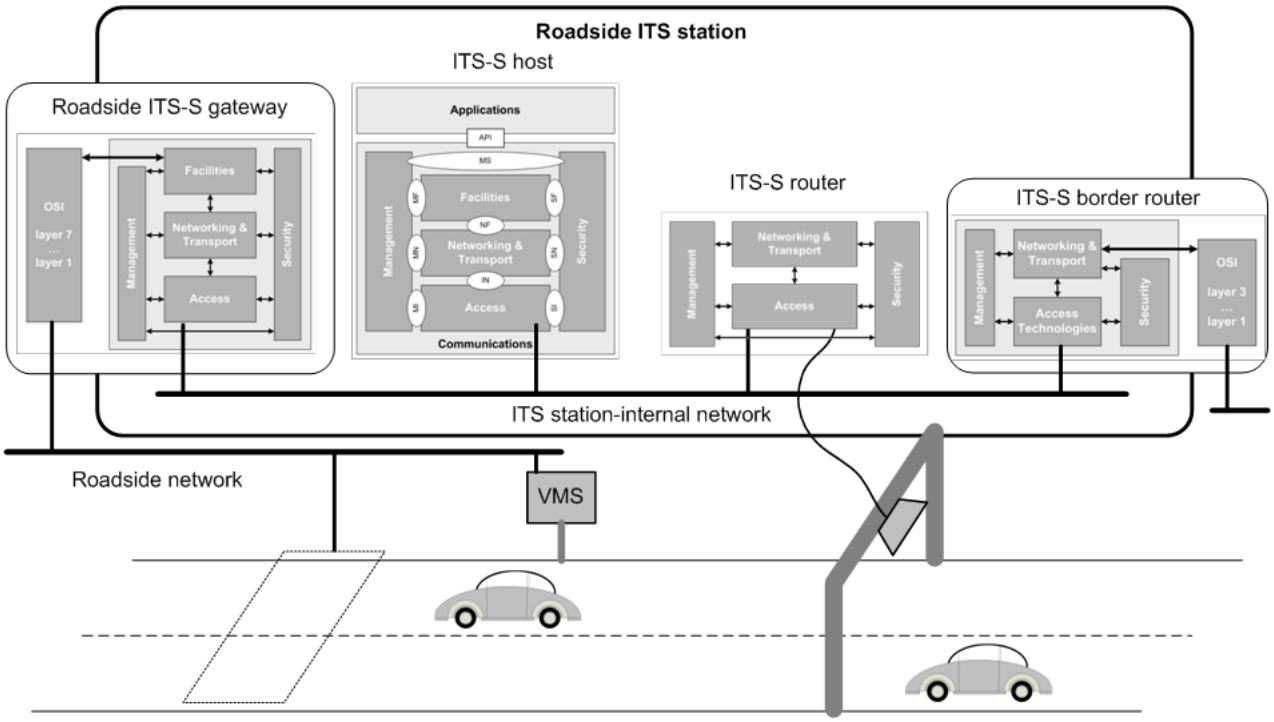

Figure 06: Example of a roadside ITS station unit (ISO 21217)

In situations where the ITS station must be linked to an network of components (e.g. CAN bus in the case of a vehicle, or a control loop or sensor network in the case of a roadside ITS station), the ITS-S communication unit that is able to

link the ITS station to that vehicle-internal network, is called an ITS-S gateway[7]. Contrary to the ITS-S router, the ITS-S gateway doesn't transfer data directly through the network layer but only from the facilities / application layer. The ITS-S gateway is therefore acting as a security firewall.

The ITS-S gateway functionality is an essential component to guarantee secure access to vehicle data, and **is thus of special interest to SECREDAS, particularly to ensure convergence of work between WP4, WP5 and WP6** (see in conclusion).

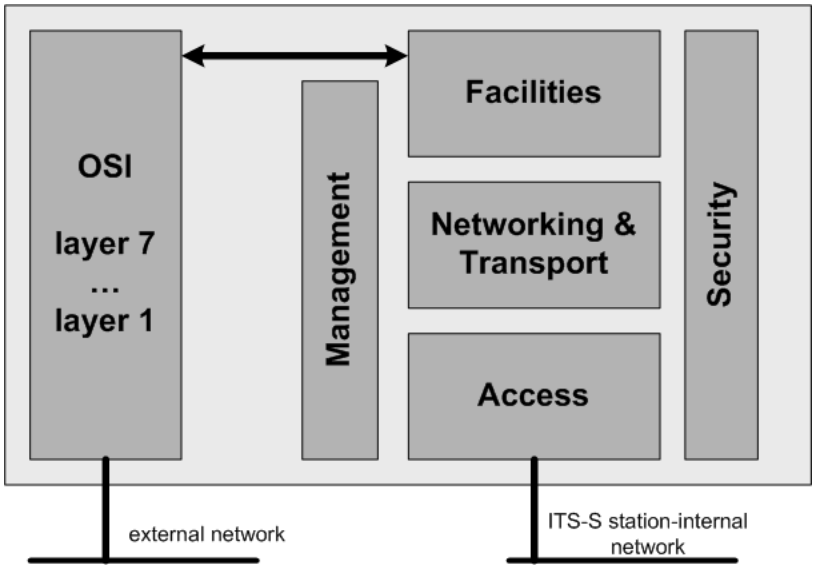

Figure 07: ITS station gateway (ISO 21217)

According to [ISO-21217], the ITS station is defined as a **bounded secured managed domain**. ITS-SCUs and ITS-SUs are thus mutually trusted devices. Security means to establish trust between ITS-SCUs and between ITS-SUs are defined in [ISO-21177] (see Conclusion).

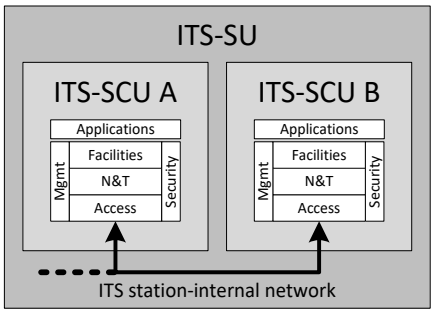

Figure 08: Interconnection between ITS station communication units in an ITS station unit (ISO 21217)

[7] As show non the figure illustrating the ITS-S gateway, the network connecting the various ITS-S communication unit composing the ITS-S is called in ITS-S internal network. From the view point of an ITS-S integrated in a vehicle, the CAN bus is viewed as an external network.

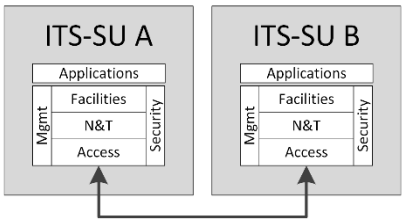

Figure 09: Interconnection between ITS station units (ISO 21217)

3.5 ITS station application layer

Applications supported by the ITS station reference architecture are traditionally spread in three categories (road safety, traffic efficiency and others). These applications rely partly on common services offered by the ITS station facilities layer. In the context of the ITS station reference architecture, these applications are referred to as ITS station applications (ITS-S applications) whereas ITS station application processes (ITS-S-APs) are the entities of the ITS station performing information processing for a particular application; they may use ITS station facilities services to receive and transmit information. ITS-S APs obey to the general requirements applying to ITS-S-APs as specified in [ISO-17423], [ISO-17429] and [ISO 24102-6].

ITS-S APs sitting on two distant ITS stations unit may communicate without subsequently involving the ITS station facilities. For example, as a result of receiving a service notification by the ITS station facilities of a charging spot for electric vehicles, the ITS-S APs may directly contact a server to enquire about the availability of the charging spot and book it. In addition, some ITS station applications may be completely standalone, i.e. not taking benefit of the ITS station facilities at all. The notion of ITS-S AP is a relatively new concept from ISO; it is not compulsory and is not yet adopted in ETSI's V2X standards. However, it is essential for benefiting from an increasing number of underlying ITS station facilities services.

3.6 ITS station facilities layer

The ITS station facilities layer (SF) is an intermediate layer between the ITS station networking & transport layer (SNT) and the applications, offering them access to information collected by other ITS stations (vehicles, roadside) and freeing them from the necessary message signalling to transmit and process data exchanged between ITS stations in a broadcast fashion. The immediate benefit is the sharing of data between various applications which would otherwise have broadcast potentially similar information, therefore increasing consumption of network resources and processing power.

The initial set of Cooperative ITS services developed for road traffic safety and traffic efficiency rely on V2X messages that are implemented as common services in the ITS station facilities layer. The most popular are:

- CAM (Cooperative Awareness Basic Service) [ETSI 302-637-2] is a message designed for time-critical road safety purposes. It provides a “Here I am” type of periodic message, including position, heading and such information on any ITS station allowing all receivers to know the status and properties of all entities nearby. This message is broadcast periodically (up to 10 times a second) and is mainly used by receiving vehicles in the vicinity to anticipate and prevent a risk of collision.

- DENM (Decentralized Environmental Notification Basic Service) [ETSI 302-637-3] is an event-based message. It describes specific events occurring in a specific geographic area which may be dangerous or otherwise important for broadcast. It is triggered as the event occurs. This message is used to report about traffic hazards (obstacle, vehicle in opposite direction, black ice).

- SPaT (Signal Phase and Timing) is a message used to deliver traffic light phases and timing of an intersection allowing the reviewer of both types of information to have a digital status and parameters of an intersection.

- MAP is a message used to provide information about the topology of an intersection; generally used in combination with the SPaT message

- IVI [ISO 19321 / ISO 19091] is a message to communicate VMS (variable message sign) and other traffic signs between infrastructure and vehicles.

- SAM (Service Announcement Message) [ETSI 102-890-1]: currently not used in European pilot deployments but is available as a tool to facilitate service announcement to ITS stations offering various UCs for SECREDAS to investigate.

ISO TC204 is also developing standards specifying common facilities not directly linked to V2X to facilitate the development of ITS applications. These include a generic messaging scheme [ISO 17429], advanced positioning [ISO 21176] and secure vehicle interface [ISO 21177], which is of particular interest for SECREDAS (see Section 0):

- Generic facilities header and profile handler: [ISO-17429] defines a generic message handler and a communication profile handler that allow to transmit any kind of data in various modes (broadcast or point-to-point, public or proprietary). Packets can be transmitted between peers using any available protocol stack (e.g. ITS-G5/GN/BTP or ITS-G5/IPv6/UDP or cellular/IPv6/UDP), transparently to the application layer, depending on the communication needs of the application and network availability. This standard is key to ensure interoperability between ITS stations deployed with a different set of features and technologies and is also a key enabler of hybrid communications;

- Generic publication-subscription mechanism: also defined in [ISO 17429], this mechanism allows applications to publish data that will be transmitted by the facilities layer to subscribed applications, either locally in the ITS station unit, or in peer ITS stations. Each application subscribes to the reception of a given piece of data (this requires a global data registry); and relevant data received at the facilities layer is forwarded by the facilities layer to all subscribed applications (push mode).

- LDM (Local Dynamic Map): Information collected from V2X messages, sensor networks and probably other sources are recorded in a Local Dynamic Map (LDM), i.e. a database where information about the environment is stamped with position and time. The LDM for vehicle implementation is specified at ETSI [ETSI 302-895] whereas ISO is defined a globally applicable LDM [ISO 18750].

- PVT (Positioning, Time and Velocity) is a new standard under development [ISO 21176]. It intends to define a generic positioning service in the facilities layer that will facilitate the development of applications. Positioning data coming from different sources is presented by this PVT facilities services to applications in a globally standardized form with an indication about the quality (accuracy, performance, authenticity) of the position.

The table below indicates the main standards related to the ITS station facilities layer considered in current European pilot deployments of Cooperative ITS services (as of 2018).

Table 02: ITS station facilities layer standards used in C-ITS deployments in Europe

Standard	Title
ETSI EN 302 637-2 (CAM)	Basic Set of Applications; Specification of Cooperative Awareness Basic Service
ETSI EN 302 637-3 (DENM)	Basic Set of Applications; Specifications of Decentralized Environmental Notification Basic Service
ETSI TS 102 894-2	Users and applications requirements; Applications and facilities layer common data dictionary
ETSI TS 103 301	Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services
ISO/CEN TS 19321 (IVI)	Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures
ISO/CEN TS 19091	Cooperative ITS - Using V2I and I2V communications for applications related to signalized intersections
ISO TS 14823	Traffic and travel information - Messages via media independent stationary dissemination systems - Graphic data dictionary for pre-trip and in-trip information dissemination systems

3.7 ITS station networking & transport layer

As shown in Figure 03, the ITS station networking & transport layer (SNT) can support a variety of networking protocols, including IPv6 (for networked communications), GeoNetworking (for localized communications in Europe), WSMP (for localized communications in North America), 6LoWPAN (for sensor networks). More networking protocols could be

added if needed. GeoNetworking (GN) and Basic Transport Protocol (BTP) have been developed for V2X broadcast communication at the network and transport layers. GN and BTP are combined to provide various network layer mechanisms to route packets in an ad-hoc and dynamically changing vehicular environment, including features like multi-hop and addressing based on geolocation.

In most other cases, an ITS station will be linked to other ITS stations and networked entities via IPv6, either a legacy IPv6 network or a proprietary IPv6 network. In some very specific cases like for instance direct localized communications between neighbour ITS stations using 802.11p / ITS-G5, IPv6 may be replaced by some ITS-specific networking protocol like GeoNetworking in Europe. The use of IPv6 in the context of the ITS station communication architecture is defined in [ISO 21210]. In pilot deployments of C-ITS services in Europe, GeoNetworking (GN) and Basic Transport Protocol (BTP) are the protocols currently used for V2X broadcast communication at the network and transport layers. GN and BTP are combined to provide various network layer mechanisms to route packets in an ad-hoc and dynamically changing vehicular environment, including features like multi-hop and addressing based on geolocation.

Table 03: ITS station network & transport layer standards used in C-ITS deployments in Europe

ETSI standard	Title
ETSI EN 302 931	Geographical Area Definition
ETSI EN 302 636-1	GeoNetworking; Requirements
ETSI EN 302 636-2	GeoNetworking; Scenarios
ETSI EN 302 636-3	GeoNetworking; Network Architecture
ETSI EN 302 636-4-1	GeoNetworking; Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Media-Independent Functionality
ETSI TS 302 636-4-2	GeoNetworking; Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Media-dependent functionalities for ITS-G5
ETSI EN 302 636-5-1	GeoNetworking; Transport Protocols; Basic Transport Protocol
ETSI EN 302 636-6-1	GeoNetworking; Internet Integration; Transmission of IPv6 Packets over GeoNetworking Protocols

3.8 ITS station access technologies layer

The ITS station access technologies layer comprises the access technologies used for communicating with other ITS station units, within the ITS station unit (i.e. between ITS station communication units of the same ITS station unit) and other legacy communication peers. Any given access technology can be integrated in the ITS station as long as it complies with the ITS station reference architecture. This requires the production of a specification that defines how the access technologies is integrated. The framework to follow is defined in [ISO 21218].

Currently supported access technologies include infrared [ISO 21214], microwave [IS 21215] (i.e. support for ETSI's ITS-G5 [ETSI 302-636-4-2] and IEEEE 1609), 802.15.4 (for 6LoWPAN) [ISO 19079], 60 GHz millimetre wave, cellular (2G/3G, LTE), satellite and wired access technologies (Ethernet). More access technologies could be supported in the future. Work items have already been opened at ISO to support LTE-D2D, LTE-V2X [ISO 17515-3] and optical communications.

[ETSI 302 571] defines the RED requirements for accessing the 5.9 GHz ETSI ITS-G5 standards. The two main functions required by the aforementioned standard is (according to Decentralized Congestion Control mechanisms and mitigation functions [ETSI 102 687] towards CEN DSRC (not the same as US DSRC!) Tolling stations [ETSI 102 792] in order to avoid radio interferences.

3.9 ITS station management entity

The ITS station management entity (SME) is in charge of all cross-layers functions including the management of the ITS station unit functionalities, management of the applications installed on the ITS station, management of the communication (communication profile, selection of the access technology and communication path, …). Security-related management operations are performed by the ITS station security entity, but this is just a conceptual view. The ITS station management entity functions are mostly specified by ISO TC 204 WG16 [ISO-24102]. ETSI TC ITS has also opened work items related to cross-layer functions and the ITS station management, in order to comply with the ITS standardization mandate M/453 from the European Commission. Related ETSI work items include Cross-layer architecture [ETSI 102-723-1].

The interactions between the ITS station management entity and the horizontal layers is performed via Service Access Points (SAPs) (see Section 3.11). [ISO-24102-6] (flow and path management) specifies the exchange of information between layers necessary to determine on which communication path, protocol and access technologies (Communication Flow Profile) packets of a given flow must be routed. This decision is performed by the SME after gathering application and user requirements [ISO 17423] and collecting networking information available at any layer of the ITS station (see Section 4.2).

3.10 ITS station security entity

The vertical ITS station security entity provides common security functionalities, performs the atomic security operations and stores credentials needed by security protocols and mechanisms implementing functions of the horizontal layer [ETSI 102-731]. The common security functionalities provided by the ITS station security entity include:

- Firewall and intrusion detection management;
- Authentication, authorization, and profile management;
- Identity, cryptographic key, and certificate management.

The HSM (Hardware Security Module) that records certificates used to secure C-ITS services is a functionality located in the ITS station security entity from a functional architecture viewpoint. Security credentials such as cryptographic keys, authorization tickets, and certificates are stored and maintained at the security entity with other security related parameters and status information. Upon request from horizontal layers, atomic security operations are provided by the security entity. Atomic security operations include:

- Arbitrary bit generation (for the pseudonym service);
- Hashing;
- Signing and verification;
- Encryption and decryption.

All V2X messages include cryptographically signed certificates, using pseudonyms to verify if a message has been changed since its original creation (and signature). V2X security currently uses asymmetric cryptography signatures station as defined in the standards indicated in Table 04. As defined in the General Data Protection Regulation (EU) 2016/679 Article 4 (5): a pseudonym is a cryptographic signed certificate, that corresponds to a public key certificate called *Authorization Ticket*. The authorization ticket represents the ITS station, without revealing the identity of the vehicle or its driver.

Table 04: ITS station security entity standards used in C-ITS deployments in Europe

ETSI standard	Title
ETSI TS 103 097	Security; Security header and certificate formats
ETSI TS 102 941	Security; Trust and Privacy Management

3.11 ITS station service access points (SAP)

The functional blocks of the ITS station communication architecture are interconnected via high-level Service Access Points (SAPs) as presented in Table 05. However, these SAPs are not necessarily followed in all C-ITS standards (particularly not ETSI standards) nor by implementers as they are not useful for proprietary implementations of the ITS station functionalities into a single ITS-SCU. There are thus of limited use.

Table 05: ITS station reference architecture – Service Access Points (SAP)

SAP (Service Access Point)	Purpose	Description
MI	Management	SAP allowing the interaction between the ITS station management entity (SME) and the ITS station access technologies layer (SAT)
MN		SAP allowing the interaction between the ITS station management entity (SME) and the ITS station networking & transport layer (SNT)

MF		SAP allowing the interaction between the ITS station management entity (SME) and the ITS station facilities layer (SFL)
MA		SAP allowing the interaction between the ITS station management entity (SME) and the ITS station applications
SI	Security	SAP allowing the interaction between the ITS station security entity (SSE) and the IITS station access technologies layer (SAT)
SN		SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station networking & transport layer (SNT)
SF		SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station facilities layer (SFL)
SA		SAP allowing the interaction between the ITS station security entity (SSE) and the ITS station applications
IN	Interaction between layers	SAP allowing the interaction between the ITS station access technologies layer (SAL) and the ITS station networking & transport layer (SNT)
NF		SAP allowing the interaction between the ITS station networking & transport layer (SNT) and the ITS station facilities layer (SFL)
FA		SAP allowing the interaction between the ITS station facilities layer (SFL) and the ITS station application layer

[ISO-24102-1] defines the services provided by these Service Access Points between the ITS station management entity and the horizontal layers. For the ITS station network and transport layer, these are:

- MN-COMMAND: Sending a command to the ITS station networking & transport layer, using the following primitives:
    - MN-COMMAND.request: this management service primitive allows the ITS station management entity (SME) to trigger an action at the ITS station networking & transport layer.
    - MN-COMMAND.confirm: this management service primitive reports the result of a previous MN-COMMAND.request.
- MN-REQUEST: Receiving a request (command) from the ITS station networking & transport layer, using the following primitives:
    - MN-REQUEST.request: this management service primitive allows the ITS station networking & transport layer (SNT) to trigger an action at the ITS station management entity (SME).
    - MN-REQUEST.confirm: this management service primitive reports the result of a previous MN-REQUEST.request.

ISO 24102 [ISO-24102-1] indicates that both MN-COMMAND and MN-REQUEST supports up to 256 possible SAP functions.

3.12 Implementing ITS stations

It is of course not required for a given deployment of an ITS station to implement neither all these functionalities nor to implement the specific functions required to support all these functionalities. So, the purpose of the standard is to specify how a given technology or functionality, if needed, can be integrated into the ITS station. It will be the purpose of deployment specifications to define what functionalities are needed according to the deployment environment and needed services.

4. ITS station functionalities in support for hybrid communications

Hybrid communications has no strict definition and may be interpreted differently from different sets of stakeholders. For some, it merely means the combination into a single communication system of a short-range access technology used for localized communications (e.g. ITS-G5) with a long-range communication technology used for cloud connectivity (e.g. cellular). For others it means the ability to deploy the same Cooperative ITS services either using localized communications or cellular-based communication. For yet another group, it means having two systems cohabitating in silos, one with short range communications for a limited set of services (time critical road safety) and one with long-range communication capabilities for another limited set of services (infotainment, telematics, non-time critical road safety). For the group of ISO TC204 people whom has developed the initial concept of the ITS station architecture, it means an optimized integration of various access technologies in order to provide extended connectivity in a technology-agnostic fashion to a range of applications with different and varying communication means over time.

It is obvious that the long-term view towards connected and cooperative vehicle is the combination of multiple access technologies into a single communication system (possibly duplicated for redundancy, or spread in multiple communication units complying to the same communication architecture) to offer connectivity to a diversity of applications with varying communication needs and in environments with varying connectivity quality. Achieving this long-term view requires a high level of security in order to prioritize the use of resources (CPU, energy, bandwidth) for which many applications are competing in parallel. This chapter presents the State of the Art in the development of the Cooperative ITS standards in which SECREDAS needs to comply with and contribute.

4.1 Connectivity maintained through multiple access technologies

Figure 010 illustrates a situation where a vehicle may have different options to choose from in order to communicate with a communication peer. In this example, the communication peer is another vehicle. Data could be exchanged using localized communication (ITS-G5 / IEEE 802.11p), urban WiFi (IEEE 802.11n) or cellular. One of the communication paths may be more appropriate, depending on the type of transmission. For V2X road safety like emergency breaking, ITS-5G / 802.11p is probably best (in broadcast mode) with repetition of the message a few times per second. For a short duration video transmission 802.11n may be best, while the cellular link is probably the only option for a long duration session between the two vehicles which may be split apart due to traffic.

ISO standards have been developed from the start, with the motivation to combine multiple access technologies in order to allow these three types of data exchange to happen simultaneously, on a single communication system gathering multiple access technologies, with priorities allocated to road safety over less time-critical data flows.

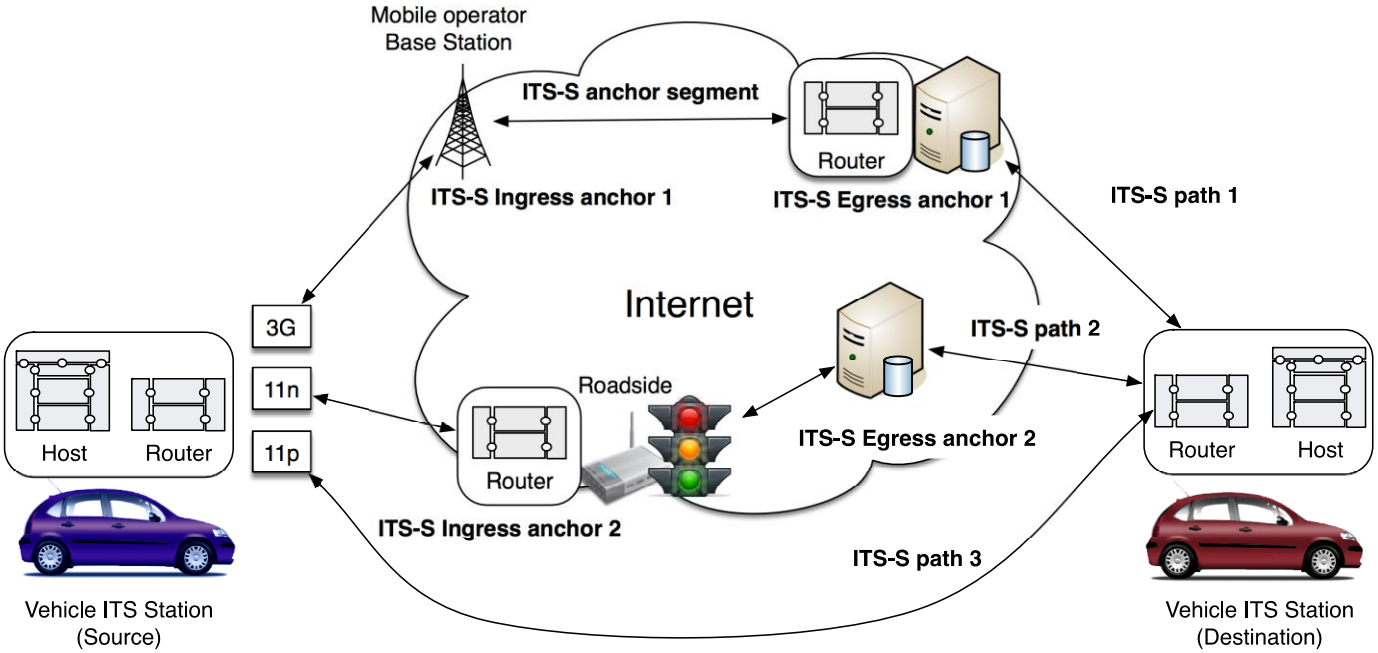

Figure 010: Multiple communication paths (ISO 24101-6)

These access technologies can be combined and used simultaneously or one after the other in order to provide more efficient and better connectivity. However, the mechanisms available to maintain connectivity and offer seamless or resilient connectivity require information about the quality of the surrounding access networks, the capabilities of the communication systems, and the needs of the applications. ISO TC204 has therefore developed a cross-layer communication management mechanism that collects communication requirements from the applications (ITS-S application process) and various communication parameters internally to the ITS station and from the surrounding networks.

The functionalities needed in the ITS station are specified in a set of inter-related ISO standards (mainly [ISO 17423, ISO 17429, ISO 24102-6). Most of these functionalities are inspired from earlier work conducted by the ITSSv6 project [ITSSv6]. The functionalities include:

- A mechanism allowing the ITS-S application process to inform the ITS station management about its communication requirements (communication profile) and other constraint for each data flow.
- A mechanism allowing the ITS station layers to provide various information about the capabilities of the layer (what functionalities are supported and their status) and about the conditions of the available surrounding networks.

- A mechanism allowing the ITS station management to determine what data flow can be transmitted on what available access networks.

A technical report [ISO 21186] is currently being prepared to describe the relevant standards for hybrid communications.

4.2 Data flow management in an ITS station

Each application may indeed transmit several data flows with different flow characteristics. As example: a voice flow and a video flow when considering a video-conferencing application; a traffic hazard application may have a broadcast flow (time-critical broadcast to nearby vehicles) and a unicast flow (non-time-critical notification to a traffic control centre). Since all applications running on an ITS station compete towards the use of a limited set of common resources (CPU, bandwidth, connectivity, …), it is necessary to manage their needs and priorities. [ISO 24102-6] and [ISO 17423] thus specify a mechanism allowing ITS-S application processes to inform the ITS station management about communication requirements for all data flows that may be initiated.

These application flow requirements are provided to the ITS station management entity so that it can determine the appropriate Communication Flow Profile (CFP) for each flow according to the capability of the ITS station to transmit the information. The CFP determines the appropriate protocol stack (e.g. IPv6 or non-IP, ITS-G5 or cellular, non-safety or safety channel, …) within the ITS station and the communication path (e.g. the access technologies) that should be used to route the packets. Each instance of an ITS-S application process indicates its communication flow requirements, using the methods specified in [ISO 17423, ISO 17429, ISO 24102-6]. In addition, ITS-S application processes can subscribe to specific data sets and services provided by the ITS station facilities using the methods specified in [ISO 17429] (see Section 3.6). If needed, a specific Communication Flow Profile may also be directly enforced by the ITS-S application process. This may occur in case regulation and deployment choices require the use of a specific communication interface.

The ITS SME is in charge of all cross-layers functions including the selection of the communication path selection based on pre-set policies, regulations, static and dynamic capabilities of the different access technologies. The ITS SME is responsible for the selection of the best communication path (communication interface and end-node) according to the application flow requirements expressed by the applications (ITS-S application processes), the capabilities of the ITS station, the access technologies characteristics and the current network conditions. The ITS SME must thus interact with the horizontal layers in order to make this determination and more particularly with the ITS station networking & transport layer (SNT) that must update its forwarding tables according to rules provided by the ITS SME. This is illustrated in Figure 03 below. As a result of the availability of multiple access technologies, the ITS SME is able to support different types of handover, including:

- Handovers involving a change of the point of attachment to the network without a change of access technology;
- Handovers involving a change of the point of attachment to the network with a change of access technology;
- Handovers involving reconfiguration or change of the network employed to provide connectivity; and
- Handovers involving both a change of the point of attachment to the network and network reconfiguration.

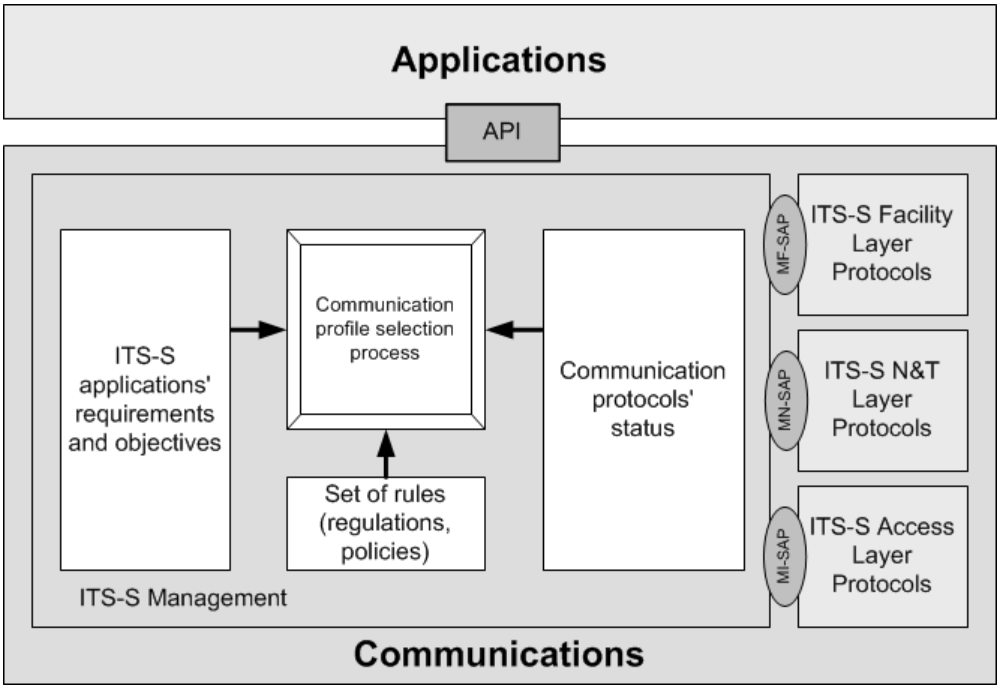

Figure 011: ITS station communication management (ISO 24101-6)

4.3 ITS station unit using IPv6

[ISO 21210] specifies how IPv6 network protocols and services should be used in the context of the ITS station reference architecture. Essentially, this specification describes how IPv6 must be configured to provide global reachability and continuous Internet connectivity of an ITS station unit. [ISO 21210] doesn't define a new protocol, a new exchange of messages at the IPv6 layer, or new data structures. It defines which and how standard IETF protocols are combined so that ITS station units can communicate with one another using the IPv6 family of protocols.

In [ISO 21210], IPv6 features are arranged into a set of modules performing a subset of the required functions. The arrangement of the IPv6 protocol block into modules allows to easily specify what is the minimum set of modules to be implemented for each type of IPv6 node composing an ITS station unit. Considering the different types of ITS station units shown on Figure 04, the following ITS-S IPv6 nodes could exist:

- In the vehicle ITS station unit, the nodes executing the ITS-S router functions are the ITS-S IPv6 vehicle routers (VRs). The ITS-S host functions may be implemented by the ITS- S IPv6 router, or by ITS-S IPv6 hosts. Vehicle

ITS-S IPv6 routers and hosts are also known as mobile routers (MRs) and mobile network nodes (MNNs) when continuous Internet connectivity is supported.

- In the roadside ITS station unit, the nodes executing the ITS-S router functions are the ITS-S IPv6 roadside routers (RRs) and the ITS-S IPv6 border routers (BRs). Roadside ITS-S IPv6 routers are also known as the ITS-S IPv6 access router (AR) when they provide access to ITS-S IPv6 mobile router (MR). border routers (BRs) are the ITS-S IPv6 routers connecting the ITS station to the Internet or other ITS stations. The ITS-S host functions may be implemented by an ITS-S IPv6 router, or by ITS-S IPv6 hosts.

- In the central ITS station unit, the nodes executing the ITS-S router functions are the ITS- S IPv6 border routers (BRs) connecting the ITS station to the Internet or other ITS stations and the ITS-S home agents (HAs) for supporting IPv6 mobility. The ITS-S host functions may be implemented by an ITS-S IPv6 router, or by ITS-S IPv6 hosts.

In the context of IPv6 networking, the terms ITS-S gateway is generally meant for an IPv6 host, while the ITS-S router could be an IPv6 access router (AR), and IPv6 border router (BR), an IPv6 mobile router, or a home agent (HA).

4.4 Connectivity management using IPv6

This Section describes the procedures within the ITS station networking & transport layer (SNT) to allow an ITS station unit to maintain continuous IPv6 connectivity while changing its point of attachment to the network. This is ensured by the IPv6 mobility support module within the IPv6 protocol block. The IPv6 mobility support module comprises mechanisms for maintaining IPv6 global addressing, Internet reachability, session connectivity and media-independent handovers (handover between different access technologies) for in-vehicle networks. This module mostly combines Network Mobility Basic Support [RFC 3963] and Multiple Care-of Addresses Registration (MCoA) [RFC 5648]. The functionalities described in this Chapter have been integrated in [ISO 21210]. A proof of concept implementation has been developed by the ITSSv6 project, based on earlier implementations. The interaction of the IPv6 protocol block with the ITS station management is performed through a service access point (SAP) defined in [ISO 24102.6] “Path and Flow management”.

4.4.1 IPv6 network mobility support (NEMO)

Network Mobility Basic Support [rfc3963] is designed to maintain Internet connectivity between **all nodes in a moving entity** and the infrastructure (this is called “*network mobility support*”). This is performed without breaking the data flows under transmission, and transparently to the nodes located behind the MR (MNNs) and the communication peers (CNs). This is handled by mobility management functions in the MR and a server known as the HA (*Home Agent*) located in an IPv6 subnet known to the MR as the *home IPv6 link*.

The key idea of NEMO is that the IPv6 *mobile network prefix* (known as MNP) allocated to the MR is kept irrespective of the topological location of the MR while a binding between the MNP and the newly acquired temporary *Care-of Address* (CoA) configured on the external IPv6 egress connecting the MR to the Internet is recorded at the HA. This registration is performed by the MR at each subsequent point of attachment to an AR. In order to do this, the MR is using its global address known as the *Home Address* (HoA). This allows a node (ITS-SCU) in the vehicle to remain reachable at the same IPv6 address as long as the address is not deprecated. The HA is now able to redirect all packets to the current location of the vehicle. MNNs attached to the MR do not need to configure a new IPv6 address nor do they need to perform any mobility support function to benefit from the Internet connectivity provided by the MR. This mobility support mechanism provided by NEMO is thus very easy to deploy, at a minimum cost.

The tunnel between the MR and the HA may be implemented as a virtual IPv6 interface pointing to a physical egress interface (*external IPv6 interface*) where packets would be encapsulated. Such an IPv6 virtual interface would then be treated by the routing module as the physical external IPv6 interface. The same rules would thus be applied to the selection of the MR-HA tunnel (this corresponds to the IPv6 forwarding module in [ISO 21210]. The earlier Mobile IPv6 mobility support specification [RFC 3775] provides Internet connectivity to a single moving IPv6 host only (IPv6 host mobility support). Mobile IPv6 is therefore inappropriate for the most advanced ITS UCs which usually consider more than one in-vehicle embedded CPU (i.e. an ITS station unit made of several ITS station communication units).

Network mobility support using RFC 3963 also supports situations where there would be only a single IPv6 node deployed in the vehicle. Indeed, the ability to support an entire network of *n* nodes includes the ability so support a network of 1 node only. So, applying NEMO Basic Support instead of Mobile IPv6 will make the solution future proof. This is the reason why NEMO Basic Support is recommended in [ISO 21210] for Cooperative ITS services complying with the ITS station reference communication architecture. The operation of NEMO Basic Support is illustrated Figure 012.

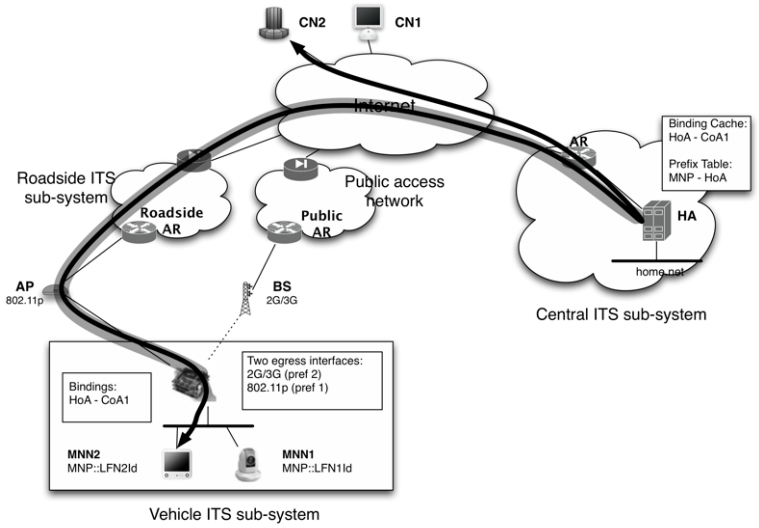

Figure 012: IPv6 session continuity with NEMO Basic Support (RFC 3963 / ISO 21210)

For a better understanding of NEMO, the terminology is specified in [RFC 4885] and the design goals behind NEMO Basic Support in [RFC 4886]. These documents are normative documents on how to apply NEMO Basic Support to the ITS station architecture.

4.4.2 IPv6 mobile edge multihoming (MCoA)

[RFC 5648] is an extension to Mobile IPv6 [RFC 3775] and NEMO Basic Support [RFC 3963] and allows a MR to register multiple Care-of Addresses (CoA) with its HA. As a result of the notification of the tunnel set-up from the IP mobility management module to the ITS SME, the ITS SME should notify the IPv6 forwarding module with new forwarding table entries. See in [ISO 21210] the description of the IPv6 forwarding module. Different approaches have been proposed at the IETF in the former MEXT Working Group for the MR and the HA to synchronize their decisions in choosing the appropriate medium [RFC 6088] and [RFC 6089]. One such approach is to exchange rules (routing policies) using NEMO signalling messages; another is more generic and uses standard transport layer protocols. The rules for performing handovers and medium switching are configurable by stakeholders, e.g. users, device vendors, service providers, car manufacturers. These rules are competitive factors among stakeholders, so the definitions of these rules are outside the scope of the standards related to the ITS station reference communication architecture. The operation of MCoA is illustrated in Figure 013.

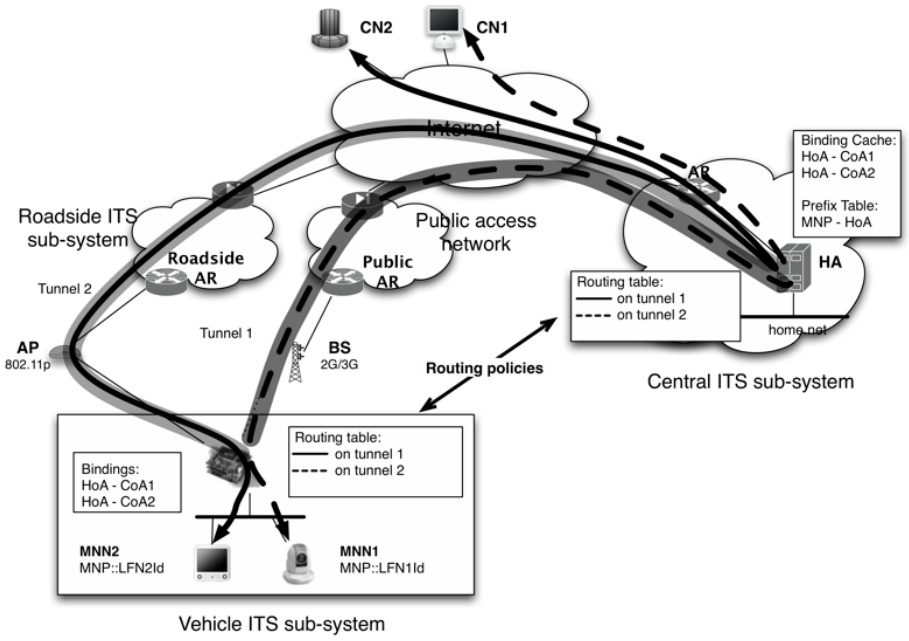

Figure 013: IPv6 mobile edge multihoming (RFC 5648 / ISO 21210)

5. Secure communications

5.1 Services requiring security

Services that require security include the following:

- Real-time access to time critical vehicle data (collision avoidance, emergency brake, …);
- Real-time data exchange for road traffic management (green wave information, priority lane access management, interactive optimum vehicle settings to minimize fuel consumption, …);
- Protection of personal data in compliance with the European “General Data Protection Regulation” (GDPR);
- Service, repair and maintenance of electronic components of the vehicle;
- Semi-automated or automated driving (regulated speed, platooning, remote driving…);
- Remote management of ITS station and software update;
- Value added services (electric charging, parking.

These services may require short-range localized communication between vehicles, roadside equipment and road users in the vicinity, or long-range distant communications with control centres and service platforms. The communications may be broadcast (one to many) or session-based (point-to-point). Moreover, some communications may just require authentication and integrity, while others may require strict confidentiality. In any case, location privacy of users must be ensured, by regulation. Appropriate security mechanisms must thus be put in place and must be integrated in communication protocols and communication devices.

5.2 Public Key Infrastructure (PKI) for identity management

The majority of information exchanged for Cooperative ITS services is critical. Ensuring integrity and authenticity of this information is a prime concern. If an actor is enabled to forge or modify a message, it could end up with incorrect information used in other computations. This kind of miss-behaviour would result in lowering the quality of a functionality and could potentially even endanger road users. To resolve this problem, each received message must be checked for authenticity and integrity.

A Public Key Infrastructure (PKI) is used to manage identities. It is called « public », because it is based on public cryptography which is also called asymmetric cryptography. This kind of cryptography uses key pairs (public and private keys) particularly effective for authentication. It is possible to encrypt a message using a private key and send it; all receivers will be able to verify that it is the sender’s message, as only the sender’s public key can decrypt it. This process is called signature. The pair of keys assures the sender’s identity and each identity corresponds to an entity. Each message can thus be associated to a known entity and if the message cannot be verified, it should be dropped.

However, as each transmitted message or data can be associated to an entity (ITS station, ITS station application process, ITS station functionality, etc.), critical information like vehicle position, speed, etc. can be uniquely associated with a given vehicle. It is then possible to follow the information associated to that entity, allowing third parties to track its movements and thus its owner. This kind of tracking and control would constitute a user privacy violation. The PKI system used to secure Cooperative ITS service (C-ITS PKI) must thus adopt a specific mechanism ensuring privacy.

The C-ITS PKI system defined in [IEEE 1609.2, ETSI 102-941 and ETSI 103-097] uses an entity authentication in two steps:

- Long-term authentication (**Enrolment**);
- Short-term authentication (**Authorization**).

Enrolment Credentials are used to identify the entity on the long term, allowing it to replenish its Authorization Tickets (AT). ATs are disposable credentials used for a short duration before being thrown away and replaced by new ones.

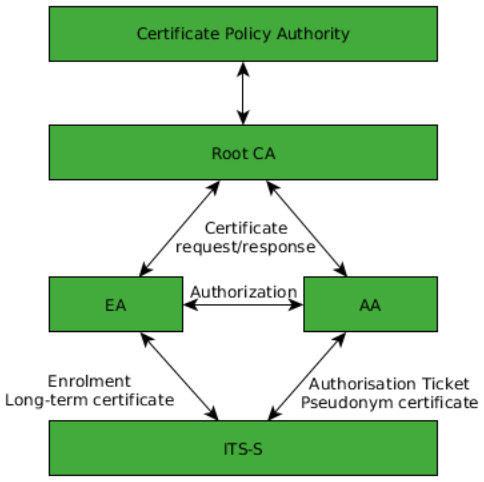

Figure 014: *PKI basic authorities and ITS-S registration basic messages*)

Certificates are used to identify entities.

Enrolment Authority

- Allow to obtain long-term identity;
- Identifies the ITS station;
- The ITS station must be registered before using the PKI.

Authorization Authority

- Allows to obtain pseudonyms (AT);
- Part of the authorization request if forwarded to the EA for identity approval;
- AT are used to encapsulate messages exchanged between ITS stations.

Root CA

- Allows ITS stations to authenticate authorities verifying their certificate chain;

- Distributes EA/AA Certificates;
- Distributes CRL (to keep invalided certificates so they can never be used again).

TLM

- Provides a list of trusted Root Certificates representing the PKI provider;
- Provides ECTL to CPOC for distribution.

CPOC

- Distributes ECTL (provides list of trusted root certificates);

C-ITS Certificate Policy Authority

- Physical organism charged to deliver Root Certificates to PKI providers;

Manufacturer / Operator

- Charged to register ITS station to chosen PKI provider(s);
- Provides ITS-S technical key (first enrolment key).

As illustrated in Figure 015, multiple PKI providers are likely to be deployed in order to fulfil scalability, regional requirements and industry requirements:

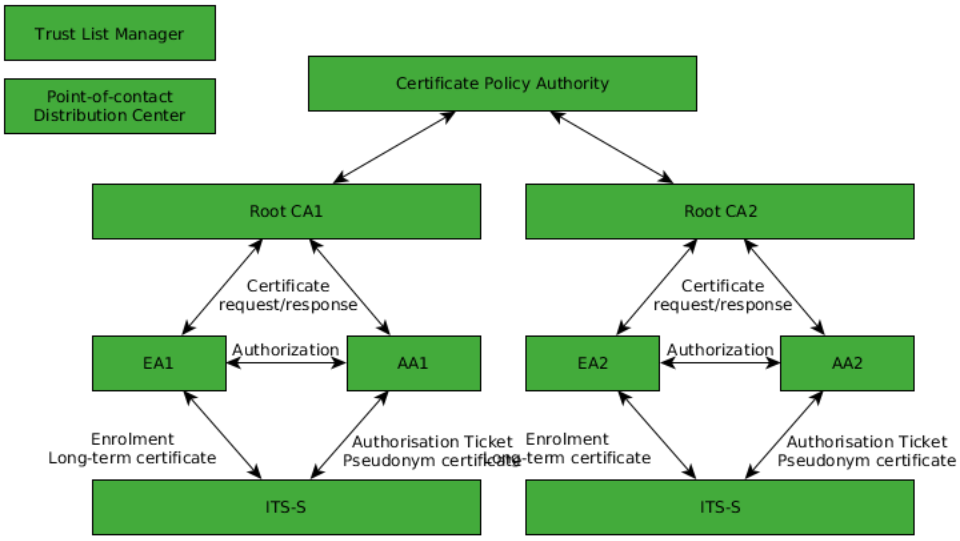

Figure 015: *Multiple PKI providers*

The PKI process is illustrated in Figure 016 below. The Root certification Authority supervises and establishes trust between the enrolment and the authorization authorities. In Europe, it is foreseen that there will be more than one RootCA, e.g., different roots may exist for vehicles and for roadside equipment. Both types have already been used in the context of pilot deployments of Cooperative ITS services.

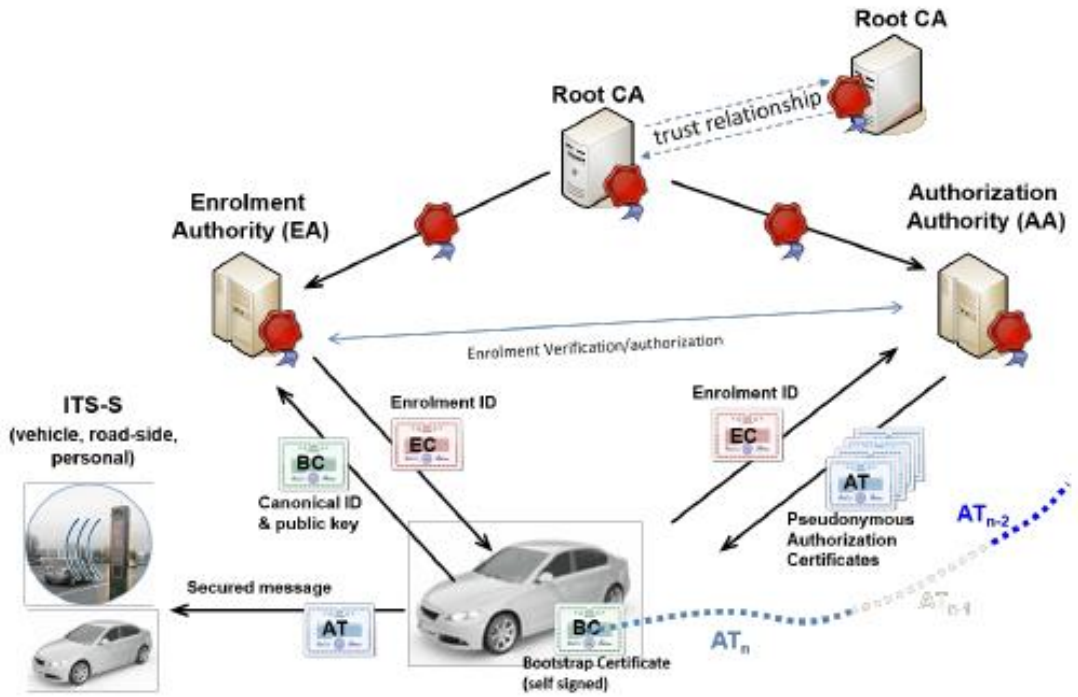

Figure 016:*Public Key Infrastructure (PKI)*[8]

The Enrolment Authority provides Enrolment Certificates (also called as long-term certificates) to ITS stations that are part of the system (e.g., vehicles which have passed Compliance Assessment tests). These certificates are then used to hide the identity of the vehicle/ITS-S by using it instead of its ID. The certificates used during V2X are provided by the Authentication Authority and are called authorization ticket. They are also standardized in Security Header and Certificate Formats [ETSI TS 103 097], as listed above) and they are also sometimes referred to as short-term certificate or pseudonym certificate. They represent the proof that the system knows that ITS station. The Authentication Authority provides ACs to vehicles which are verified using their EC by the EA. New certificates are required as they expire. The PKI also allows the so-called Revocation of Trust, meaning that misbehaving ITS stations are removed from the system by listing them as untrusted (revocation list) and also by disabling the provision of valid certificates (and their certificates will expire).

5.2.1 Example of enrolment request

1. The ITS station provides its identity and EC candidate public key.
2. It signs this data with the candidate private key to prove it possesses the key pair for which enrolment is asked.
3. It signs with its current EC (or registration key = technical key) to prove its claimed identity.
4. It encrypts using a freshly generated symmetric key.

[8] (Curtesy of: Cooperative ITS Security Framework: Standards and Implementations Progress in Europe by Brigitte Lonc and Pierpaolo Cincilla)

5. The encryption key is encrypted with the authority public key and concatenated to the message. So that only the authority can retrieve the key and decrypt the message.

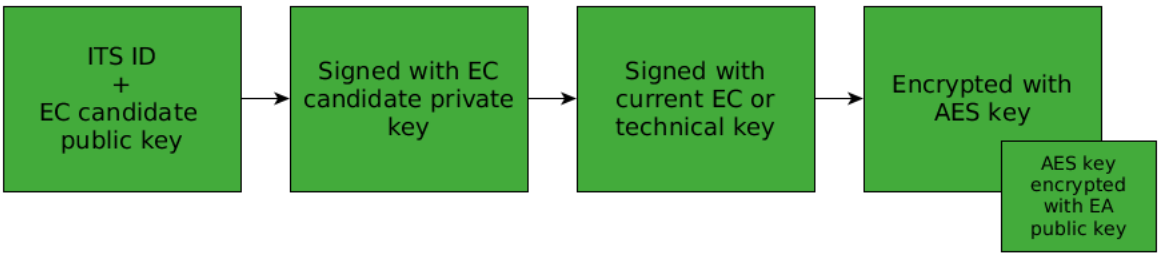

Figure 017: *Enrolment request message structure (example)*

5.2.2 Example of enrolment response

1. The message contains the asked Enrolment Credentials (if the request has been validated.
2. The authority signs the message with its private key to prove its claimed identity.
3. The authority encrypts the response with the symmetric key used for the request.

The new Enrolment Credentials are ready to be used by the ITS station to obtain Authorization Tickets.

Figure 018: *Enrolment response message structure (example)*

5.2.3 PKI integration in the ITS station reference architecture

The PKI enrolment and authorization processes take place at the time of the security activation and every time credentials or tickets need to be renewed by an ITS station. Certificates are requested to PKI servers hosting the relevant authorities. Once the ITS-S possesses AT, it can start using them to encapsulate messages; depending on the security profile, messages can be signed, encrypted and signed and encrypted. This encapsulation is executed in the ITS station networking & transport layer of the functional communication architecture. Private keys are stored on the HSM, a tamper resistant device allowing to securely store and manipulate private keys.

The ITS station security entity is charged to handle enrolment requests and response. The ITS-S creates Enrolment Credentials key pair and the public part is sent to the EA. The authority then answers with the certificate created from the public key. The ITS-S can store it for future use while the private key is stored in the HSM. When the enrolment is finished, the station can start the authorization request and response. Once again, the ITS-S generates the candidate AT key pair and the authority answers with certificates derived from the public key provided by the ITS station. The certificate is stored and can be used for packet encapsulation while the private resides within the HSM.

The AT certificates and private keys addresses within HSM are to be forwarded to the network layer in order to proceed with message encapsulation. When a CAM or DENM message to be sent is forwarded from the facilities to the network layer, it is encapsulated using AT. For example, the message is signed and placed in the ASN.1 data structure before being COER encoded and processed by the network layer as usual. This encapsulation is called security header and is configured using security profiles.

5.3 Security between trusted devices and applications

Security services needed in the ITS station to ensure secure information exchange between ITS station communication units (ITS-SCU) are defined in [ISO 21177]. ISO 21177 defines security services to establish trust between ITS station communication units (ITS-SCU) and to establish trust between ITS station units (ITS-SU). Those security services include authentication and secure session establishment.

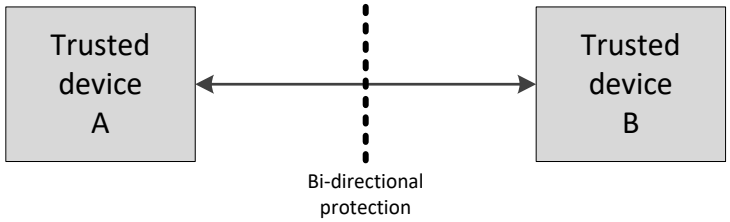

Figure 019: Bi-directional protection between trusted devices (ISO 21177)

When it comes to the in-vehicle sensor and control network (IVN), trust must be established between the ITS station unit and the IVN via an interface, as illustrated in Figure 020. This interface may be part of the ITS station unit, or part of the IVN, or a standalone device.

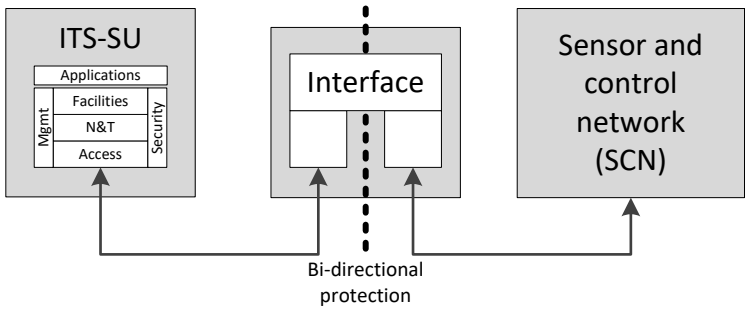

Figure 020: Bi-directional protection between an ITS station unit and the internal sensor and control network (ISO 21177)

Applications running in an ITS station unit need to exchange data with applications running on the same ITS station unit, or on a peer ITS station unit, or on a device that is not in compliance with the ITS station reference architecture (e.g.in the sensor and control network, or on a personal device or a server in the Internet). However, it is assumed that as a minimum the ITS-S application process is issued with a certificate by a trustworthy Certificate Authority (CA) that

also ensures that certificates are issued to ITS-S application process residing on ITS station units that meet the security requirements for that application

[ISO 21177] contributes mainly the following:

- Specify ITS station security services for enabling trust between ITS-S application processes running on different ITS-SCUs of the same ITS-SU, i.e. establishing a trusted processing platform, considering also trust inside an ITS-SCU:
    - Protection of applications from the actions of other applications;
    - Protection of shared information;
    - Protection of shared processing resources such as communications software and hardware, which includes methods of prioritisation and restricted access.
- Specify ITS station security services for enabling trust between ITS-S application processes running on the same ITS-SU.
- Extend these ITS security services for enabling trust between an ITS-SCU and devices being part of a sensor and control network.

Such security services include e.g. the basic security features of:

1. Authentication and authorisation;
2. Confidentiality and privacy;
3. Data integrity;
4. Non-repudiation.

Tasks related to communications are:

1. Establishing secure sessions for bi-directional communications, e.g. based on service advertisement specified in [ISO 22418].
2. Authenticating a sender of broadcast messages, e.g. CAM, DENM, BSM, SPaT, MAP, FSAM, WSA, ...
3. Encrypting messages.

Tasks 2. and 3. above related to communications are already specified in other standards, see e.g. IEEE Std. 1609.2TM and several related standards from ETSI TC ITS.

The functional security architecture specified in [ISO 21177] and shown in Figure 021 below, is designed to accomplish the following goals:

- Two peer ITS-S application processes can communicate securely, i.e. in an authorized, integrity protected and confidential manner.
- The ITS-S application processes can authenticate to each other using role- or attribute-based access control.

- Each individual incoming application protocol data unit (APDU) can be subject to individual access control processes.
- The security state of the connection (i.e. the authentication status of one ITS-S application process with respect to access to the other connection) can be updated within the secure session as follows.
    - An ITS-S application process can prove to the other that it knows a shared secret (Enhanced Authentication, – the intended use of this is to allow the owner or other legitimate operator of one ITS-S application process to permit access by a specific peer ITS-S application process.
    - An ITS-S application process can provide additional authentication within the secure session – for example to provide an identity as well as application permissions, or to provide additional application permissions.
- Secure session communication uses the same credentials as ITS-S application processes use.
- An ITS-S application process can configure a secure session so that it terminates under specific conditions (e.g. timeouts of different kinds) and can also terminate the secure session directly.
- To allow secure and private service discovery, the initialization stage (the “handshake”) of one secure session between two peer ITS-S application processes can be proxied over an existing secure session between two different peers.

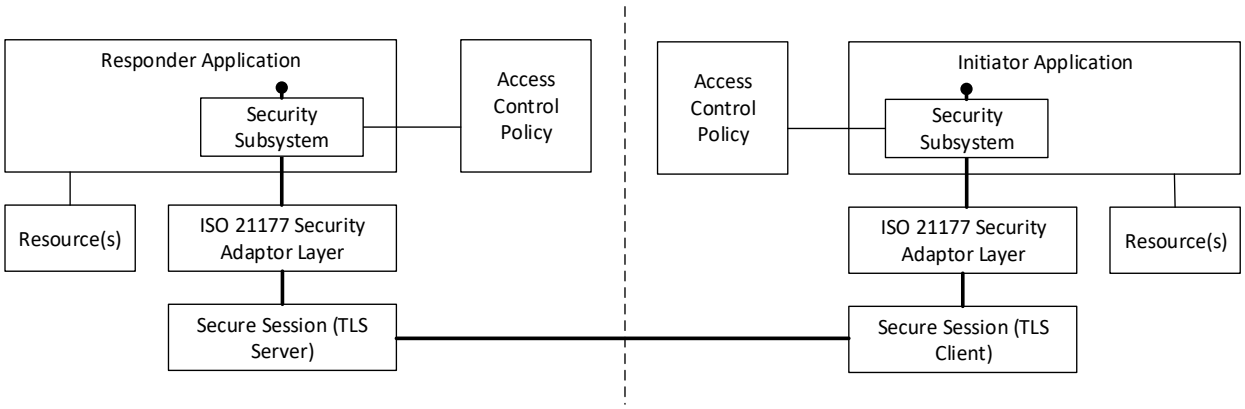

Figure 021: Functional security architecture (ISO 21177)

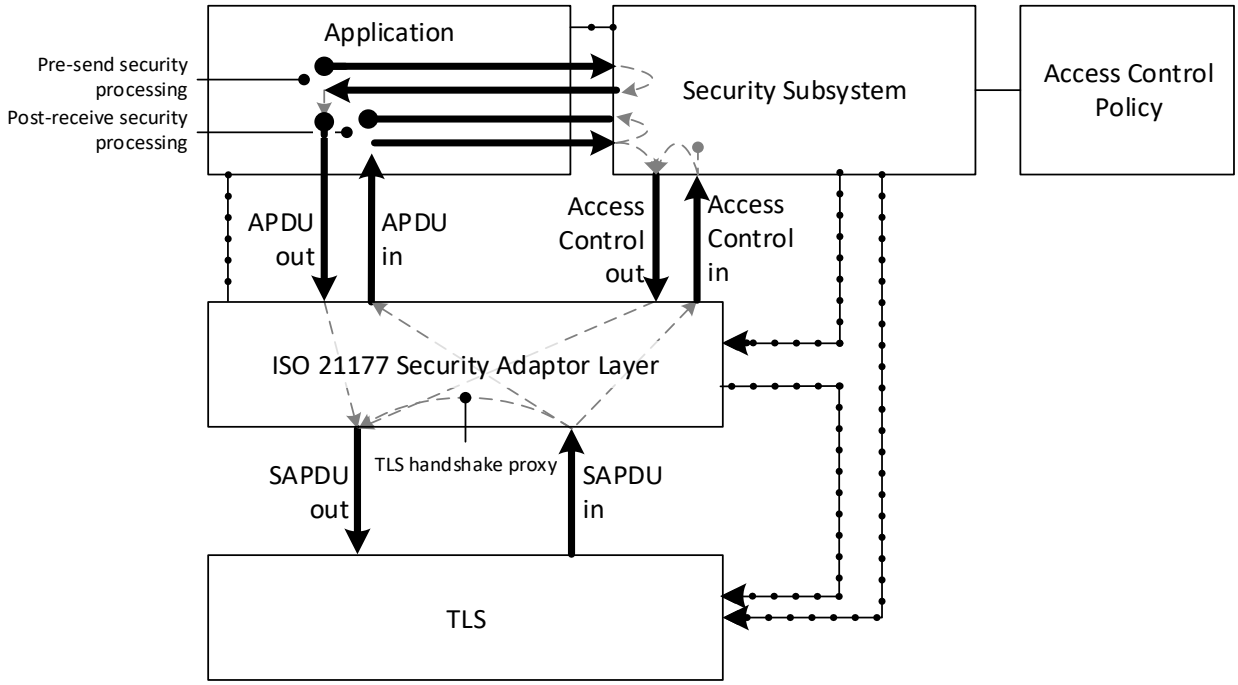

Figure 09: Interaction between functional security components (ISO 21177)

6. Conclusions

D5.1 "*Initial ITS station architecture with functional security features*" is the first output of WP5 (T5.1). This document will be continuously improved until the end of the WP5 at month 3 and will be presented as D5.12 "*Final ITS station architecture with functional security features*".

The purpose of the initial analysis presented in D5.1 is to shed light on the existing functional ITS station communication architecture and related Cooperative ITS standards and to share this knowledge internally within SECREDAS. It will serve within SECREDAS as the reference document guiding WP1 Use Case definitions, WP5 development, WP9 demonstrations and WP10 contributions related to Cooperative ITS standards. It will serve as the main input from WP5 to analyse how SECREDAS secure elements developed in WP3 can fit into the functional ITS station communication architecture, and how the security of communications can be improved in compliancy with functional ITS station communication architecture. The final conclusions of all this analysis will be presented in D5.12.

From the current state of the analysis of existing standards, we can observe that Cooperative ITS standards are already integrating security features. Localized and broadcast V2X communications using ITS-G5 include security features to ensure location privacy of the vehicle users and authenticity and integrity of the broadcast messages. More recently, a functional security architecture has been developed to ensure sessions organized between peer ITS stations are set up securely, therefore guaranteeing secure connectivity and remote access to embedded sensor and control networks data (CAN bus or sensor network in the case of a vehicle ITS station, but also a magnetic loop or other mechanisms in the case of a roadside ITS station). This access is managed through an ITS station gateway providing bi-directional protection between the communication system in charge of managing external connectivity and the embedded control and sensor network, as shown on Figure 022).

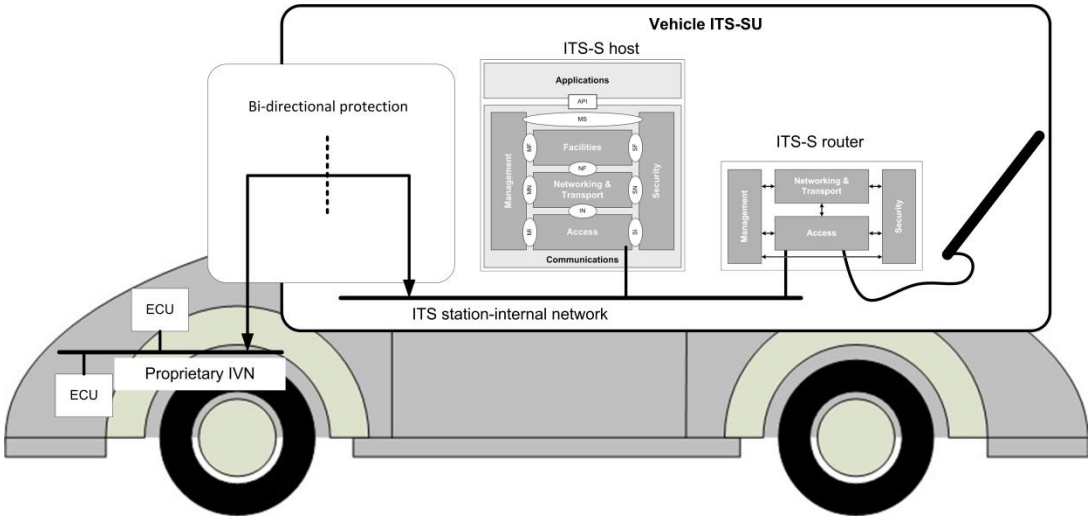

Figure 022: Functional security architecture (ISO 21177)

This functional security architecture will actually provide an answer to security threats addressed by the SECREDAS project. However, as it could be directly seen on the figure, the ITS station gateway functionality is seating at the corner stone between WP4, WP5 and WP6 and is thus in the scope of the three WPs[9]. In order to ensure interoperability and convergence of the SECREDAS work, concrete developments in both WP4, WP5 and WP6 must adopt the same approach.

We also observe that the Cooperative ITS standards are designed to specify functional elements, and not to specify how these functional elements are implemented. SECREDAS's high level security architecture must now be mapped to the functional ITS station architecture taking into consideration the functional security architecture recently proposed in Cooperative ITS standards. This will lead to recommendations on implementations of security functions into communication systems complying with the ITS station communication architecture.

[9] Note that the need for the ITS station gateway functionality was identified at the earliest development of the standards, but it has been specified only recently. Real work started in spring 2018, just before SECREDAS started.

Figures

Tables

References

C-ITS Platform 1
C-ITS Platform Final Report, January 2016
https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf

C-ITS Platform 2
C-ITS Platform Final Report Phase II
September 2017 (https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf)

C-ROADS
C-ROADS reference documents
https://www.c-roads.eu/platform.html

ETSI 101 607
Intelligent Transportation Systems (ITS); Cooperative ITS (C-ITS); Release 1. ETSI Technical Report 101 607 V1.1.1. May 2013

ETSI 102 637
Intelligent Transportation Systems (ITS); Vehicular Communications; Basic Set of Applications. ETSI Technical Specification 102 637

ETSI 102 637-2,
Intelligent Transport Systems (ITS) — Vehicular Communications — Basic Set of Applications — Part2: Specification of Cooperative Awareness Basic Service. ETSI Technical Specification 102 637-2

ETSI 102 637-3,
Intelligent Transport Systems (ITS) — Vehicular Communications — Basic Set of Applications — Part2: Specification of Decentralized Environmental Notification Basic Service. ETSI Technical Specification 102 637-3.

ETSI 102 638
Intelligent Transportation Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. ETSI Technical Report 102 638 V1.1.1. June 2009.

ETSI TS 102 687
Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part. ETSI Technical Specification 102 687 v1.1.1. July 2011

ETSI 102 723-9,
Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 9: Interface between security entity and facilities layer

ETSI 102 792
Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range. ETSI Technical Specification 102 792.

ETSI 102-890-2

Intelligent Transportation Systems (ITS); Facilities layer function; Part 2: Facility Position and Time management and Geolocation referencing service. ETSI TS 102 890-2 V0.0.6 (Early Draft).

ETSI 102-894-2
Intelligent Transportation Systems (ITS); Users and applications requirements; Applications and facilities layer common data dictionary. ETSI

ETSI 102-940,
Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. ETSI Technical Specification 102-940.

ETSI 102-941 1.2.1
Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. ETSI Technical Specification 102-941 V1.2.2. May 2018

ETSI 103-097 1.3.1
Intelligent Transport Systems (ITS); Security; Security header and certificate formats. ETSI Technical Specification 103-097. V1.3.1. October 2010.

ETSI 103-141
Intelligent Transportation Systems (ITS); Facilities layer function; Communication Congestion Control. ETSI TS 103 141 V0.0.9 (Draft)

ETSI 103 175
Intelligent Transportation Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and TS G5B medium. ETSI TS 103 175 V1.1.1. June 2015

ETSI 103 298
Intelligent Transportation Systems (ITS); Platooning; Pre-standardization study [Release 2]. ETSI TR 103 298 V0.0.2 (Draft)

ETSI 103 299
Intelligent Transportation Systems (ITS); Cooperative Adaptive Cruise Control (CACC); Pre-standardization study [Release 2]. ETSI TR 103 299 V0.1.5 (Draft)

ETSI 103 300-1
Intelligent Transportation Systems (ITS); Vulnerable Road Users (VRU); Study of UCs and standardization perspectives [Release 2]. ETSI TR 103 300-1 V0.0.8 (Draft).

ETSI 103-300-2
Intelligent Transportation Systems (ITS); Vulnerable Road Users (VRU); VRU Architecture [Release 2].
ETSI TS 103 300-2 V-.-.- (To be expected)

ETSI 103-300-3
Intelligent Transportation Systems (ITS); Vulnerable Road Users (VRU); VRU Basic Service [Release 2]. ETSI TS 103 300-3 V-.-.- (To be expected)

ETSI 103 301
Intelligent Transportation Systems (ITS); Basic Set of Applications; Facility layer protocols and communication requirements for infrastructure services. ETSI TS 103 301 V1.1.7 (Draft)

ETSI 103 324
Intelligent Transportation Systems (ITS); Basic Set of Applications; Specification of the Collective Perception Service [Release 2]. ETSI Technical Specification 103 324 V0.0.12 (Draft)

ETSI 103 561
Intelligent Transportation Systems (ITS); Basic Set of Applications; Maneuver Coordination Service [Release 2].
ETSI Technical Specification 103 561 V-.-.- (To be expected)

ETSI 103 562
Intelligent Transportation Systems (ITS); Basic Set of Applications; Information Report for the Collective Perception Service [Release 2]. ETSI Technical Report 103 562 V0.0.10 (Draft)

ETSI 302 571
Radiocommunications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU. ETSI European Norm 302 571 v2.1.1. February 2017.

ETSI 302-636-4-1
Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and for3warding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-Independent functionalities for ITS-G5. ETSI European Norm 302-636-4-1

ETSI 302-636-4-2
Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and for3warding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5. ETSI European Norm 302-636-4-2 V1.1.1. September 2013

ETSI 302-636-5-1
Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol. ETSI European Norm 302-636-5-1.

ETSI 302-636-6-1
Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols. ETSI European Norm 302-636-6-1.

ETSI 302 663
Intelligent Transportation Systems (ITS); Access Layer specification for Intelligent Transportation Systems operation in the 5GHz frequency band. ETSI European Norm 302 663 V1.2.1. July 2013

ETSI 302 665
Intelligent Transport Systems (ITS); Communications Architecture. ETSI European Norm 302 665 V1.1.1. September 2010.

ETSI 302 895
Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM) Specification. ETSI European Norm 302 895 V1.1.1. September 2014.

IEEE 1609-2

IEEE Std. 1609.2TM, IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages

IEEE 1609-2a
IEEE Std. 1609.2aTM, IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages — Amendment 1

IEEE 1003.1
IEEE Std 1003.1-2017 (Revision of IEEE Std 1003.1-2008), IEEE Standard for Information Technology — Portable Operating System Interface (POSIX(R)) Base Specifications, Issue 7

INSPIRE
INSPIRE Directive 95/46/CE on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

ISO 14823
Traffic and travel information - Messages via media independent stationary dissemination systems - Graphic data dictionary for pre-trip and in-trip information dissemination systems. ISO Technical Specification 14823

ISO 16460
Intelligent transport systems — Communications access for land mobiles (CALM) — Communication protocol messages for global usage. ISO Technical Specification 16460.

ISO 17419,
Intelligent transport systems — Cooperative systems — Globally unique identification. ISO Technical Specification 17419

ISO 17515-3
Intelligent transport systems — Evolved-universal terrestrial radio access network — Part 3: LTE-V2X. ISO Technical Specification 17515-3.

ISO 17423
Intelligent transport systems — Cooperative systems — Application requirements and objectives. ISO Technical Specification 17423

ISO 19079
Intelligent transport systems — Communications access for land mobiles (CALM) — 6LoWPAN networking. ISO Technical Specification 19079

ISO 19080
Intelligent transport systems — Communications access for land mobiles (CALM) — CoAP facility. ISO Technical Specification 19080.

ISO 19091
Intelligent transport systems — Cooperative ITS — Using V2I and I2V communications for applications related to signalized intersections. ISO Technical Specification 19091

ISO 19321
Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures. ISO Technical Specification 19321.

ISO 21176
Intelligent transport systems — Cooperative ITS — Position, velocity and time functionality in the ITS station. ISO Technical Specification 21176 (work in progress)

ISO 21177
Intelligent transport systems — ITS-station security services for secure session establishment and authentication between trusted devices. ISO Technical Specification 21177. 2019 (work in progress)

ISO 21184
Intelligent transport systems — Management of messages containing information of sensor and control networks specified in data dictionaries. ISO Technical Specification 21184

ISO 21185
Intelligent transport systems — Communication profiles for secure connections between trusted devices. ISO Technical Specification 21185

ISO 21186
Intelligent transport systems -- Cooperative ITS -- Guidelines on the use of C-ITS standards for hybrid communications. ISO Technical Specification 21186 (work in progress)

ISO 21210
Intelligent transport systems – Communications Access for Land Mobiles (CALM) – IPv6 Networking, ISO Technical Specification 21210. January 2011

ISO 21214
Intelligent transport systems — Communications access for land mobiles (CALM) — Infra-red systems. ISO Technical Specification 21214

ISO 21215
Intelligent transport systems — Localized communications — ITS-M5. ISO Technical Specification 21215

ISO 21217
Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture

ISO 21218
Intelligent transport systems — Hybrid communications — Access technology support

ISO 22418
Intelligent transport systems — Fast service advertisement protocol (FSAP)

ISO 24102-2
Intelligent transport systems — ITS station management — Part 2: Remote management. ISO Technical Specification 24102.2.

ISO 24102-3
Intelligent transport systems — ITS station management — Part 3: Service access points. ISO Technical Specification 24102.3.

ISO 24102-4

Intelligent transport systems — ITS station management — Part 4: Station-internal management communication. ISO Technical Specification 24102.3.

ISO 24102-6
Intelligent transport systems — ITS station management — Part 4: Flow management. ISO Technical Specification 24102.6.

ITSSv6
IPv6 ITS station stack for Cooperative ITS field operational tests (ITSSv6). European Project, Grant Agreement 210519.Call ICT-2009-6. 2010-2014.

ITSSv6-D2.4
Final System Specification, ITSSv6 European Project, Grant Agreement 210519, Deliverable D2.4 , 2014.

Mandate M/453
Standardization Mandate to ETSI, CEN and CENELEC. European Commission Mandate M/453. http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=434

RFC 3775
D. Johnson, C. Perkins and J. Arkko. *Mobility Support in IPv6*. IETF RFC 3775 (Proposed Standard), June 2004. Obsoleted by RFC 6275

RFC 3963
V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. *Network Mobility (NEMO) Basic Support Protocol*. IETF RFC 3963 (Proposed Standard), January 2005

RFC 4885
T. Ernst and H-Y. Lach. *Network Mobility Support Terminology*. IETF RFC 4885 (Informational), July 2007.

RFC 4886
T. Ernst. *Network Mobility Support Goals and Requirements*. IETF RFC 4886 (Informational), July 2007.

RFC 5648
R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami. *Multiple Care-of Addresses Registration*. IETF RFC 5648 (Proposed Standard), October 2009

RFC 6088
G. Tsirtsis, G. Giarreta, H. Soliman, and N. Montavont. *Traffic Selectors for Flow Bindings*. IETF RFC 6088 (Proposed Standard), January 2011. pages

RFC 6089
G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi. *Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support*. IETF RFC 6089 (Proposed Standard), January 2011.

www.secredas.eu
mail@secredas.eu
Social media @secredas_eu

Horizon 2020
European Union funding
for Research & Innovation

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis