EVOLVING THE EUROPEAN ITS ARCHITECTURE FOR CAR-TO-X COMMUNICATION

M. Bechler[1], T. M. Bohnert[2], S. Cosenza[3], A. Festag[4], M. Gerlach[5], D. Seeberger[6]

1. BMW Group Research and Technology, Germany, Marc.Bechler@bmw.de
2. SAP Research, Switzerland, Thomas.Michael.Bohnert@sap.com
3. Centro Research Fiat, Italy, Stefano.Cosenza@crf.it
4. NEC Europe Ltd., Laboratories Europe, Germany, Andreas.Festag@nw.neclab.eu
5. Fraunhofer FOKUS, Germany, Matthias.Gerlach@fokus.fraunhofer.de
6. Daimler AG, Germany, Dieter.Seeberger@daimler.com

ABSTRACT

With the publication of a first framework of the communications architecture for European Intelligent Transport Systems (ITS), a major milestone was achieved in harmonization of various R&D efforts towards a unified architecture. Relying on this framework, the project PRE-DRIVE C2X further elaborates four main aspects of the ITS communications architecture: (i) overall system architecture, (ii) network architecture, (iii) integration of ad hoc, infrastructure and backend services, and (iv) security architecture. This paper presents the main aspects of the architecture views and gives an outlook to further developments of the architecture, standardization, and deployment in future Field Operational Tests of cooperative systems.

INTRODUCTION

Intelligent Transportation Systems (ITS) will have a great and positive effect on future mobility of people and goods. The integration of information and communication technology with road infrastructure and vehicles leads to cooperative systems that help to improve road safety, traffic efficiency, transportation times, fuel consumption, and driving pleasure. Connecting cooperative systems to backend services, ITS enable the integration of up-to-date road traffic information into business processes of central IT systems.

In Europe, ITS development is strongly driven by large-scale research and development projects on cooperative systems (CVIS, SAFESPOT, COOPERS) complemented by more focused projects (GEONET, SEVECOM) [3]–[7]. To consolidate these efforts towards a European solution, the COMeSafety project [2] defines a common European ITS communication architecture as a basis for future development and standardization. This architecture framework is currently being refined and complemented by the European research and development project PRE-DRIVE C2X [1] working towards future Field Operational Tests (FoT) for cooperative systems. In summary, the COMeSafety architecture framework specifies a reference protocol architecture of an ITS station. The ITS station represents a generic component for vehicles and roadside communication infrastructure. The reference protocol architecture basically obeys the ISO/OSI reference model, vertically extended by a management and a security layer (Fig. 1).

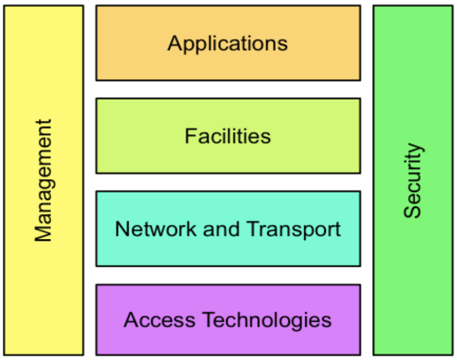

Fig. 1: ITS Station reference protocol architecture, introduced in [2]

In this document, we introduce the consolidated system architecture for cooperative systems, which is the basis for the field operational tests in PRE-DRIVE C2X and which will be further evolved for standardization. The system architecture will be described by different views, which reflect different aspects of this architecture: The general overview of the ITS system architecture is given in section 2, the network architecture view is detailed in section 3. Section 4 addresses the backend integration aspects, i.e. the integration of the vehicular network into a backend services landscape, and section 5 discusses the security architecture. Finally, section 6 concludes this document with an outlook on future activities in this field.

SYSTEM ARCHITECTURE

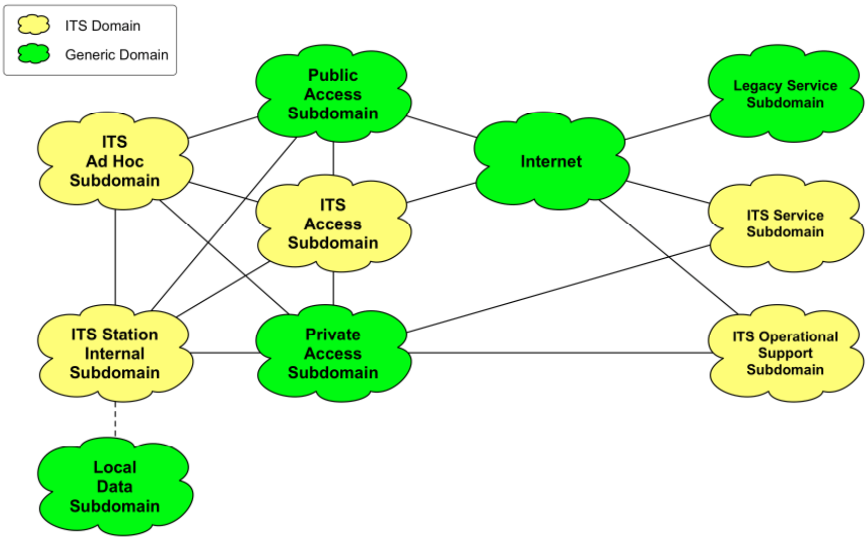

Fig. 2: Proposed ITS System Architecture

The system architecture represents the highest level of abstraction, how cooperative systems are structured. Fig. 2 shows the system architecture, which will be the basis for the field operational trials in PRE-DRIVE C2X. In general, the domains in the system architecture can be ITS-specific domains or generic domains. The ITS ad hoc subdomain comprises ITS (vehicle and roadside) stations and enables ad hoc communication among them using WLAN-based technology operating in 5 GHz band (termed ITS-G5A [13]). The ITS station itself is considered as the ITS Station internal subdomain, which can be connected to a local data subdomain. Generally speaking, the local data subdomain provides access to respective data of the “domain” the ITS station is installed. In case of an ITS vehicle station, this would be access the information within the vehicle. In case of an ITS roadside station, it could be, e.g., access to the traffic sign the ITS roadside station is mounted to. Access to the world outside the ad hoc network is provided by three potential access subdomains:

- Public Access Subdomain. In this subdomain, an ITS vehicle or roadside station gets access to the Internet using typical (IP-based) broadband communication technologies. This could be UMTS (named ITS Public in current ETSI terminology). For ITS roadside stations, it could be even an Ethernet or DSL link, which can be used to access backend services.
- ITS Access Subdomain. ITS roadside stations can also provide access to the Internet since they may be connected to it. Hence, the ITS roadside stations may act as gateways to the Internet, enabling ITS vehicle stations to access backend services using the Internet.
- Private Access Subdomain. Of course, private access networks can also be used to provide access to backend services. An example would be the network that connects traffic signs to traffic management centers in order to optimize and control the traffic flow dynamically.

In general, the Internet domain brings together the communication domains (vehicles and roadside stations) with backend applications and services, which are structured in Fig. 2 by the three subdomains (i) Legacy Service Subdomain, which provides "typical" Internet services, (ii) ITS Services Subdomain representing specific ITS backend services, and (iii) ITS Operational Support Subdomain supporting security and privacy services.

NETWORK ARCHITECTURE

The network architecture defines the main network components with their interfaces, fundamental communication principles, and frameworks for the design of network and transport protocols. Core component is the ITS Station, which consists of Communication & Control Unit (CCU) and Application Units (AU) (Fig. 3). While both may collapse into a single physical unit, they can also form an in-vehicle mobile network, where AUs obtain connectivity to the ITS ad hoc network via the egress interface of the CCU. For an ITS station, four main instantiations exist: ITS vehicle station, ITS roadside station, ITS personal station, and ITS central station.

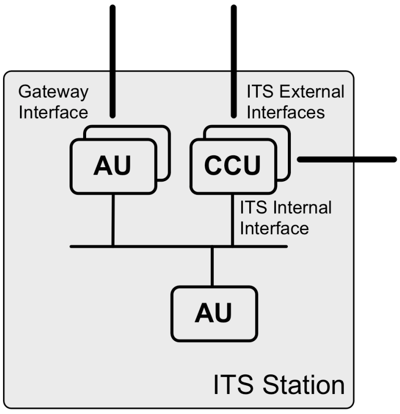

Fig. 3: ITS Station components

Fig. 4 illustrates the role of the ITS station, which can communicate via an ITS ad hoc network, an ITS access network, a public access network, via a private access network, the Internet, or a local data network (such as a Controller Area Network CAN in a vehicle or a station-internal network in a road-side unit to connect to a roadside legacy infrastructure). The ITS station can be part of all these networks, which is indicated by the dashed circle representing the boundary of an ITS station.

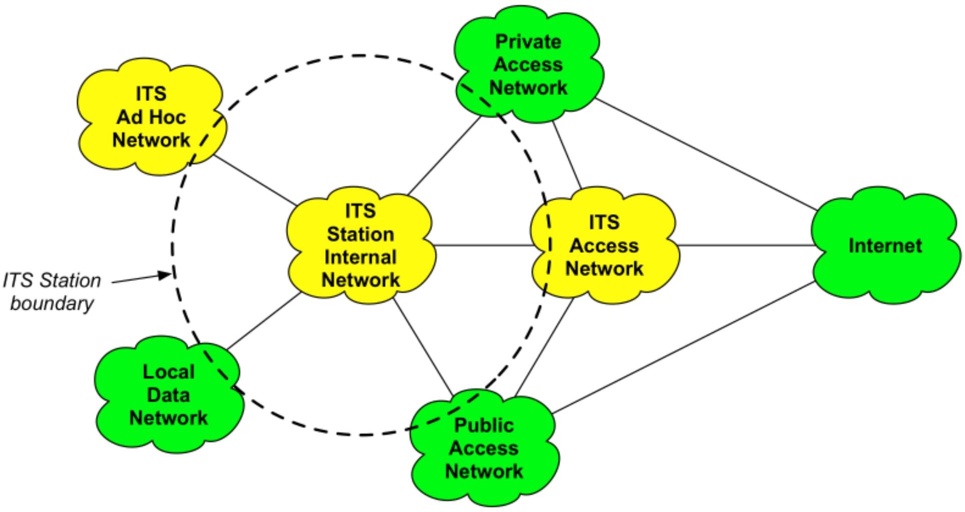

Fig. 4: ITS network architecture

The ITS architecture can be deployed in different scenarios to adapt to specific economical and regulatory conditions and to facilitate a gradual introduction of ITS. Basically, a deployment scenario is a subset of the overall architecture (Fig. 1) created by a combination of the different network types. Four basic deployment scenarios can be defined: Scenario A (ad hoc network), B (ITS access network), C (public access network), and D (private access network). The connectivity among the components for the scenarios A–C is shown in Fig. 5.

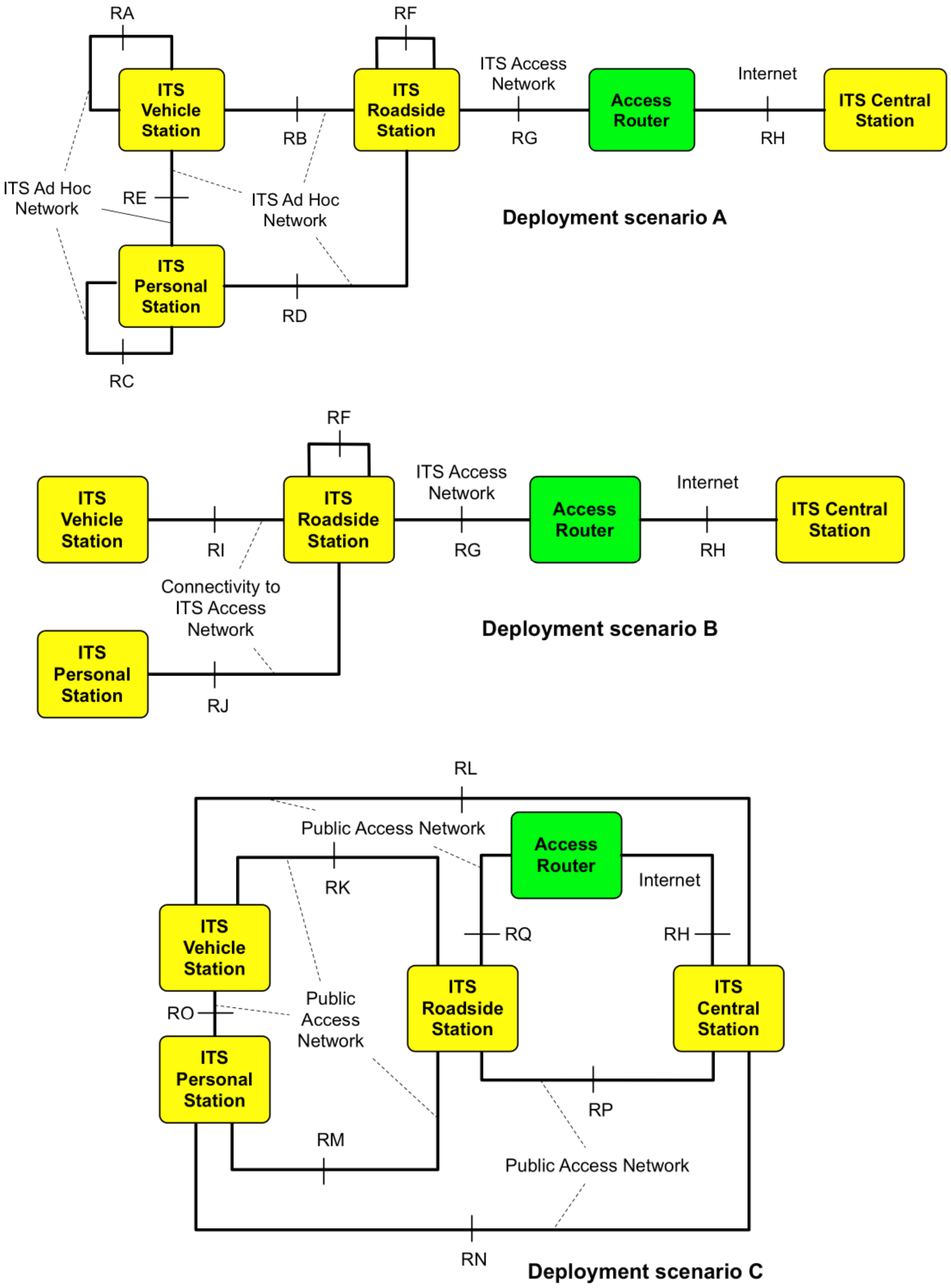

Fig. 5: Connectivity among ITS stations

In PRE-DRIVE C2X, a combination of the two basic deployment scenarios is studied, i.e., the ad hoc network uses WLAN technology working in the 5GHz frequency for ITS (ITS-G5) and the public access network uses UMTS. Particular instances of the ITS central stations are backend server (as explained in the next section) and the test management center. The routing and packet transport in the ITS ad hoc network is based on a specific approach for wireless multi-hop communication with ITS-G5 utilizing geographical positions [10]. This approach can cope with the specific requirements of the system, in particular high mobility of vehicles and scalability with the number of network nodes. It also meets application requirements, in particular for road safety. IP packet transport is assured either by means of encapsulation and tunneling over the ad hoc network for vehicle-to-vehicle and vehicle-to-roadside communication, or by using the public access network. For IP networking, we foresee IPv6, Mobile IPv6, and NEMO to ensure global reachability and session continuity for Internet connectivity [11][12]. The network architecture also defines design concepts for, e.g., data congestion control, interworking between ad hoc and infrastructure-based communication, interworking between different wireless technologies and others.

BACKEND INTEGRATION

The integration of ITS stations into backend service delivery platforms can be best achieved by applying the Service-Oriented Architecture (SOA) paradigm. SOA systems incorporate the concept of services, where a service is software that provides certain functionality via a public interface and communicates over standard protocols, like HTTP, which itself relies on TCP/IP. Since the ITS system architecture natively supports TCP/IP-based communications, they can be easily integrated into TCP/IP based SOA systems. From the SOA viewpoint, vehicles are considered as (moving) services interacting with services residing in the backend service system over standard Internet protocols.

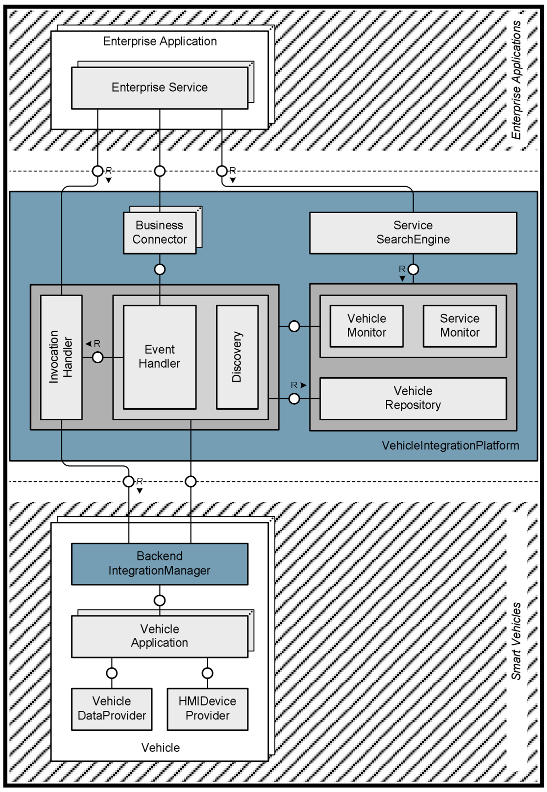

Fig. 6: Backend integration

Based on these concepts an integration architecture is specified that is made of two dedicated components: the Vehicle Integration Platform (VIP) and the Backend Integration Manager (BIM), c.f. Fig. 6. The VIP covers multiple components for efficient information exchange between vehicles and backend systems as well as management features for related software components. The message broker (EventHandler), e.g., enables publish/subscribe interactions and allows for a scalable decoupling of vehicles, applications, and backend services. The InvocationHandler is another VIP component and facilitates invocation of applications running on a vehicle. It provides buffering mechanisms to account for intermittent connectivity of moving vehicles connected over radio interfaces. The VIP further features several components to discover, organize, and search for functionality. It maintains a repository of registered vehicles and supports monitoring services running on them for management purposes All these communication facilities are essentially aiming at integrating moving terminals with static backend systems and services and hence run on top of the fundamental communication services described in other sections of this paper.

The in-vehicle component BIM is the counterpart to the VIP and designed to connect applications and services on the vehicle with backend services via the VIP. Vehicle applications, which are encapsulated in Web services, connect the BIM that provides additional functionality such as message caching, message prioritization and the rescheduling of message delivery. In brief, the BIM implements all the fundamental functionality corresponding to those in the VIP. It does so by implementing the Devices Profile for Web Services (DPWS) specification, which allows for secure Web services operations on resource-constrained devices.

SECURITY ARCHITECTURE

The security view of the architecture describes all relevant technical aspects of providing trustworthy and privacy preserving ITS communications, with major focus on ITS5G safety communications. These are (1) secure communication, (2) privacy, (3) in-vehicle security, (4) identity management and (5) administrative processes.

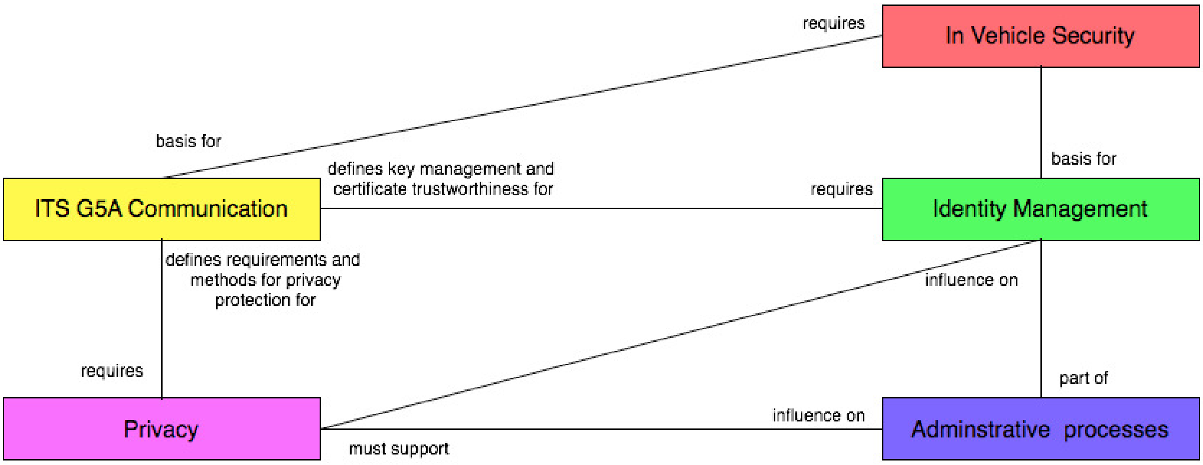

Fig. 7: Interdependencies between technical aspects

Fig. 7 depicts the interdependencies of the identified technical aspects for the PRE-DRIVE C2X security architecture. ITS-G5A communication is at the core of these technical aspects requiring at least in-vehicle security and identity management as a basis. Introduced by the stakeholders such as customers as well as legislation, privacy mechanisms must be present for the communication, as well as for the identity management solution and influences the use of the mechanisms defined there, as well as the administrative processes. Administrative processes are part of identity management that in turn determines how keys used for the communication is managed. Keys are part of the vehicle identity that needs in vehicle security measures as a basis.

Secure communication deals with security related to the actual communication process. Various security services can be used on any layer of the communication stack and in PRE-DRIVE C2X are modeled by a layer-independent interface that creates generic secure messages. These messages can be configured to be insecure, signed or encrypted, and to also include mobility data that need particular protection for ITS-G5A safety use cases. A complete ITS communication stack will need to support a variety of different security services ranging from well-known application layer security services such as https to newly developed security services for vehicular communications based on ITS G5. The security architecture presented in PRE-DRIVE C2X mainly addresses the latter; consequently, the descriptions in the following paragraphs refer to this communication mode.

Privacy defines the components necessary for protecting the privacy of the users of the communication system. For ITS systems, privacy can be broken down to (1) location privacy, where a user's current and past location cannot be combined to form a trace or reveal other sensitive information. (2) Anonymity of the user against unauthorized entities; potential attackers should not be able to link the identity of a user to his or her vehicle. (3) Resolvable pseudonymity for cases where a vehicle or its user must be held responsible for his or her actions. This will also be necessary for implementing reactive security measures such as revocation of nodes.

In order to implement these requirements, PRE-DRIVE C2X identifies two logical components: the obfuscator and the identifier management; the obfuscator shall check whether information is sent out that can potentially leak private information, such as too accurate positions or static vehicle properties; it would then obfuscate information such that it meets the desired privacy level. The identifier management component is responsible for changing and creating identifiers (i.e., MAC and NET addresses) at the right time. Identity information generated by the Identity Management subsystem can be input to the identifier creation.

Identity management describes how identities and keys for their use in secure communications are managed. At least two types of vehicle identities are required for an ITS system: First, the Safety Identity conveys all major information about a node present within the ITS G5A network. These contain a temporary identifier, authentication information (such as a public key certificate), attributes describing the node, the validity of the identity, its provider and – only visible for authorized parties – a link to the long-term identity. Second, the Long Term Identity conveys all major information about a node to be admitted to the ITS G5A network. This contains information about the configuration, installed software, and depending on the desired scope of this identity information about the user or owner of the vehicle. The long-term identity shall not be used for communications. Abstract mechanisms for identity creation, use and validation have been defined and the interdependencies between the types of identities investigated within PRE-DRIVE C2X.

In-vehicle security stresses the necessary components within the vehicle, such as intrusion detection systems or firewalls, to create a trustworthy sender and protect in vehicle systems. At the same time, a concrete mapping of security functionality to so-called *security units (SU)* is proposed. The SU-C (communication) contains methods to provide security communications, and therefore the collection of security services. The SU-G (Gateway) is responsible for isolating the ITS station from the vehicle systems connected via the gateway. The SU-D provides mechanisms for the detection of attacks and intrusions on the various in-vehicle networks. Finally, the SU-V is responsible for deciding and adapting the security policies currently used by a system and the vehicles identities used.

Finally, the administrative processes look at vehicular communications to ensure vehicle homologation, insurance updates, and in field operation. The five major services within the administrative processes have been identified: the attestation service is responsible for checking the configurations of ITS stations before issuing long-term identities. The long-term identity provider is responsible to create and assign long-term identities to vehicles. The safety identity provider – based on the long-term identities – will provide safety identities to vehicles for use within the ITS 5GA network. A certificate trust hierarchy must be set up maintained as part of the administrative processes; this will include issues such as cross certification between different legal domains as well. Finally, a certificate revocation service as part of the trust hierarchy must be set up; note that using short-lived safety identifiers and frequent system integrity checks may mitigate the need for large revocation lists.

The overall security architecture is suitable, extendable and future proof for the use in different use cases. It is the foundation for the later specification of the security system. Selected aspects of the security architecture can be tested and validated in later field trials, such as privacy provisioning, identity management and trustworthy movement data. More details on the different technical aspects of the security system described in this Section can be found in [1].

CONCLUSIONS

This paper introduces extensions and refinements of a European ITS architecture for cooperative systems covering aspects of the system, network, backend service, and security architecture. We particularly emphasize the importance and the role of the ITS stations and the boundaries of its network: the ITS station (as on board unit or as road side unit) can have access to different subdomain at the same time and via different means, providing a full integration in a network that connects the services in the backend with the mobile system. The development of the ITS stations and the related architecture must consider the role and the interaction with backend delivery platforms, which is achieved by applying SOA paradigm. The concept of the vehicle as a moving service interacting with other services in the backend service system is presented, opening to a broad range of possible scenarios with very specific constrains and requirements. In this architecture, security is a fundamental module to guarantee the public trustiness on the ITS systems as a whole. The adoption of security procedures is an indispensable feature that cannot be neglected in the future. The architecture described in this paper aims to represent a synthesis of the effort provided via several IP projects; PRE-DRIVE C2X target is to provide a reference platform implementation under software and hardware point of view based on the PRE-DRIVE C2X proposal ready and available for the future European FoT.

ACKNOWLEDGEMENTS

PRE-DRIVE C2X is a European project co-funded by the European Commission Information Society and Media among the initiatives of the 7th Framework Program and is coordinated by Daimler AG.

REFERENCES

[1] PRE-DRIVE C2X Project, "Preparation for Driving implementation and Evaluation of Car-2-X communication technology", Available at http://www.pre-drive-c2x.eu

[2] COMeSAFETY Project, "European ITS Communication Architecture, version 2.0", Available at http://www.comesafety.org

[3] CVIS Project, Available at http://www.cvisproject.org

[4] SAFESPOT Project, Available at http://www.safespot-eu.org

[5] COOPERS Project, Available at http://www.coopers-ip.eu

[6] GEONET Project, Available at http://www.geonet-project.eu

[7] SEVECOM Project, Available at http://www.sevecom.org

[8] Manner, J. and Kojo, M., "Mobility Related Terminology", RFC 3735, June 2004.

[9] 3GPP, "UMTS Standard, Release 08 Specification", Available at http://www.3gpp.org

[10] "Car2Car Communication Consortium Manifesto", Available at http://www.car-2-car.org, Version 1.1, August 2007

[11] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6": RFC 3775, June 2004.

[12] Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P., "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[13] ISO/IEC 42010:2007, "Systems and Software Engineering – Recommended Practice for Architectural Description of Software-Intensive Systems", September 2007

[14] ETSI TC ITS, "Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band", Draft ES 202 663, work in progress.

[15] Hess, S., Segarra, G., Evensen, K., Festag, A., Weber, T., Cadzow, S., Arndt, M. and Wiles, A., "Towards Standards for Sustainable ITS in Europe", ITS World Congress, Stockholm, Sweden, October 2009.