FABRIC

Feasibility analysis and development of on-road charging solutions for future electric vehicles

ICT functional architecture and specifications

Deliverable No.		D2.4.1	
Workpackage No.	WP2.4	Workpackage Title	**Architecture and system specifications**
Authors		Yannis Damousis, Angelos Amditis (ICCS), Andrew Winder (ERT), Francesco Belloti (UNIGE), Hasnaa Aniss (VEDE), Maria Paola Bianconi (CRF)	
Status (Final; Draft)		Final	
Dissemination level (Public; Restricted; Confidential)		Public	
Project start date and duration		01 January 2014, 48 Months	
Revision date		01-15-2015	
Submission date			

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 605405

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABBREVIATION	DESCRIPTION
AAA	Authentication Authorization Accounting
ADAS	Advanced Driver Assistance Systems
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
AU	Applications Unit
BMS	Battery Management System
BT	BlueTooth
C2C	Car to Car
C2X	Car to anything
CALM	Communication Architecture for Land Mobile
CAM	Cooperative Awareness Message
CAN	Car Area Network
CDMA	Code Division Multiple Access
CI	Charging Infrastructure
CIO	Charging Infrastructure Operator
CU	Communications Unit
DC	Direct Current
DENM	Decentralized Environmental Notification
DoS	Denial of Service
DoW	Description of Work (of the FABRIC project)
DSL	Digital Subscriber Line
DSO	Distribution System Operator
DSRC	Dedicated Short Range Communications
DX.X.X	Deliverable X.X.X
ECU	Engine Control Unit
ER	Energy Retailer
ETH	Ethernet
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Electric Vehicle
EVB	EV backend
EVSE	Electric Vehicle Supply Equipment
FABRIC	Feasibility analysis and development of on-road charging solutions for future electric vehicles

FEMP	FABRIC Electric Mobility Platform
FEV	Fully Electric Vehicle
FOT	Field Operational Studies
FP7	7th Framework Programme
GHz	Giga Hertz
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Services
GPS	Global Positioning System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
HV	High Voltage
HW	Hardware
I2I	Infrastructure to Infrastructure
ICE	Internal Combustion Engine
ICT	Information and Communications Technologies
ID	Identity
INS	Inertial Navigation System
IR	Infrared
IT	Information Technology
ITS	Intelligent Transport Systems
ITS-S	ITS-station
Km/h	Kilometres per hour
kW	Kilo Watt
LTE	Long Term Evolution
MMWAVE	Millimetre wave
N/A	Not applicable
NIST	National Institute of Standards and Technology
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
PC	Personal Computer
PKI	Public Key Infrastructure
PLC	Power Line Communication
PoI	Point of Interest
REST	Representational State Transfer
RF	Radio Frequency
RO	Road Operator
RSU	Road Side Unit
SAM	Service Announcement Message

SOAP	Simple Object Access Protocol
SoC	State of Charge
SPX	Sub-Project X
SSL	Secure Sockets Layer
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TX.X.X	Task X.X.X
UDP	User Datagram Protocol
UML	Unified Modelling Language
UTC	Coordinated Universal Time
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to anything
VPN	Virtual Private Network
WAN	Wide Area Network
WAVE	Wireless Access in Vehicular Environments
WiFi	Wireless Fidelity
WPT	Wireless Power Transfer
WPXX	Work-Package XX

REVISION CHART AND HISTORY LOG

REV	DATE	REASON
0.1	03-09-14	TOC and document structure.
0.2	14-10-14	First draft. Sequence diagrams added.
0.3	15-11-14	Chapter 4: Security and privacy requirements added.
0.4	24-11-14	Chapter 2: FABRIC OBU functional architecture added.
0.5	01-12-14	Chapter 2: FABRIC EVSE, CIO, EV backend functional architecture added.
0.6	05-12-14	Chapter 2: FABRIC Electric Mobility Platform functional architecture added.
1.0	11-12-14	Document finalized. Formatting complete.
Final	01-15-15	Peer review input integrated. Document finalized.

EXECUTIVE SUMMARY

This report forms part of Sub-Project 2 (SP2) of FABRIC, which relates to Information and Communications Technologies (ICT) solutions for wireless on-road charging of electric vehicles (EVs).

It is the first output of ***WP24 "Architecture and system specifications",*** covering the functional ICT architecture of FABRIC and listing the security and privacy requirements. A second (confidential) version of D24.1 will include the specifications of the system and will be available in Month 15 of the project.

The main research, development and demonstration focus in FABRIC is on ***Wireless Power Transfer (WPT)*** charging for vehicles while moving ("***dynamic charging***" mode), either in a specific reserved lane or a general traffic lane, both equipped with a series of "charging pads". Two (simpler) variations of this mode are also covered. Firstly, the "***static charging***" mode is charging when a vehicle is parked (driver presence not necessary for the charging except perhaps in order to initiate it) and receives rapid wireless charging from pads for a period typically over 5 minutes (but shorter than the several hours which are typically required for conventional plug-in charging). Secondly the "***stationary charging***" mode, which can be considered as an intermediate mode between static and dynamic, is rapid charging of a vehicle during a short stop or pause, typically for less than 5 minutes (and possibly only a matter of seconds), with the driver typically present. This could include vehicles waiting at traffic lights, buses at bus stops, taxis in taxi ranks, etc. This deliverable further elaborates on the definition of these three modes based on the outputs of Sub-Project 3 (SP3).

The ***functional design*** defines the main architectural elements of the FABRIC system and their high-level interconnections. The report describes the functional structure of the main subsystems using interaction models (UML sequence diagrams) to demonstrate how the system will implement the functional requirements focusing on the ***demonstrable use cases*** (to be implemented in the project) but also providing suggestions having the ***feasible use cases*** in mind (potential operating scenarios beyond the scope of the FABRIC demonstrators, with a year 2030 vision) as they were both defined in D43.1 "FABRIC final use cases".

The principle adopted by FABRIC consortium for the system architecture definition is to provide FABRIC services from backend wherever possible, allowing collection and processing of large amount of data from multiple infrastructure systems and from EVs. Based on this, a high level ***physical architecture*** of the FABRIC system has been defined in order to identify the main subsystems and their topology. The main FABRIC ***high level sub-systems*** in this architecture are:

- ***On Board Unit (OBU)****:* installed inside the EV that will host the FABRIC applications and provide in-vehicle end-user access to FABRIC services via a HMI.
- ***EV backend (EVB)****:* the main EV access point to FABRIC system. It will host a database that will contain the data of the EVs and their users, EV characteristics and billing information. It will also store in this database the history and data of past EV charges. It

will provide POI and navigation services to the EVs and also communicate with the clearing house in order to carry out the payment processes.

- ***FABRIC electric mobility platform (FEMP)****:* the core of the system, acting as an information coordination system. It will host all interfaces with the external actors and route the information received to the appropriate recipients. It will host databases that contain information for the state of the whole system such as a database with the charging infrastructures' characteristics and availability status, logs for system usage, etc.
- ***Charging infrastructure operator (CIO)****:* to control the charging pads, monitor the charging process and transmit aggregated information to EVB and FEMP. It will contain a module for balancing the demand from EV charging with the energy supply restrictions imposed by the Distribution System Operator (DSO). It will also perform locally EV authentication and authorisation tasks.
- ***Charging infrastructure (CI)****:* comprises the primary power transfer coil and its electronics and software that communicates with the CIO and the OBU and monitors and controls the charging process based on the information received by the CIO and the EV.
- ***Road Side Unit (RSU)****:* to transmit information to EVs in the vicinity. It can also gather information from EVs and forward it to the CI.

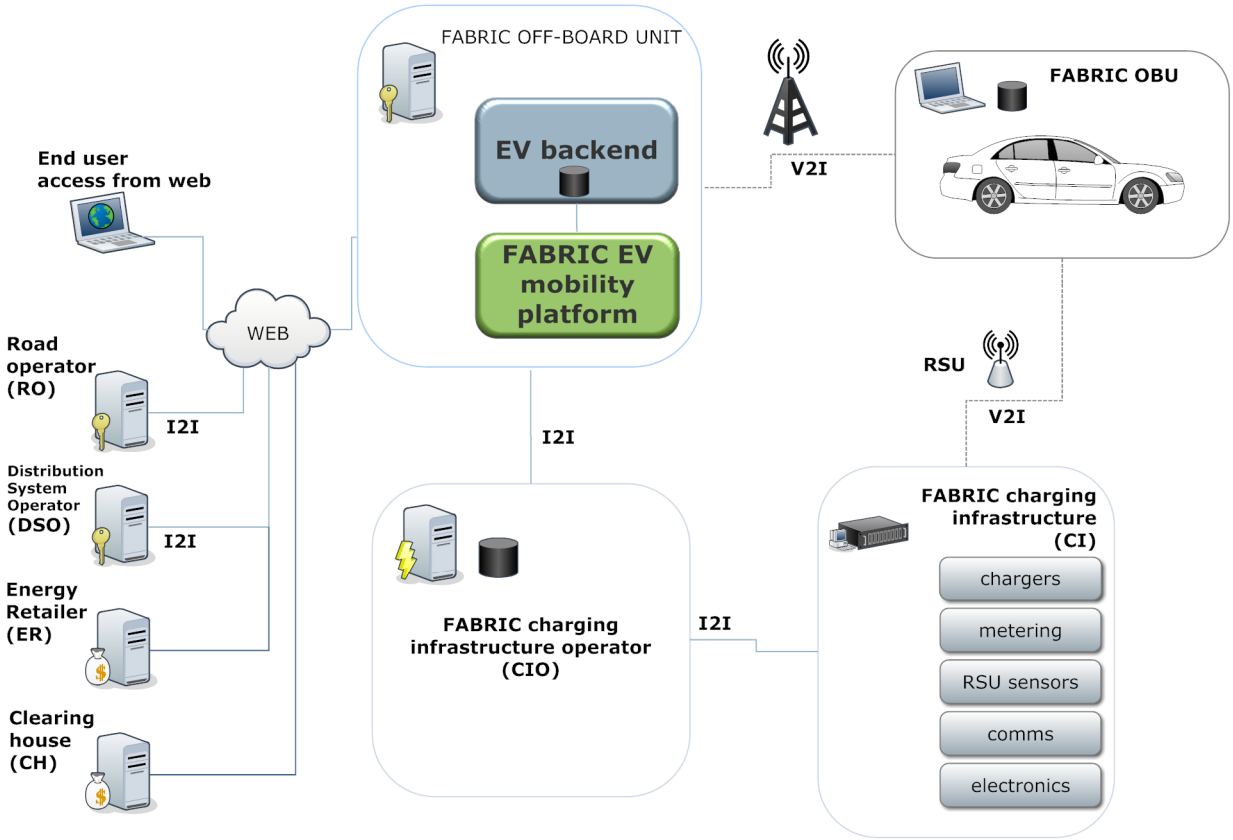


Figure: High level architecture diagram identifying the main subsystems, external actors and communication channels.

The ***functional components*** of each of these sub-systems are listed and described in the main body of this report (Chapter 2).

UML sequence diagrams have been provided for the following use cases, showing interactions and foreseen information flow between sub-systems, external actors and the end user:

- End-user logging into FABRIC via web page;
- End-user logging into FABRIC via OBU;
- End-user account management;
- Trip planning;
- Assisted static charging;
- High level charging supply management;
- Energy tariff modulation;
- EV identification;
- Facility availability status updating;
- Charging or road infrastructure availability status updating during emergencies;
- Logging into the FABRIC interfaces for external operators;
- Structured and unstructured operator messaging;
- Charging management for dynamic and stationary charging;
- End-user billing;
- Charging infrastructure booking.

Concerning ***data security and privacy***, WP24 has identified the information flow through the FABRIC network and the information stored in various systems, as well as identifying the vulnerabilities and risks involved in order to draft requirements for data security. Based on this analysis, problems in terms of attack models have been reported, together with their counter-measures in terms of available security and privacy mechanisms. This led to a list of recommendations that will guide the selection of specific currently available security solutions (commercial products, standards, APIs and software solutions) to be used by the FABRIC platform developers in the application development work-package (WP25).

The study specifies the following ***communication types*** as being required for FABRIC:

- V2I (FABRIC off-board unit) long-range communication (wireless);
- V2I (FABRIC charging infrastructure operator) long/medium-range communication (wireless);
- V2I (RSU) short-range communications (wireless);
- V2V short-range communications (wireless);
- I2I Grid operator to energy supplier communication (wired);
- I2I external actors to FABRIC (wired);
- I2I RSU (metering/control) to FABRIC charging infrastructure operator (wired);
- Infrastructure to driver nomadic device (mobile phone or other) (wireless).

V2V communications are not foreseen in the development and testing phases of FABRIC project, however they are potentially relevant for a feasible longer term potential deployment.

The following ***security requirements*** were formulated to respond against threats or system vulnerabilities:

- The platform will respect the common security targets;
- There shall be security association between communication participants;
- The platform must not require permanent online access to the backend systems;
- Unique as well as anonymous authorisation shall be provided for end-users;
- Integrity and authenticity of communications shall be ensured;
- There shall be a central ITS authority, which impersonates the root of trust;
- There shall be a public key infrastructure to establish security associations;
- The ITS authority shall issue enrolment and authorisation credentials;
- The ITS authority shall provide mechanisms to revoke security associations;
- Security credentials shall contain immutable attributes reflecting access rights and privileges of a node;
- Integrity and authenticity of aggregated data shall be preserved;
- Secure user login to FABRIC applications;
- FABRIC has to authorise applications before allowing their installation;
- Safe exchange of personal data with third party applications.

Finally, FABRIC has identified data (driver/owner data and vehicle identity data) that should be subject to ***privacy requirements***. These requirements are defined as follows:

- Privacy of mobile nodes shall be preserved through anonymous or pseudonymous communications;
- Public identifiers of a mobile node shall be changed in regular intervals;
- All public identifiers must be variable and shall follow the joint ID change;
- During safety critical situations node ID changes shall be suspended;
- An ID Management component shall trigger ID changes and provide unique IDs;
- One-to-one communication channels should not allow interception by third parties;
- Aggregated data is confidential and shall be protected from unauthorised access;
- Before sharing data with backend services, mobile nodes should apply additional anonymisation measures;
- Compliance with EU Directive 96/46/EC4 is mandatory;
- Provide users with a clear and understandable privacy policy notice;
- Provide users with data privacy settings modification functionality;
- Lawful lifecycle of stored private information;
- Stored sensitive data should be encrypted.

These are in addition to a range of recommendations from a Privacy Impact Assessment conducted by the US National Institute of Standards and Technology, which are listed in full at the end of Chapter 3.4.2.

1. INTRODUCTION

1.1 Introduction to FABRIC and to SP2: ICT Solutions

Electromobility is expected to be an essential component in the pursuit of the decarbonisation of road transportation and mobility. Issues concerning current on-board battery packs (high weight and cost) limit the usage of fully electric vehicles (FEVs) predominantly to urban/local trips. For this, on-road power transfer solutions are being investigated, since they would allow practically all of the drawbacks of on-board battery packs to be avoided or circumvented.
In this context, the principal motivation for the FABRIC project is the feasibility assessment of on-road charging solutions, including their technological feasibility, socio-economic viability and environmental sustainability from all perspectives. The ultimate aim of FABRIC is to provide a pivotal contribution relevant to electro-mobility in Europe, identifying the expected benefits and required costs so that the investments required for research, development and implementation in each of the components of the mobility system of the future can be fully understood, quantified and ratified.
FABRIC is undertaking an in-depth assessment of user and technological requirements across the main areas which this technology could impact, such as road and energy infrastructure, and will identify gaps between current capability and what is required for such a system to succeed and provide the anticipated benefits.

Sub-Project 2 (SP2) of FABRIC is one of four technical SPs in the project. It deals with solutions related to Information and Communications Technologies (ICT). ICT can offer solutions to the challenges of electro-mobility provided that there is a holistic approach, bringing vehicle, driver and infrastructure together in a highly integrated environment where information is securely, swiftly and reliably communicated and processed. A future where each node in this system is aware of the system's status and the end user is able to pre-book infrastructure, charge the EV, and pay seamlessly and effortlessly is feasible and can be envisioned. This can be achieved by a feasible FABRIC implementation, providing the necessary ICT infrastructure (including Intelligent Transport Systems – ITS) is deployed.
Work-Packages of SP2 cover user needs and system concept/functionalities (WP22), technical benchmarking of ICT solutions (WP23), architecture and system specifications (WP24: reported in this deliverable), design of ICT applications (WP25) and verification (WP26).

1.2 Task description, purpose and contributions to other tasks in FABRIC

WP24 – User needs and requirements – is composed of the following three tasks:

- Task 2.4.1 on *architecture definition;*
- Task 2.4.2 on *system specifications;*
- Task 2.4.3 on *data security and privacy.*

D24.1 is the sole output of WP24 and comprises the outcomes of all WP24 tasks. This document is the first (public) version of D24.1 which describes the functional ICT architecture of

FABRIC (Task 2.4.1) and lists the security and privacy requirements (Task 2.4.3). A second, confidential, version of D24.1 will include the specifications of the system (Task 2.4.2) and will be available in Month 15 of the project when WP24 also ends.
The functional architecture design is based on the input from the use cases and system requirements specified in the FABRIC deliverables D43.1 “FABRIC final use cases” [1] and D22.1 “User needs, system concept and requirements for ICT solutions” [2] respectively, as well as the system functionalities, boundaries and modules that were defined D22.1.
The purpose of this deliverable is to match the end users’ expectations from FABRIC with the development of ICT applications and the adaptation of existing ones within WP25. Although the delivery date for this document was set in the DoW for Month 10, its task continues until Month 15 which means that the deliverable will be updated as necessary to include the information regarding specifications and interfaces that becomes available as development design progresses.
This deliverable further specifies the components, sub-components, their interactions and the system ICT functionalities necessary to develop and test the EV charging prototypes in SP3. It also provides a blueprint for FABRIC ICT development that will take place in WP25. These relationships are shown in Figure 1.

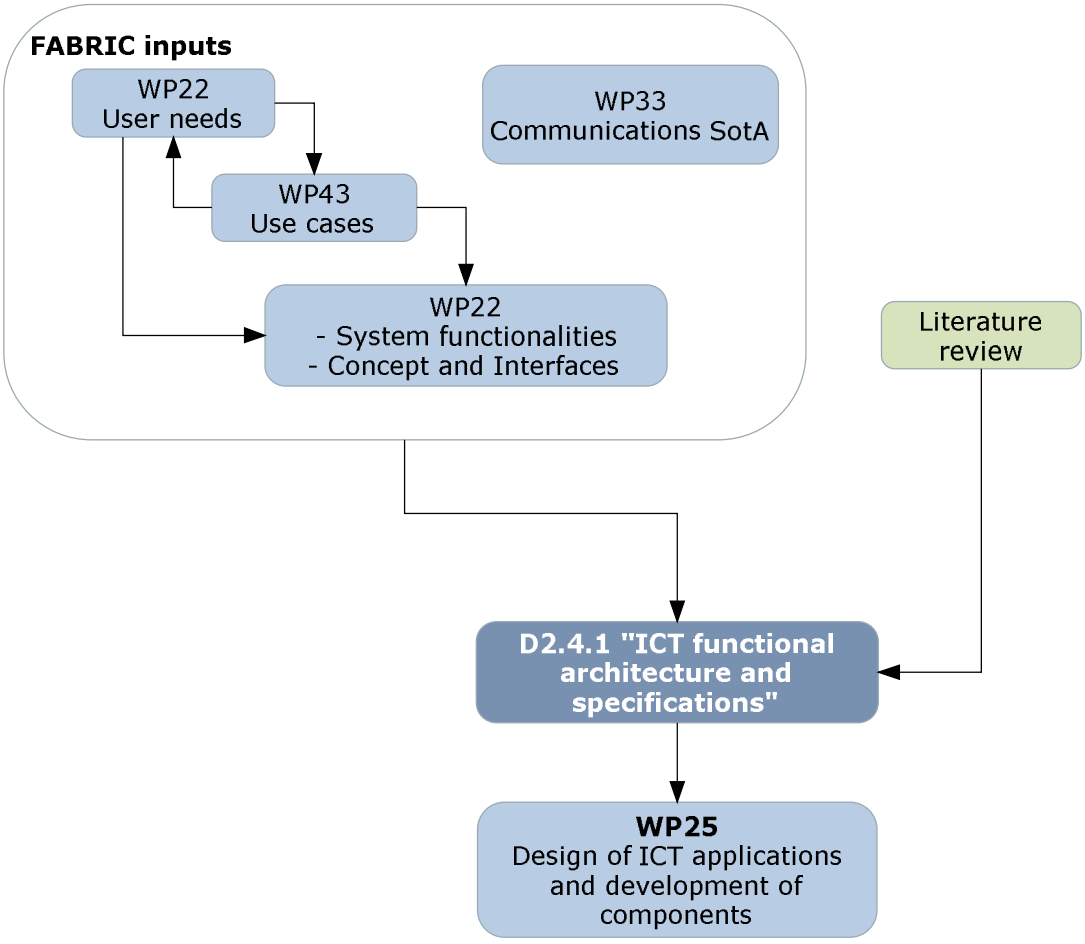


Figure 1: Inputs and outputs for D24.1

The scope of the deliverable is twofold: the functional architecture of the demonstration prototypes within the FABRIC project and also that of a feasible future system (year 2030+) based on FABRIC when ICT and ITS proliferation is a given in a "connected" environment. This is done because FABRIC is a feasibility research project and the architecture definition should consider probable implementations that go beyond the strict boundaries of the system that will be developed and tested within the project itself. As an example, infrastructure booking, routing and accounting have been considered although it is not planned to implement and test these at the FABRIC test sites.

1.3 Methodology

The first step for the definition of the architecture was the formation of a taskforce of key partners that play important role in the design and development of the ICT part of the system. SP2 and SP3 leaders were also included to ensure seamless inter-SP information flow. This taskforce was chosen to be small, consisting of only critical partners in order to ensure agile decision making process and efficient communication. The decisions of this group were then presented to the rest of the consortium for feedback and approval.

The first task was to decide on which charging modes FABRIC will support and define their naming and description.

The second task was to identify for these charging modes the necessary ICT subsystems that the system should have in order to provide the functionalities described in the use cases of [1]. For each subsystem the functional requirements were initially described and its functional design followed.

The third task was to translate the use cases of D43.1 [1] in UML sequence diagrams. The diagrams revealed in detail the information flow between the major subsystems and the components they should include to realize the required functionalities.

The fourth task was to design the functional architecture of each component and describe the component functionalities and the communication interfaces among them. A literature review took place to find objectives similarities with other electromobility related research projects. Then, effort was put to follow, adapt and extend existing ICT architecture of electromobility projects for functionalities that are common or similar with FABRIC functionalities. This was done to capitalise on the experience gained on ICT development for ITS in general and for electromobility systems in particular, as is the case with the ecoFEV project [4], in order to avoid duplication of work but also help towards standardisation of electromobility ICT. The transfer of knowledge was achieved via common project partners.

Having defined the high level architecture of the system a data security and user privacy analysis took place by identifying potential threats for vulnerable nodes of the system based on literature review. Guidelines to developers were issued for security and privacy requirements.

1.4 Deliverable structure

Besides this introductory chapter, the present document consists of two main parts following the structure of WP24 "Architecture and system specifications".

In Chapter 2 the functional architecture of the system is defined. The major subsystems are defined and the use cases of [1] are translated in UML sequence diagrams that show the information flow between the subsystems and highlight the tasks distribution among them. Based on these functionalities, the components for each subsystem are identified and the functional architecture is designed.
In Chapter 3 data security and user privacy requirements are drafted as input to the development tasks. The points of potential attack to the system are identified based on a literature review for security on ITS and ICT and then the technology means that act as threat countermeasures are listed as suggestions for implementation in order to ensure the user's privacy and data integrity. It has to be noted that FABRIC will not develop new security methods or algorithms but rather follow existing practices as is done in other ITS and electromobility projects that are not specifically focused on security and privacy research.
Chapter 4 summarizes the findings of the document.

2. FABRIC FUNCTIONAL ICT ARCHITECTURE

2.1 FABRIC supported charging modes

Electromobility that is nowadays available to the consumer revolves around plug-in electric vehicles, that is EVs that have to be immobile and plugged into an electricity outlet to recharge. The recharging time typically spans for several hours although recent (and expensive) developments allow fast recharging at special recharging stations, lasting only one hour for a complete recharge. This is great progress towards increasing user acceptance, however the EV still has to remain immobile for a significant amount of time and the user still has to deal with the not so convenient process of handling very high powered electric cables (120kW) with his/her hands. Vandalism or even weather conditions may damage to the recharging cables which might even pose risks for the safety of individuals that access or are in the vicinity of the charging infrastructure.
FABRIC focuses its research and development on wireless charging. Wireless power transfer allows EV recharging without the user coming in contact with charging equipment (cables). It also enables new charging modes such as charging while the vehicle is moving or during very short stops (e.g. at traffic lights or, for public transport or logistics/utility vehicles, at bus stops, loading points, etc) where plugged-in charging would be impractical or impossible. The new charging possibilities allow more frequent charging during daily commutes so, in theory, smaller batteries could be used and the vehicles will be at the user's disposal all day like an ICE vehicle. Below are the wireless charging modes as they were specified in [5] that FABRIC will study by constructing prototypes and evaluating their efficiency and potential for large-scale deployment:

- **Charging mode 1: Static Charging**

Power is transferred to the vehicle while the vehicle is immobile for a long period of time (>5 minutes) and without the necessity for the driver to be in the vehicle.

Short description:

This mode refers predominantly to charging of vehicles while they are parked. This mode is analogous in its principle to conventional plug-in charging which would also be described as static mode charging. The vehicle would be parked in a dedicated space where charging would commence either automatically with the driver's confirmation from within the vehicle or, manually by driver starting the charging process through some sort of off-board user interface. Note that in either case, no handling of a connector is necessary to couple the vehicle to the charger, this is done automatically. Typically, no driver or passenger would be present on board during charging (other than to confirm the charging process).

Example application scenarios:

- Car parked in a garage or car park.
- Bus parked at a bus terminus or station.
- Freight vehicles while loading or unloading at an off-road location.

Mode Definition parameters:

Estimates for each parameter defining the charging mode are provided below.

Table 1: Static charging parameters.

Parameter	Range	Comments
Vehicle speed (km/h)	0	Mode applicable if immobile for longer than 5 minutes.
Vehicle acceleration (m/s^2)	N/A	
Transmitted power level range (kW)	3 to 50	Similar to existing plug-in charging solutions and wireless charging solutions.
Charging time (minutes)	>5	Upper limit of charging time is subject to use, charging facility power rating and vehicle on-board energy storage system capacity.
Vehicle status	N/A	Vehicle engine / power will generally be off during charging (but may be on for a short time while initiating coupling / charging process).

- **Charging mode 2: Stationary en-route charging**

Power is transferred to the vehicle while the vehicle is stationary for a short amount of time (< 5 minutes) but is en-route and therefore would typically have a driver (and maybe passengers) on-board.

Short description:

This mode refers predominantly to charging of vehicles while they are stationary for a short period of time but are en-route to another location. This mode could in theory be satisfied in some cases by conventional plug-in charging, however, in reality this is unlikely to be practical or safe and is therefore, considered to be a mode unique to on-road charging solutions (either inductive or conductive). The vehicle would stop in a location that would be suitably equipped but is not a dedicated stopping / parking spot, typically this would be on a road but power transfer would only be activated when the vehicle is stationary. Charging would commence automatically after the driver's confirmation from within the vehicle. Typically, the driver (and passengers) would be present on board the vehicle during charging, particularly as they might be required to interrupt the charging and drive away at any moment due to traffic conditions (stationary queue that starts to move forwards).

Example application scenarios:

- Taxis queuing in a taxi rank.
- Bus stopping at bus stops.
- Delivery vehicles making short on-street stops to load or unload.
- Vehicles stopping at junctions, traffic lights, tolls, rail level crossings, etc.

Mode Definition parameters:

Estimates for each parameter defining the charging mode are provided below. Note that at this stage of the project, these are provisional estimates only and may be subject to revision once the solutions have been developed.

Table 2: Stationary charging parameters.

Parameter	Range	Comments
Vehicle speed (km/h)	0	Mode applicable if stationary for less than 5 minutes.
Vehicle acceleration (m/s^2)	N/A	
Transmitted power level range (kW)	20 to 200	Similar to existing fast and rapid charging solutions (plug-in and wireless).
Charging time (minutes)	<5	Upper limit of charging time is subject to use, power rating and vehicle on-board energy storage system capacity.
Vehicle status	N/A	Vehicle engine / power can be on or off depending on the vehicle powertrain control and exact application.

- **Charging mode 3: Dynamic charging**

Power is transferred to the vehicle when the vehicle is in motion at constant or variable speed.

Short description:

This mode refers predominantly to power transfer between the charging infrastructure and the vehicle while the vehicle is moving. The electric power / energy flow is variable depending on the conditions, including also possible phases with power flowing from the on-board energy storage and the grid to the on-board traction system (however this is a feasibility scenario that will not be investigated via a prototype in FABRIC).

The vehicle could be travelling at a variable speed and power transfer level could be responsive in real time to vehicle power demand or the condition of the electric grid / distribution system, within the constraints of the system capability or other fixed parameters. Charging would commence automatically after the driver's confirmation from within the vehicle, once the vehicle enters a charging zone on the road. The driver (and passengers) would be present on board the vehicle during charging.

Example application scenarios:

- Highways (multiple lanes).
- Urban roads with dedicated charging lanes.

Mode Definition parameters

Estimates for each parameter defining the charging mode are provided below. Note that at this stage of the project, these are provisional estimates only and may be subject to revision once the solutions have been developed.

Table 3: Dynamic charging parameters.

<table>
<tr><th>Parameter</th><th>Range</th><th>Comments</th></tr>
<tr><td>Vehicle speed (km/h) – Low Speed scenario</td><td>>0, <50</td><td>Constant or variable speed.</td></tr>
<tr><td>Vehicle speed (km/h) – High Speed Scenario</td><td>>50, <130</td><td>High speed scenario - Constant or variable speed.</td></tr>
<tr><td>Vehicle acceleration (m/s^2)</td><td>>0, <5</td><td>Range covers possible accelerations of vehicles ranging from cars to trucks.</td></tr>
<tr><td>Transmitted power level range (kW) – Low Speed Scenario</td><td>7 to 140</td><td>Maximum Power. Refers to both cars and trucks.</td></tr>
<tr><td>Transmitted power level range (kW) – High Speed Scenario</td><td>18 to 360</td><td>Maximum Power. Refers to both cars and trucks.</td></tr>
<tr><td>Charging time (seconds) – Low Speed Scenario</td><td>N/A</td><td>Depends on vehicle speed and dimensions of the primary charging infrastructure. Possible range indicated below:
<table>
<tr><td>Charging time (sec)</td><td colspan="2">Size of primary charging infrastructure</td></tr>
<tr><td>Speed</td><td>1m</td><td>100m</td></tr>
<tr><td>10Km/h</td><td>0.35</td><td>35.7</td></tr>
<tr><td>50km/h</td><td>0.07</td><td>7.14</td></tr>
</table></td></tr>
<tr><td>Charging time (seconds) – High Speed Scenario</td><td>N/A</td><td>Depends on vehicle speed and dimensions of the primary charging infrastructure. Possible range indicated below:
<table>
<tr><td>Charging time (sec)</td><td colspan="2">Size of primary charging infrastructure</td></tr>
<tr><td>Speed</td><td>1m</td><td>100m</td></tr>
<tr><td>70Km/h</td><td>0.05</td><td>5.1</td></tr>
<tr><td>130km/h</td><td>0.028</td><td>2.8</td></tr>
</table></td></tr>
<tr><td>Vehicle status</td><td>N/A</td><td>Vehicle engine / power is on during the power transfer process</td></tr>
</table>

From the above it can be concluded that stationary charging is a special case of the dynamic charging for 0 km/h velocity and the static charging is a special case of stationary charging for charging time greater than 5 minutes. Dynamic charging is the most technologically challenging mode of the three because of communications and processing very demanding requirements: As one can see in Table 3, when the EV travels at 130km/h, the contact duration between the EV and a charging pad (assuming that the charging pad is 1 meter long) is less than 30 milliseconds. Within this period communication between the EV and infrastructure must be established, the EV must be identified and be authorized to recharge, the primary coil has to be switched on and transmit power at the appropriate level which should be defined by a load balancing algorithm that runs in the charging infrastructure backend. Finally data regarding the consumed power and the state of battery charge must be transmitted from the EV to the charging infrastructure. From the above it can be seen that stationary (where the vehicle remains over the same charging pad for several minutes) or static (where the vehicle remains over the same charging pad for hours) charging can be easily covered by an architecture that is designed for dynamic charging. This is why the next sections describe the functional architecture of a system capable of dynamic charging which satisfies the much more relaxed requirements of static and stationary charging modes as well.

2.2 System functional overview

The functional design defines the main architectural elements of the FABRIC system. In this chapter, the functional structure of FABRIC main subsystems including the key functional elements, their responsibilities, and the information flow between them will be described using interaction models (UML sequence diagrams). This is done in order to demonstrate how the system will implement the functional requirements as described in [1] and [2]. In [1] two types of use cases are defined for FABRIC:

1) The demonstrable use cases provide services to FEV users and external operators and will be realized in the project since they are essential for the evaluation of the wireless charging prototypes and the long-term feasibility studies.
2) The feasible use cases that refer to system operating scenarios with a 2030 vision. In this case several assumptions are made such as seamless and large-scale real-time V2V communications that enable the realization of these scenarios. Since such systems will not be developed and tested in FABRIC, the corresponding architecture is not being considered in this document.

The principle adopted by FABRIC consortium for the system architecture definition is to provide FABRIC services from backend wherever possible, allowing collection and processing of large amount of data from multiple infrastructure systems and from FEVs. Based on this, a high level physical architecture of the FABRIC system is defined in order to identify the main subsystems and their topology as illustrated in Figure 2.

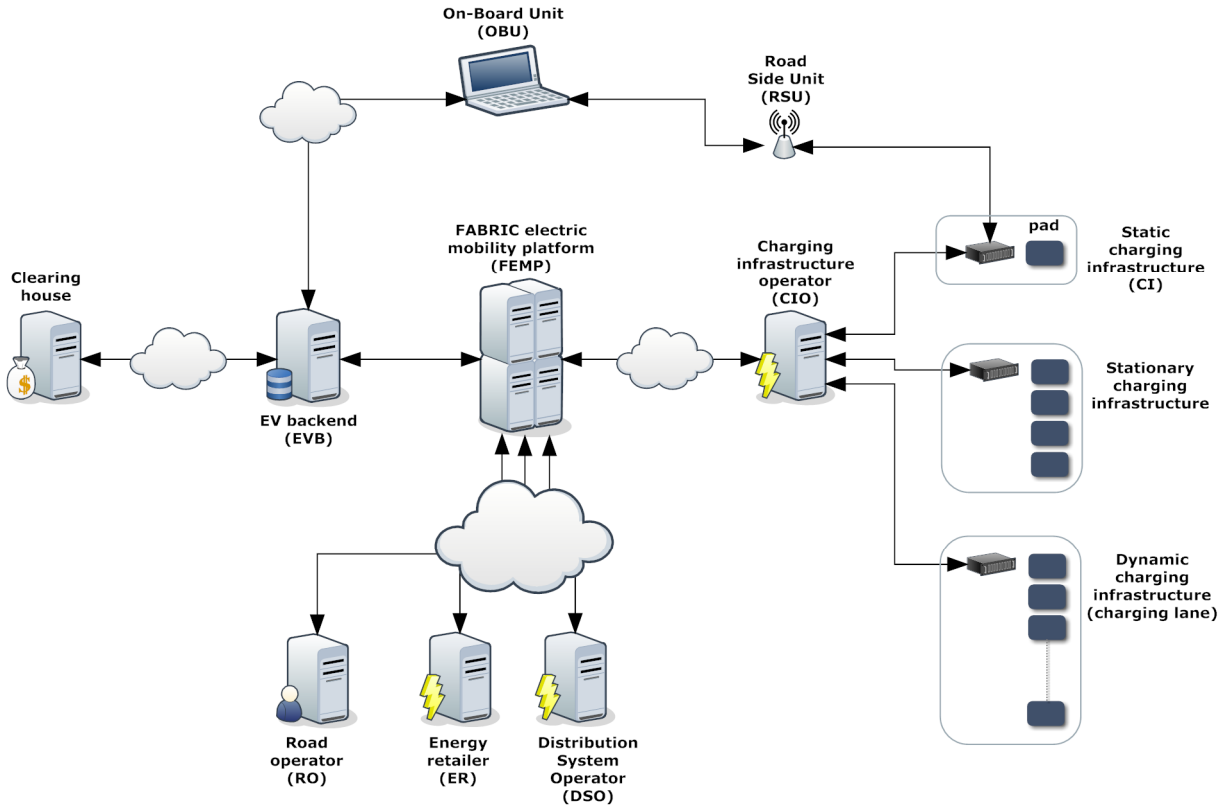


Figure 2: FABRIC high level physical architecture.

Considering only the high level architectural design, the main FABRIC sub-systems are:

- **On Board Unit (OBU)**: This is a machine installed inside the EV that will host the FABRIC applications and provide in-vehicle end-user access to FABRIC services via a HMI. The OBU will be able to communicate with the vehicle ECU and collect vehicle and battery information via the CAN-bus. The OBU will include the communications infrastructure (hardware, software and antennas) necessary to exchange information with external entities, such as the charging infrastructure and RSUs, and the FABRIC EV backend. The OBU will also monitor and control the secondary coil installed under the vehicle.
- **EV backend (EVB)**: This is a machine that will be the main EV access point to FABRIC system. It will host a database that will contain the data of the EVs and their users, EV characteristics and billing information. EV backend will also store in this database the history and data of past EV charges. EVB will provide POI and navigation services to the EVs. EVB will also communicate with the clearing house in order to carry out the payment processes after a successful recharging.
- **FABRIC electric mobility platform (FEMP)**: This machine will be the core of the system and act as information coordination system. It will host all interfaces with the external actors and route the information received to the appropriate recipients. FEMP will host databases that contain information for the state of the whole system such as a database with the charging infrastructures' characteristics and availability status, logs for system usage, etc. FEMP also enables a human system operator to supervise the system operation, filter and assess messages from external actors and set global reach system

parameters such as the formula that is used for the calculation of the final charging cost (which may depend in many parameters).

- **Charging infrastructure operator (CIO)**: The charging infrastructure operator is a machine that controls the charging infrastructure (charging pads), monitors the charging process and transmits aggregated information to EVB and FEMP. It contains a module for balancing the demand from EV charging with the energy supply restrictions imposed by the DSO. CIO also performs EV authentication and authorization tasks.
- **Charging infrastructure (CI)**: The charging infrastructure comprises mainly the primary power transfer coil and its electronics and software that communicates with the CIO and the OBU and monitors and controls the charging process based on the information received by the CIO and the EV. The Charging Infrastructure may have sensors for vehicle detection or it may communicate directly with RSUs for this or other tasks.
- **Road Side Unit (RSU)**: The Road Side Unit is a machine that can transmit information to EVs that are in its vicinity. It can also gather information from EVs and forward them to the CI. It contains the hardware, software and antennas that are necessary for short-range V2I communications.

Associated with FABRIC (but outside the architecture) are also the DSO backend and the Road Control backend (which provides traffic and other relevant information to the FEMP).

2.3 Use case sequence diagrams

Based on the conceptual high-level architecture of the system, the next step was to design in detail the interactions among the various subsystems and between the system and external actors. In order to do that the demonstrable use cases defined in [1] are translated into UML sequence diagrams that show the information flow between the several actors and the system components. The information flow reveals the subsystem functionalities and leads to defining the functional architecture of the components and subcomponents. Below are the sequence diagrams for the use cases of FABRIC.

2.3.1 UC1.1 Registration to FABRIC – end users

The sequence diagram for the registration of end-users (drivers/owners) to the system is shown below. The registration requires (at the very least) the following information:

- User identity and contact information (name, address, ...)
- Accounting related data (this is dependent on the implementation of the system. Most commonly credit card data are requested, perhaps PayPal, or a bank account). An interface with a third party who will validate the data submitted by the user is necessary, as is done with online shops when credit card information is submitted. Other business models may include contracts with EV charging companies following the example of mobile phones billing. However this depends on the implementation of the commercial system and it is out of the R&D scope of FABRIC.
- EV information. The data may contain registration number, model. The model could be selected from drop down menus that include all EV models. In that case an interface with a vehicle database which is always updated is required. The charging characteristics

of the vehicle should not be requested by the user at this point because first it is technical information, second the reliability of information coming from the user is low. If charging is based on erroneous information, there could be damage to the EV and the infrastructure.

- Other information may be required depending on the custom implementation of the system and the services that will be offered (e.g. parking spot reservation, contract ID, etc.).

After the user submits the information and the information is validated, the system produces the login credentials and displays them to the user for future use.

The process is very similar to registering for an Electronic Toll Collection tag (for free-flow road or motorway tolling systems), of which numerous systems and providers exist in Europe. A key difference is that tolling accounts in some cases do not require the vehicle information, as a tag can be interchanged between different vehicles provided they are in the same tolling category (cars, vans/minibuses, different types of bus/coach/truck). This is the case for example in France, but not in Italy, UK or Ireland. For FABRIC, even if a movable tag system is used, linking it to a specific identified vehicle would be necessary as that would ensure that the identity of the vehicle make and model (and hence its technical information) is known, allowing the power transfer to be adapted to the vehicle. Transferring payment tags to other vehicles would risk power transfer adapted for one vehicle type to be applied to another, either causing it not to work, to lose efficiency or to create an unsafe situation.

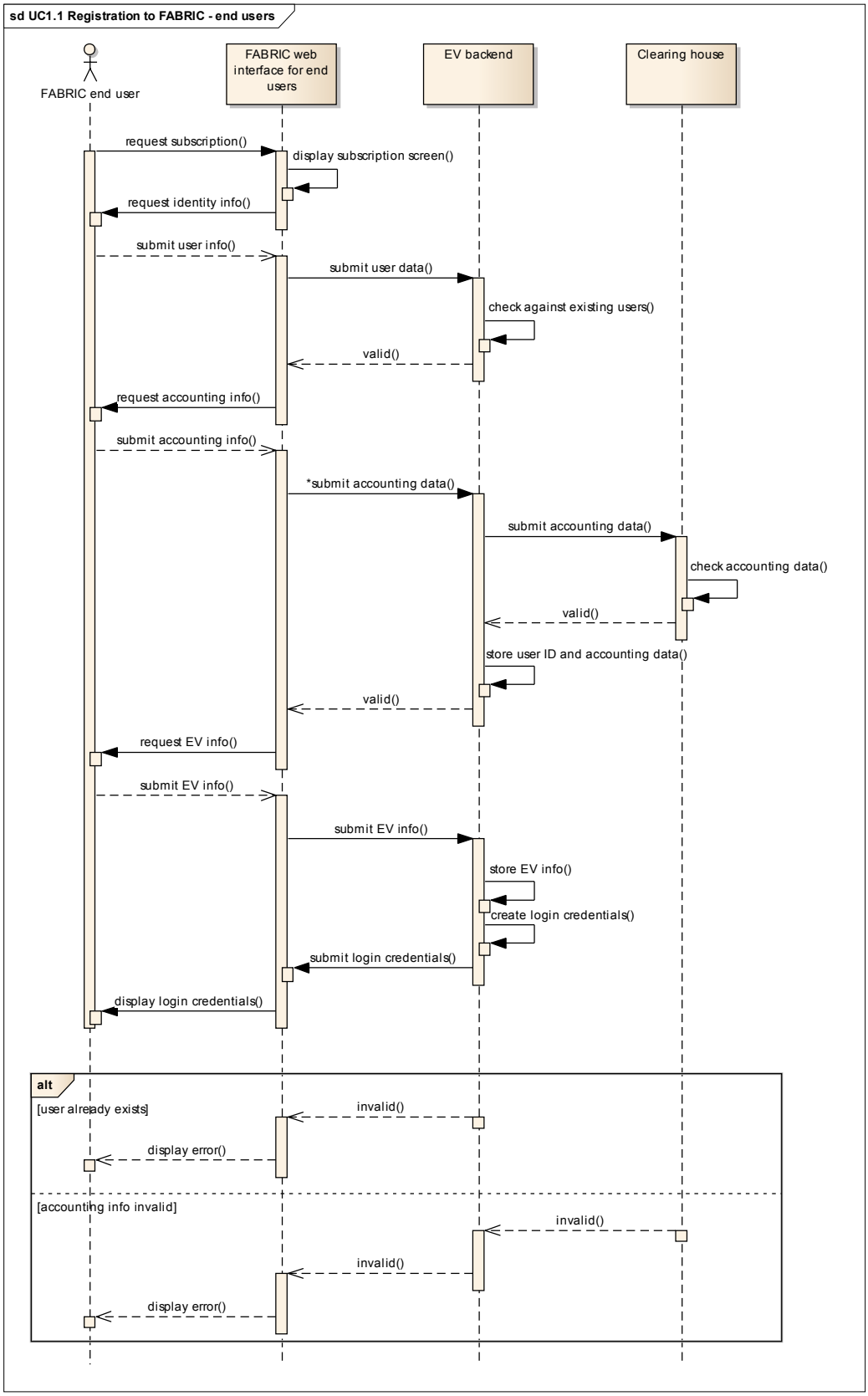


Figure 3: Registration to FABRIC sequence diagram.

2.3.2 UC1.2 Logging into the FABRIC interfaces – end users

This basic functionality enables a registered end-user to access FABRIC services. The logging in can take place either via the OBU of the EV or via a web portal. Depending on the access mode, the interface offers different functionalities to the user. In the following figure the sequence diagram of logging into FABRIC via web interface is shown. This can be done using any device that has access to the web such as desktop computers, tablets or smart phones. By accessing FABRIC in this way, the user has the ability to manage the registration information and profile, to review data and statistics about the charging and payment history, etc. The functionalities offered depend on the custom implementations of FABRIC and the third party services that may be integrated to the platform. This logging in mode is typically expected to take place prior or after a trip.

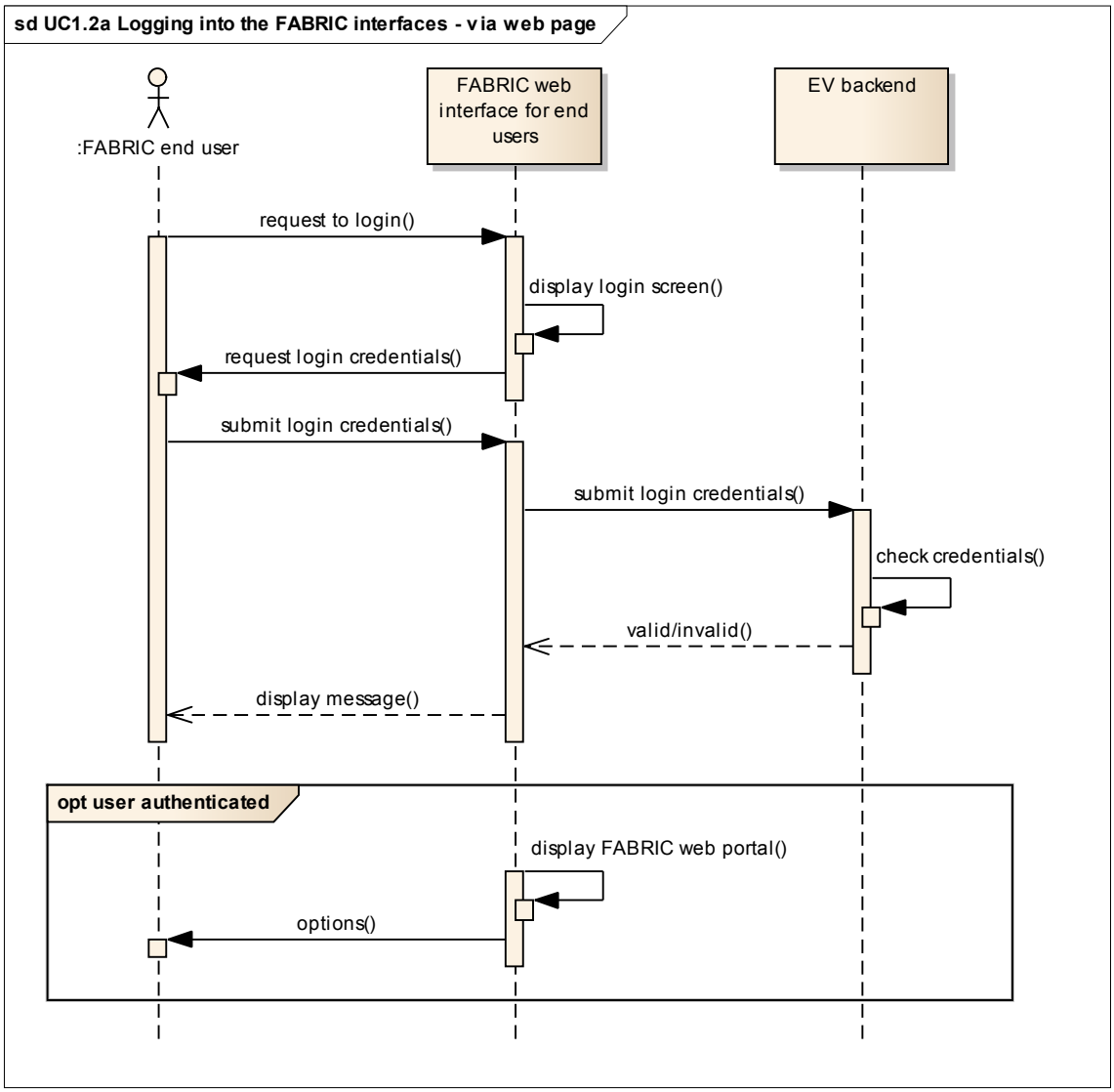


Figure 4: End-user logging into FABRIC via web page sequence diagram.

The second mode of accessing FABRIC will be via logging into the OBU. The OBU will provide a credentials submission dialog box and after the successful login, it will present the user with options that are related to FABRIC services. This mode is typically expected to take place just before or during a trip so that the driver is able to access the charging services of FABRIC. When the user is logged in, in addition to the user's credentials, the OBU submits EV related data to the EV backend to enable FABRIC services. The sequence diagram for this mode is shown below.

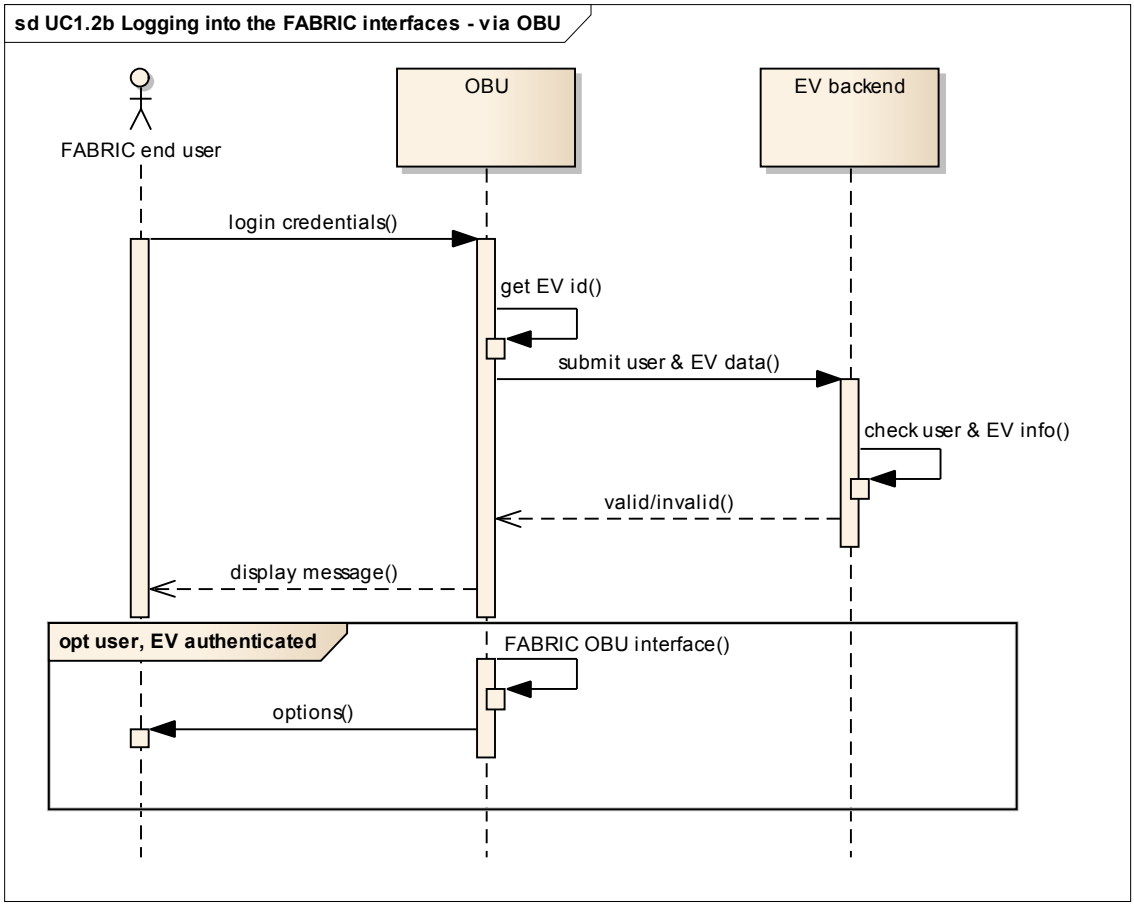


Figure 5: End-user logging into FABRIC via OBU sequence diagram.

2.3.3 UC1.3 User account management

This functionality enables subscribed end-users to edit the information in their accounts or delete them.

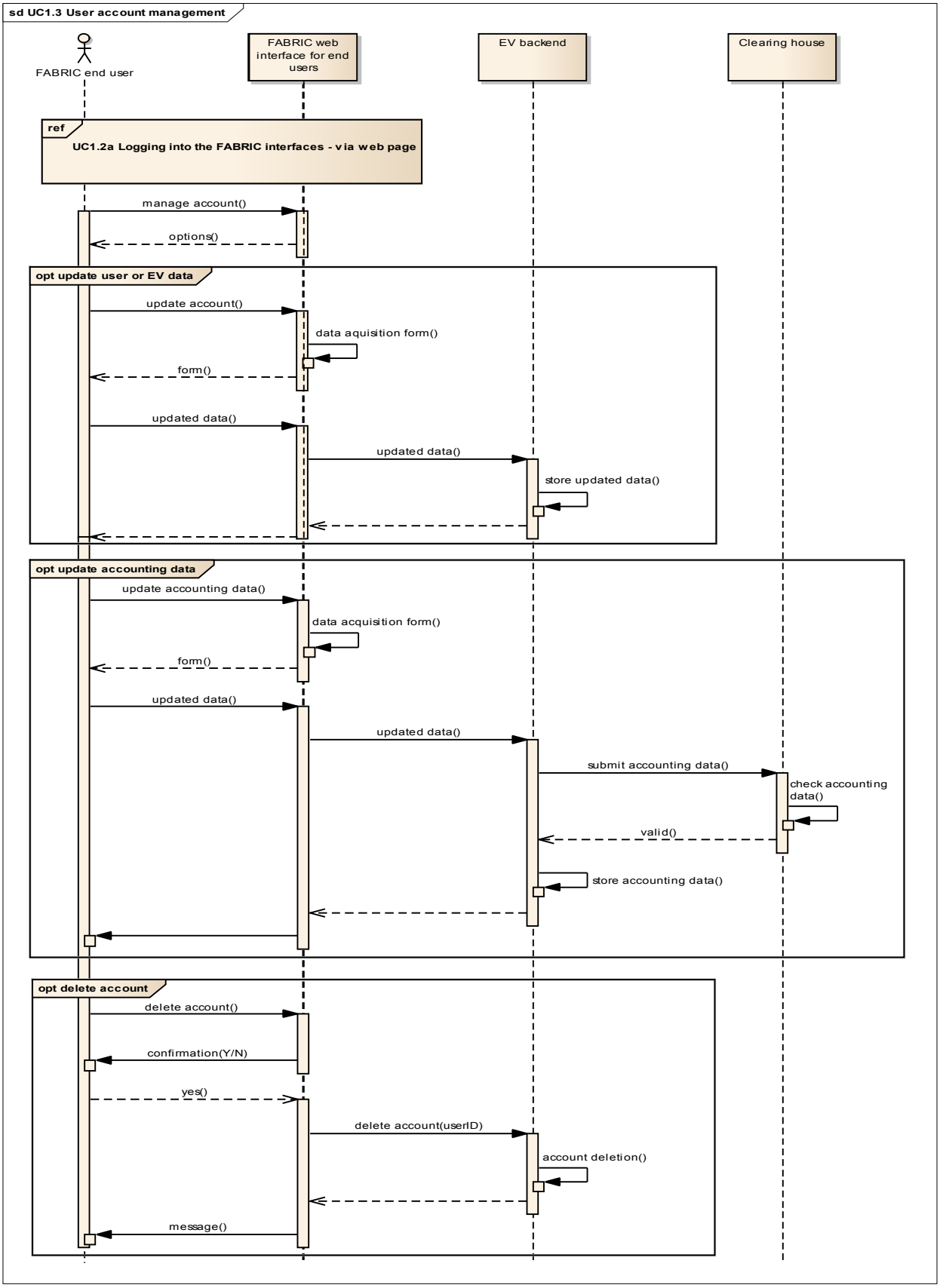


Figure 6: End-user account management.

2.3.4 UC1.4 Trip planning

Trip planning is a functionality that is not essential for the project's goals that are focused on assessing the feasibility and performance of wireless dynamic charging. In addition, trip planning is extensively covered in other ITS projects such as MyWay and electromobility projects that are focused on ICT services such as eCo-FEV. Furthermore FABRIC testing facilities and foreseen tests will not support trip planning functionalities. Trip planning for electromobility is a special case of the optimal navigation R&D field which is addressed by hundreds of GPS navigation OEMs and research projects. For these reasons FABRIC is not expected to develop navigation functionalities and systems but rather provide interfaces for connection with third party solutions.

The trip planning for EVs presents some peculiarities compared to the conventional vehicle trip planning due to the limited charging infrastructure deployment, the increased recharging time and the limited EV range. However large deployment of electromobility (including rapid charging facilities: on-road and off-road) will eliminate these limiting factors and complex trip planning functions such as the one shown below will become largely unnecessary.

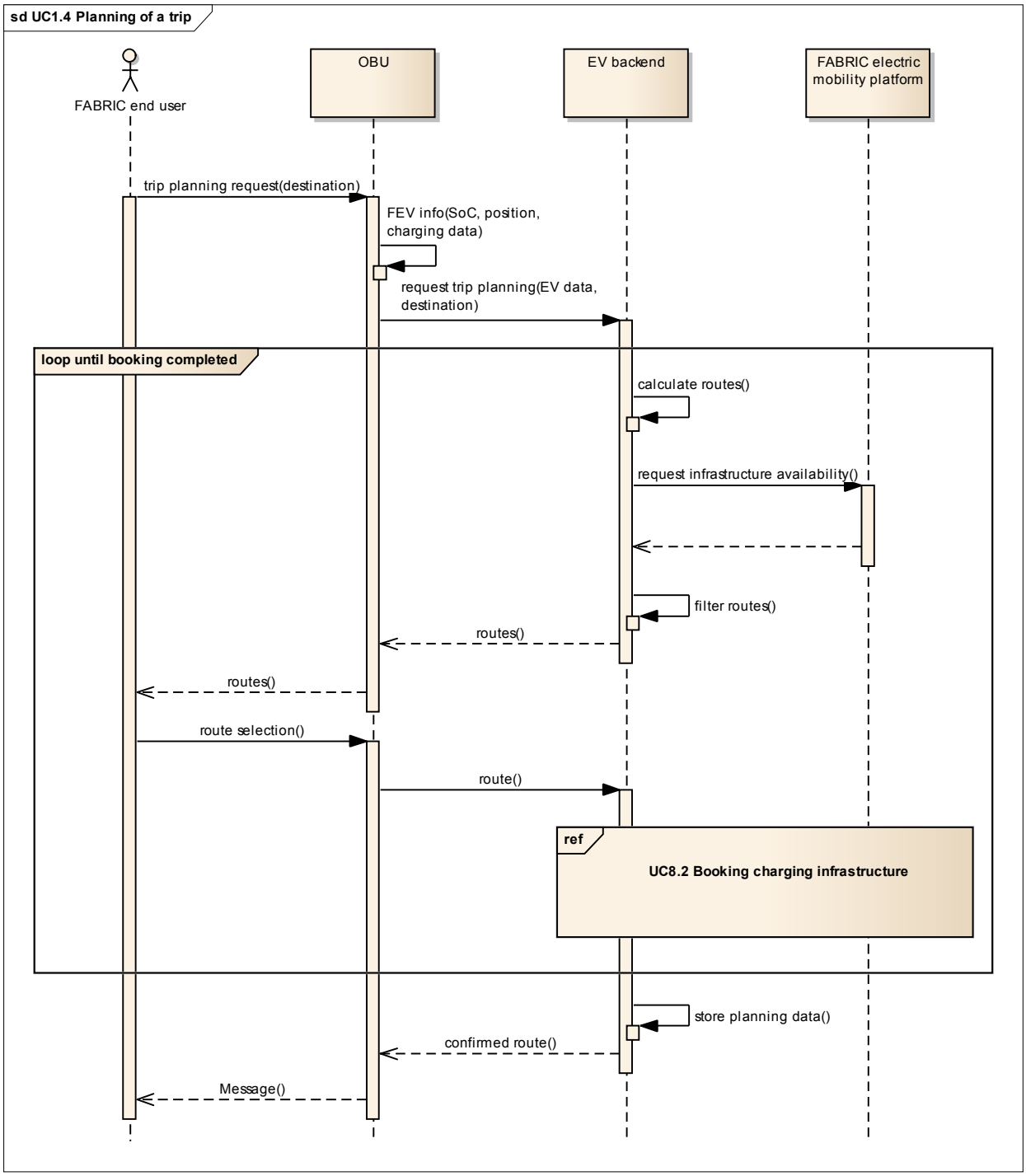


Figure 7: Trip planning sequence diagram.

The diagram above shows the information flow from the trip planning request by the end-user to the delivery of the actual route. It begins with the request via the OBU. The OBU collects EV data regarding the charging profile of the vehicle (static, stationary dynamic capability, fast charging capability, charging power, battery capacity, state of charge, range estimation etc.) and the current position. It forwards the information to the EV backend that hosts the route calculation module. The route calculation module takes into account the charging profile of the

EV to filter the charging infrastructures that are compatible to the EV. It then requests the infrastructures availability information from the FABRIC electric mobility platform that hosts a charging infrastructure status database that is continuously updated. Based on the above information, the EV backend calculates alternative routes and forwards them to OBU that presents the user with routing options like a conventional navigator.
After route selection the system proceeds with booking the infrastructures along the route. In case the availability changes while the user decides on the route, the procedure is repeated. Upon successful booking, the route is stored and a confirmation message is sent. The user can then select to proceed with navigation.

2.3.5 UC1.5 Guidance to charging facility

This is special case of trip planning which is considered separately due to its expected high usage. The main application scenario foresees the ad-hoc guidance of the EV to the nearest available charging facility. However the user might prefer to recharge at a more distant facility so the system displays a list with the charging facilities that are within the EV range, for the user to select. The presented list of facilities will be created by filtering out incompatible with the EV facilities, and facilities that are not available at the estimated time of EV arrival for the expected recharging duration. In that way the end-user is relieved of this burden and the infrastructure booking takes place much faster.

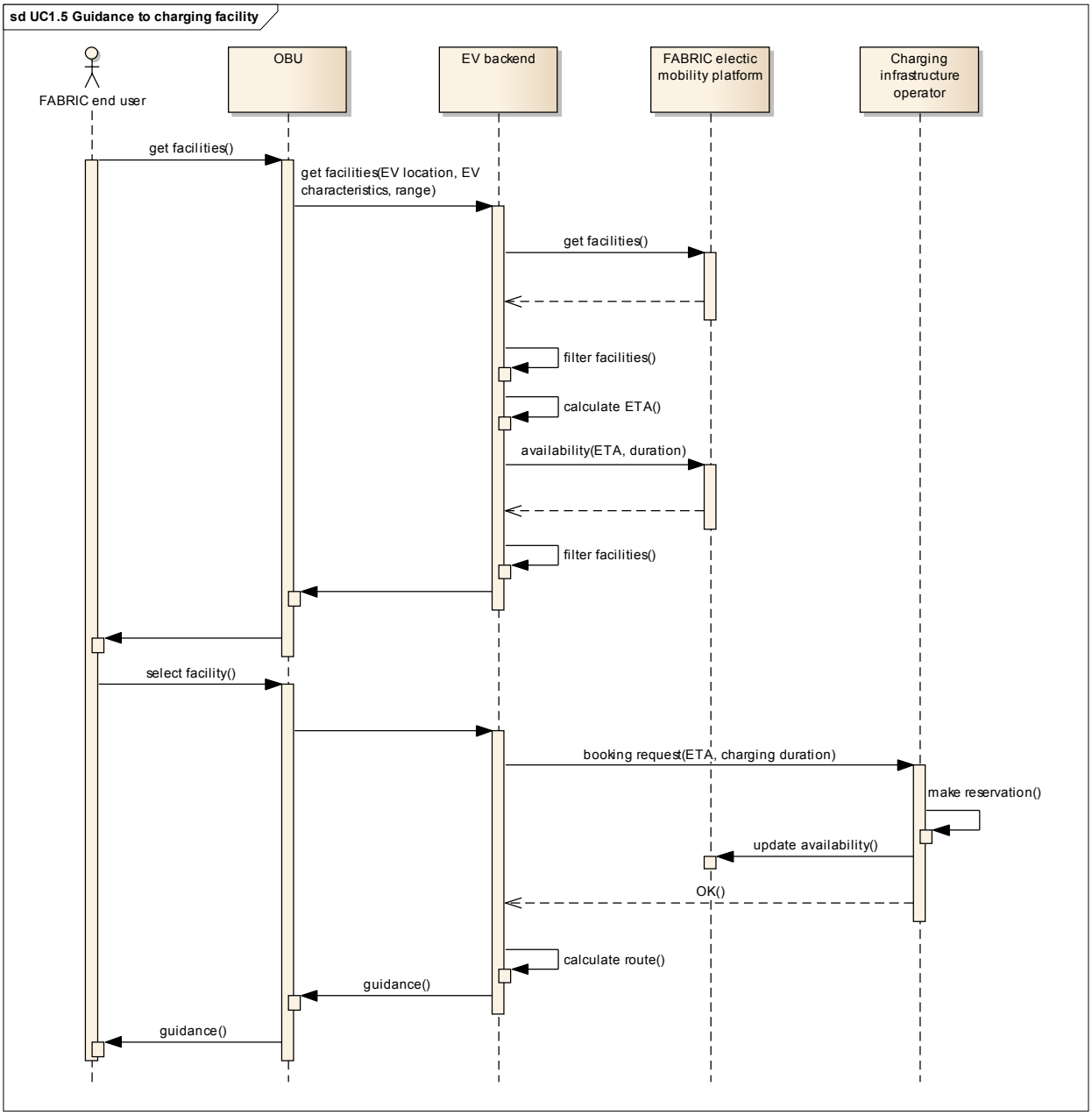


Figure 8: Guidance to charging facility.

2.3.6 UC1.8, UC1.9, UC1.10 Assisted charging – static, stationary, dynamic

This functionality helps the end-user (driver) initiate and complete the charging process. For wireless charging maximum efficiency is achieved when the primary and secondary coils are aligned perfectly. This is possible if the driver is guided to position the vehicle properly, either via infrastructure visual cues (painted marks or lanes indicating the correct parking position) or via HMI instructions similar to the parking assistance systems found in many vehicles. The sequence diagram below describes how such a system could be implemented in FABRIC.

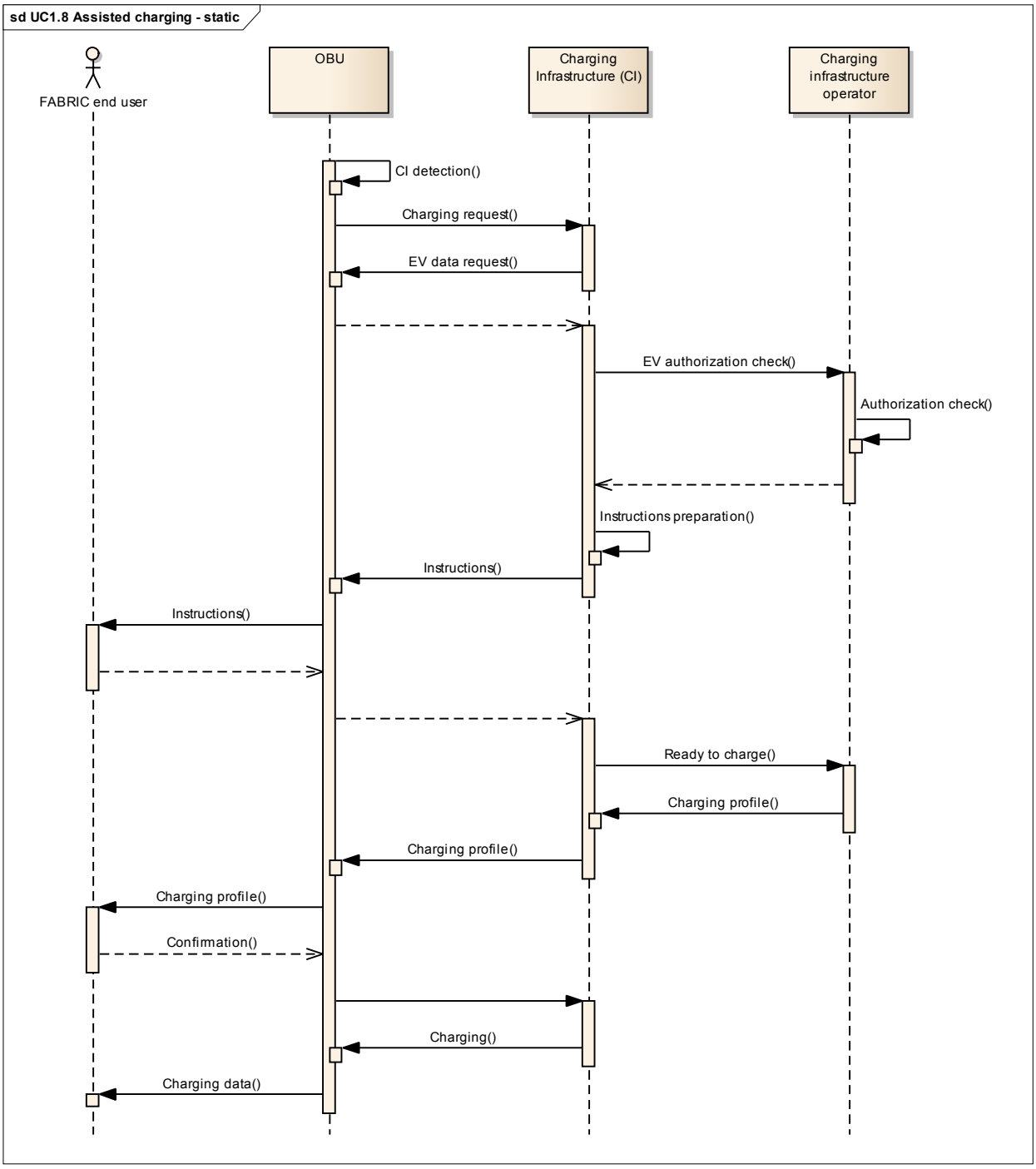


Figure 9: Assisted static charging sequence diagram.

Initially the EV OBU detects a nearby charging infrastructure. This can be done if the Charging Infrastructure (CI) has or cooperates with an RSU that broadcasts its presence at a very small area (so that there is no interference with other broadcasts). After the detection of the CI (so the EV is already in the vicinity of the CI) the OBU sends a request to charge. The charging infrastructure operator checks whether the EV should be authorized to charge. This can take into account many parameters such as infrastructure pre-booking by the EV, grid restrictions, etc. After the EV is authorized to charge it receives instructions on how to optimally align the

coils. The instructions depend on the way the system estimates the misalignment and they can be transmitted to the driver via an In Vehicle Information system. After the alignment is successful, the charging may begin based on a custom charging profile for the specific EV, and the driver is notified about the charging progress.

Notes:

- Pre-booking of CI for stationary and dynamic charging is not possible due to the opportunistic nature of these modes. For example in stationary charging, booking of an infrastructure at a traffic light or junction is not possible, but rather the driver should be presented with the option to charge if the EV happens to be stationary on top of such CI. In that way, the sequence diagram for the assisting functionality does not differ from the one for static mode but only the internal processes e.g. for EV authorization to charge the infrastructure operator will not consider the booking of the infrastructure.
- For dynamic charging due to the speed of the EV and the very low duration of charging per pad (for example it is estimated that for 130km/h the "contact" duration per pad will be less than 30 ms), coil alignment assistance will probably be based on infrastructure visual cues since there will be no time for position detection and misalignment estimation per pad. In addition providing HMI based instructions during charging while driving at high speeds may be distracting and dangerous.
- ADAS may be the solution to the proper alignment during dynamic (or even static and stationary) charging in the future. However currently the technology is not mature enough, there are a lot of ADAS approaches using different sensors and different inputs (camera-based, laser-based, platooning techniques based on radars) to achieve the desired result. Each company develops its own system that implements a custom subset of driver assisting functionalities, ranging in the most advanced cases from automated parking to automated driving, so there is no ADAS "standard" that can be considered at this point for application in FABRIC. On the other hand the developing partners are at the moment of writing not specific about the means they will use to perform the optimum alignment during charging so in this document the simplest approach was selected in order to ensure that there isn't a significant inconsistency between the deliverable and the actual developments.

2.3.7 UC2.1 Charging supply management – high level

This functionality provides the DSO with the ability to manage the maximum power of a specific charging facility or even set a charging facility offline in order to ensure grid stability during emergencies. This is also useful in order to shape the load at peak demand times while reserves are low or energy from RES is lower than anticipated.

The DSO initially has to login successfully to the FABRIC interface and then by selecting the charging infrastructure he/she is able to manage the maximum power for this infrastructure. Depending on the implementation model, more information can be transmitted, such as time interval for which the limitation is valid or a daily schedule. The information is then transmitted to FABRIC electric mobility platform which stores the request along with DSO ID and timestamp (for non-repudiation purposes) and then forwarded to the charging facility. After the operating

limits change confirmation, FEMP updates the characteristics of the facility in its database and messages EV backend to readjust the trips of the vehicles that have already booked this charging facility.

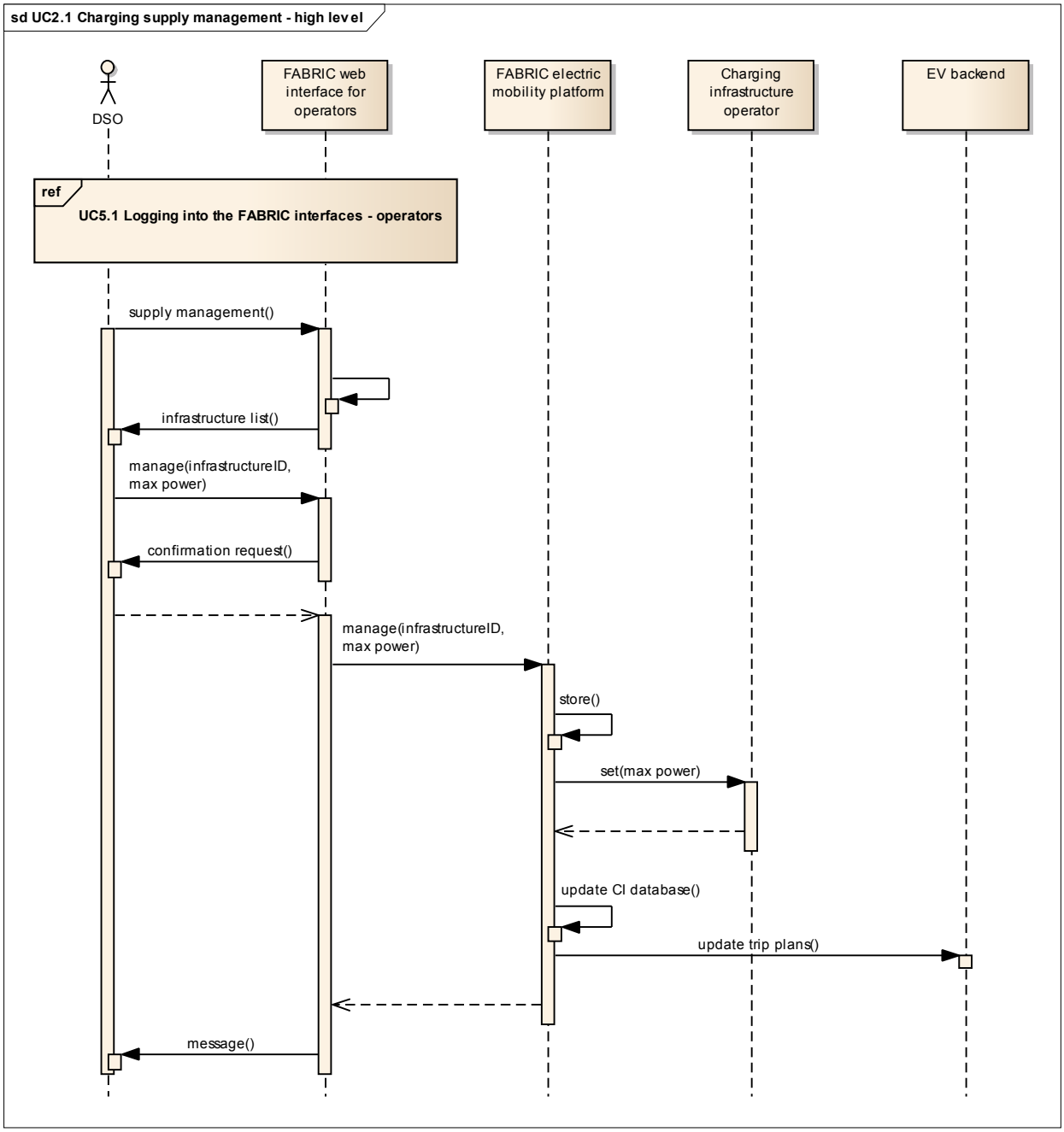


Figure 10: High level charging supply management sequence diagram.

2.3.8 UC3.1 Energy supply tariff modulation

In FABRIC the energy retailer is foreseen as external actor. This actor will provide the energy pricing (tariff) for charging the EVs. Based on this information, FABRIC will be able to calculate

(using a formula that is dependent on custom system implementations) the charging cost for each session. The energy cost may be global for all FABRIC-controlled facilities or dependent on the charging facility id in case there are different contracts between charging operators and the energy retailer. Several energy retailers may also be foreseen, and a feasible FABRIC system could act as energy marketplace hub for the charging infrastructures it supervises. Below, the simplest case for one energy retailer who is able to change the tariff information that is applicable globally is shown.

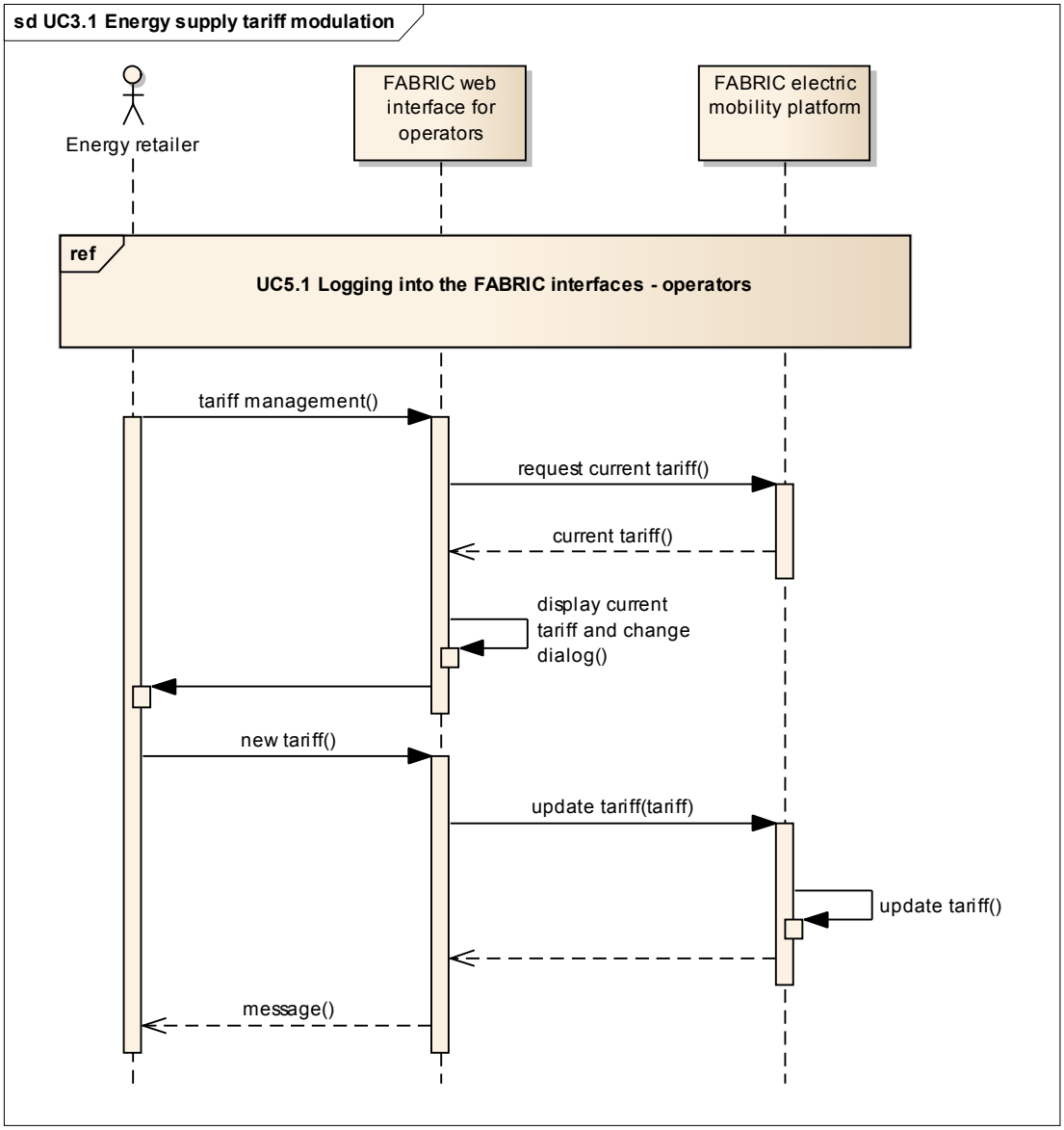


Figure 11: Energy tariff modulation sequence diagram.

2.3.9 UC4.2 EV identification

The vehicle identification and the access control to recharging zones, whether static or dynamic, is crucial for proper charging authorization and billing activities. Being able to identify

authorized vehicles and at the same time to prevent fraud is one of the primary tasks in the management of a charging resource.
In addition, with a proper policy for identification and access control, the FABRIC system can create charging specifications for each type of user and EV, thus optimizing the resources of the charging system. As shown in the sequence diagram of Figure 12 two identification methods can be implemented. The default identification method is for the EV to transmit EV identification data to the charging infrastructure when they are in proximity. The second method is using Automatic Number Plate Recognition camera-based system to identify the EV from a distance. The second method can be used in addition to the first one in order to provide some time for the charging infrastructure operator to prepare the custom charging profile or to make pre-charging arrangements. This however depends on custom implementations of the system. ANPR method can be used to also control access to a charging lane and as an offline means to verify that the EV ID transmitted by the OBU is the real and not a fake one (OBU hacking). EV identification data will be transmitted to the FABRIC electric mobility platform for storage and availability to other FABRIC subsystems upon request.

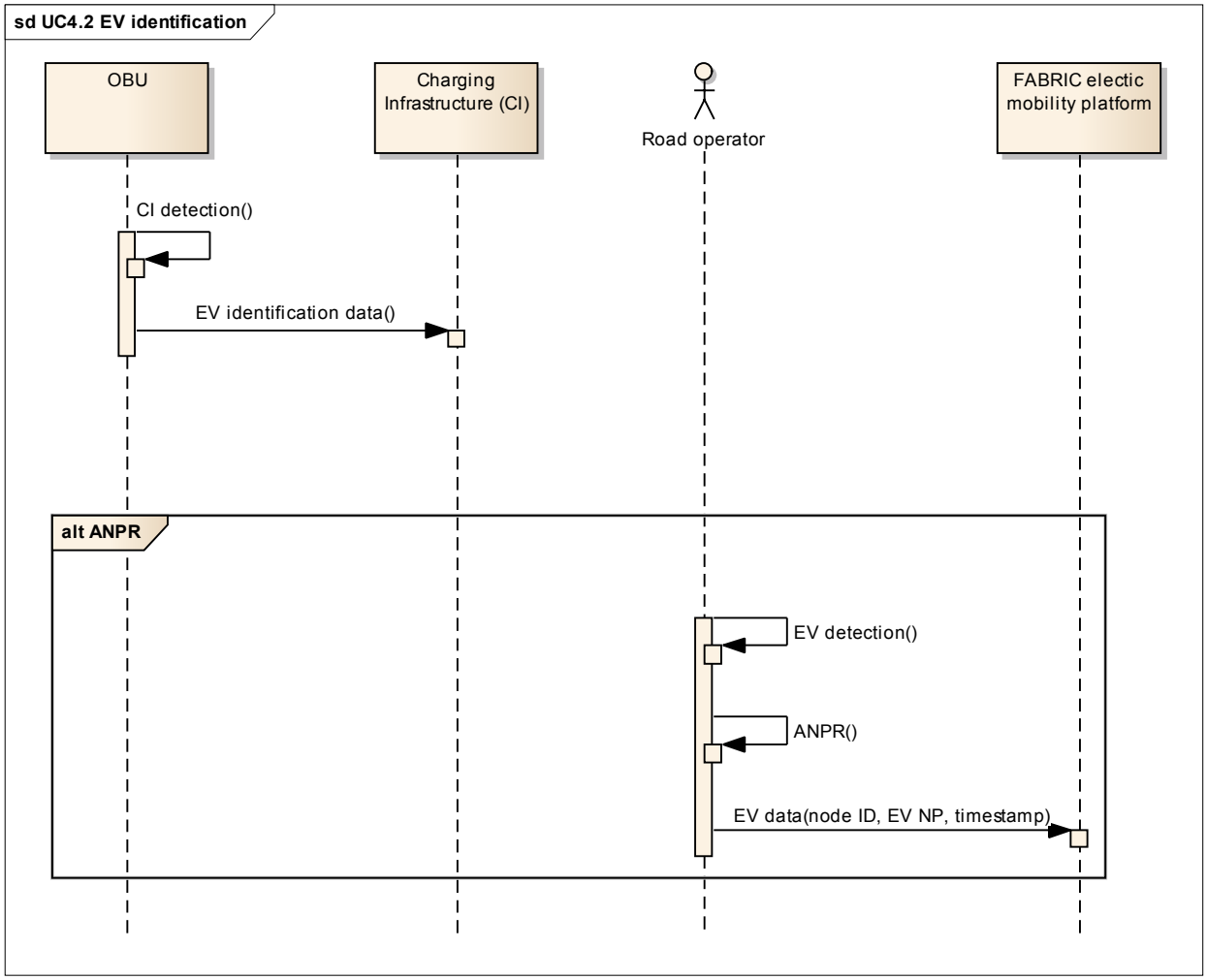


Figure 12: EV identification sequence diagram.

2.3.10 UC4.3 Charging or road infrastructure availability status updating (scheduled)

The charging facility and road operators need to have the ability to schedule the availability of the infrastructures under their control. In that way they can inform the system about scheduled maintenance periods or downtimes due to various scheduled reasons. The operators can login to the operator interface of FABRIC and manage the availability of the infrastructures. The system should display only the infrastructures that are assigned under the specific operator's control during the operator subscription process. In that way it is prohibited for one operator to manage the availability of other operator's facilities. The availability of the infrastructure is updated in FEMP CI database and a message will be sent to the EV backend to update the trip plans of the EVs that have booked the relevant facilities.
It can be envisaged that scheduled availability management could be done automatically without the need of a human operator input if the appropriate interfaces between the road/charging operator systems and FABRIC are in place.

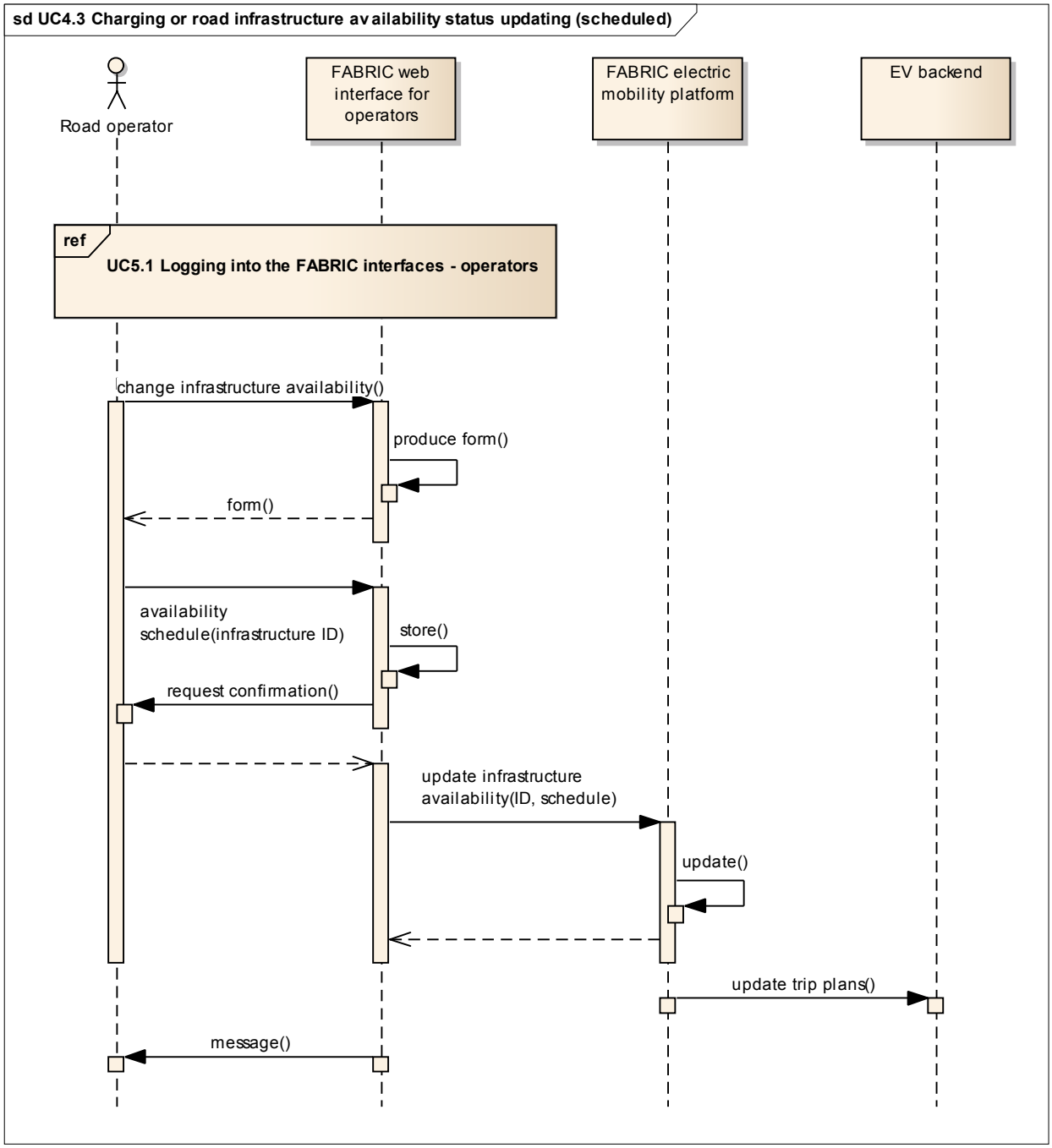


Figure 13: Facility availability status updating sequence diagram.

2.3.11 UC4.4 Charging or road infrastructure availability status updating (unscheduled)

This functionality addresses the need to directly manage infrastructure availability as fast as possible due to unforeseen circumstances such as road accidents, extreme weather phenomena, electricity blackouts etc. The difference with UC4.3 is only the FABRIC interface option at this point; however the functionality could be automated and thus drastically faster if

there is an interface with the road operator traffic monitoring system that feeds DATEX II messages that are then translated to availability signals for each infrastructure item that is affected by the incident.

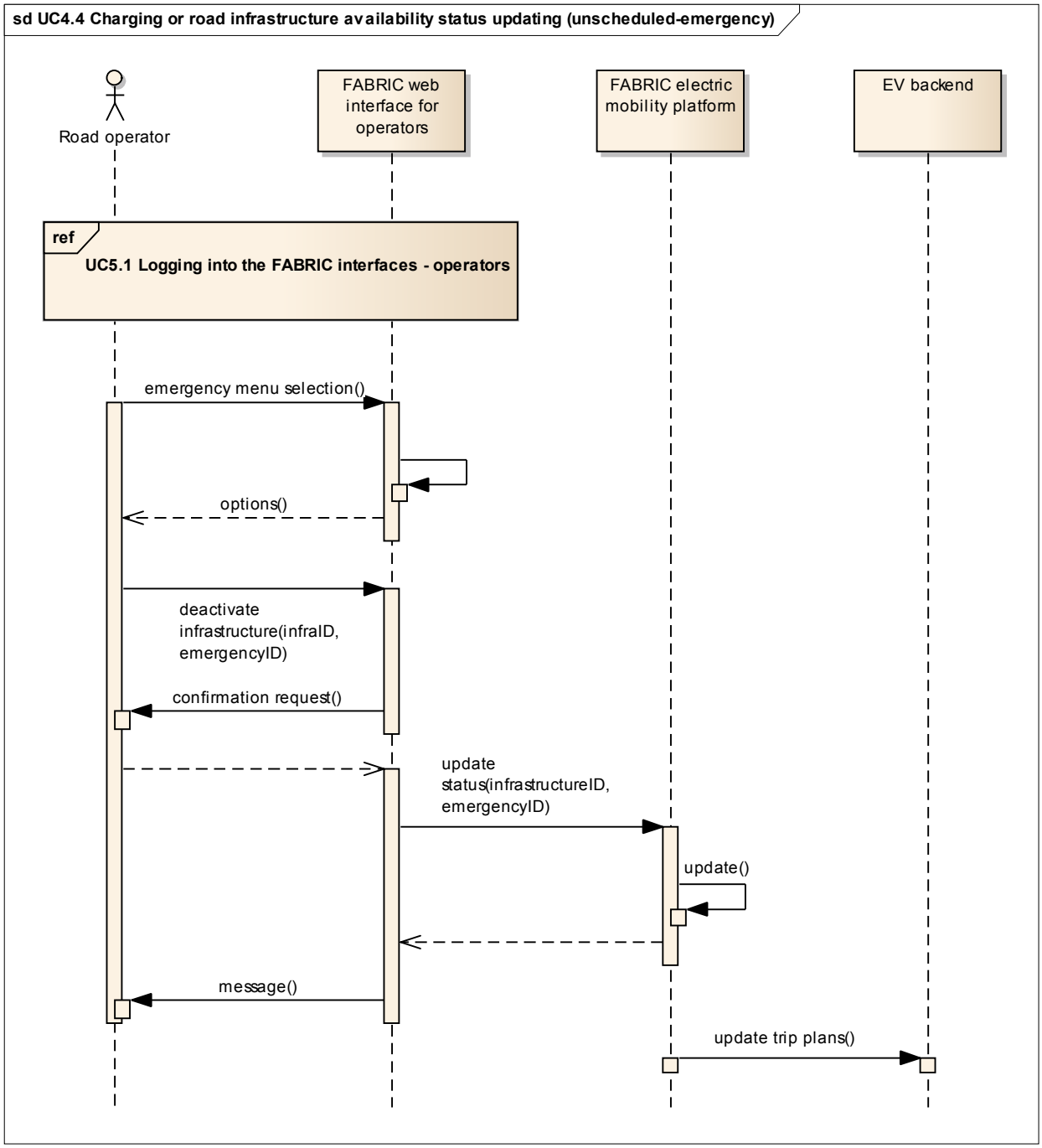


Figure 14: Charging or road infrastructure availability status updating during emergencies.

2.3.12 UC5.1 Logging to the FABRIC interfaces – operators

Below is the sequence diagram for operators' login to the FABRIC system from a computer with internet access. By logging into the system the operator will be able to access a FABRIC web portal for operators and will be able to send messages and perform operator specific tasks. FABRIC portal will be customized according to the type of operator and will offer operator-specific functionalities. Logs will be kept for security purposes.

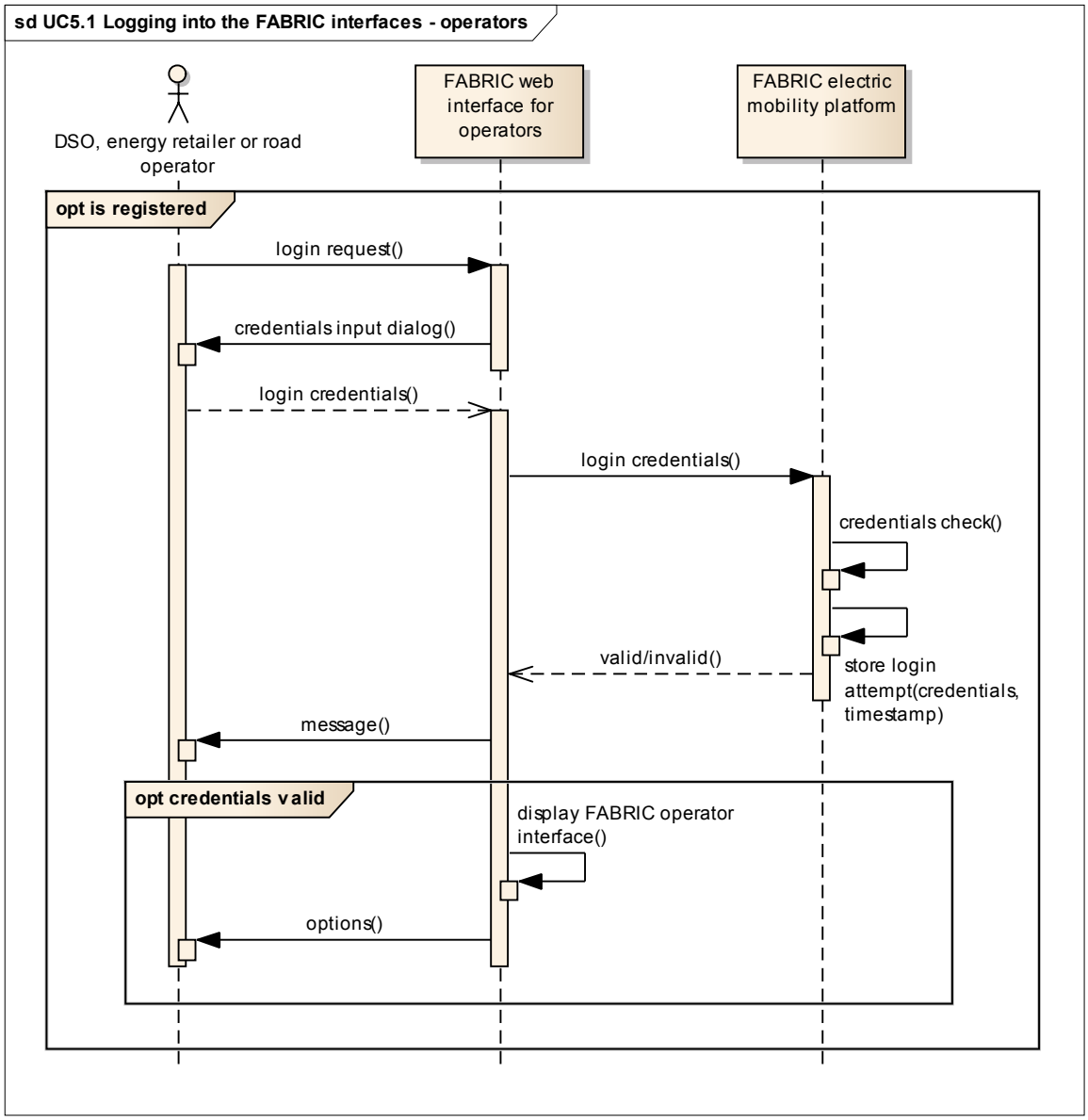


Figure 15: Logging into the FABRIC interfaces for external operators.

2.3.13 UC5.2 Messaging to FABRIC platform - operators

Figure 16 shows the operator messaging information flow. The operator actions are stored in FEMP for non-repudiation reasons. After the reception of the message actions follow depending on the message.

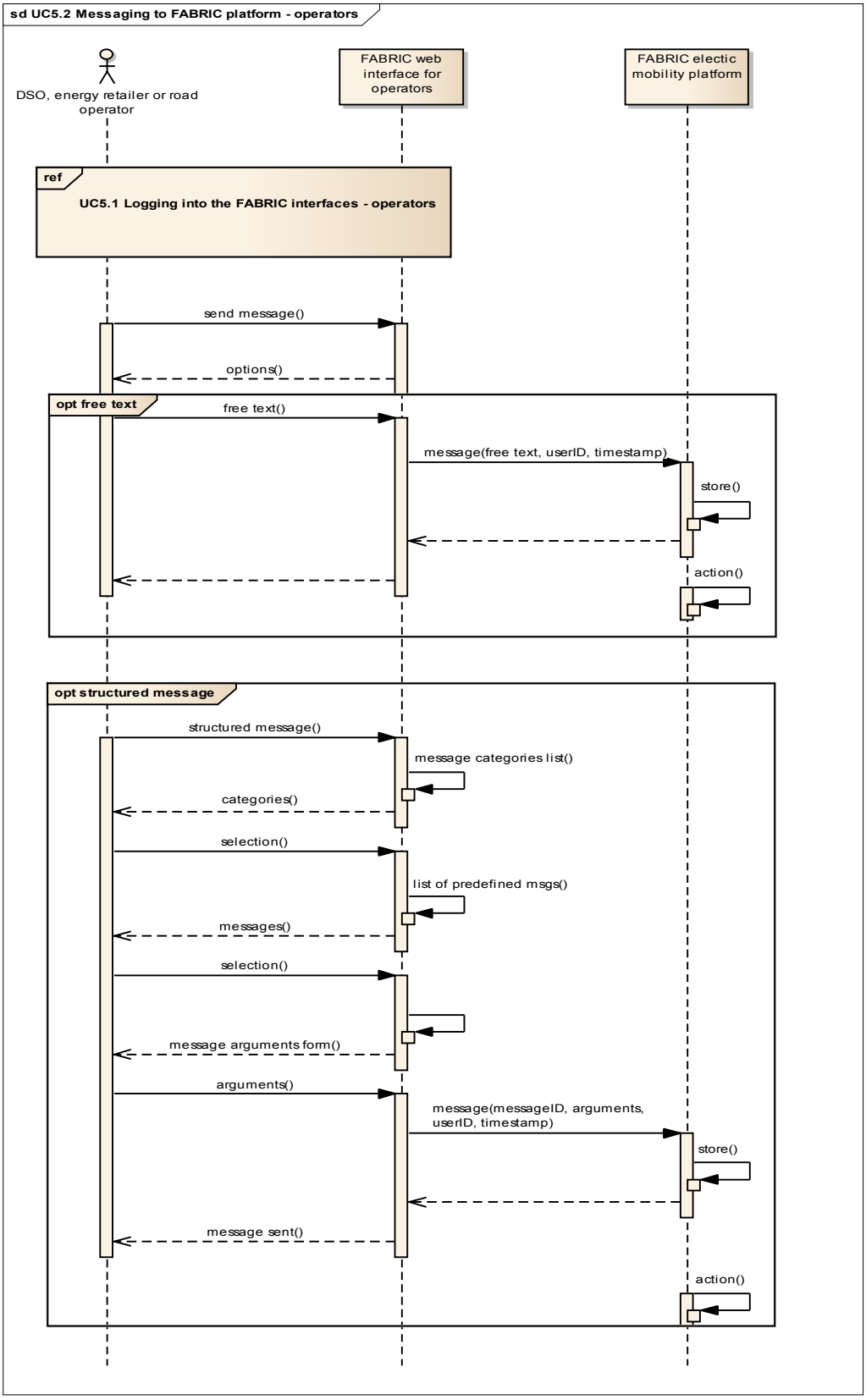


Figure 16: Structured and unstructured operator messaging.

2.3.14 UC6.1 Dynamic routing and booking management

Guidance to a destination for EVs differs from the classic GPS based guidance because it needs to take into consideration the EV's range, the time to recharge, the locations and availability of charging infrastructure so as to guarantee that the EV has enough energy to reach the destination. The importance of a system that takes into account automatically information from various sources and guides the driver in a seamless and unobtrusive manner increases with the scarcity of charging infrastructures and the charging duration of the EV. The fewer infrastructures are installed and the longer the charging duration, the more careful and meticulous the trip planning and monitoring has to be in order to avoid lengthy delays and potentially EV immobilization due to drained battery.

Figure 17 depicts the information flow among the various subsystems while the EV is en route, in order to address issues that were not present during the initial trip planning. Such issues could be:

- Significant delays in reaching the booked charging infrastructures on time due to traffic, weather, etc.
- Changes of the charging infrastructures' availability status due to malfunction or other reasons.
- Changes of the charging infrastructures' operational characteristics due to DSO imposed restrictions.
- Obligatory traffic re-routing.

In case the EV backend detects a significant deviation from the original planning, it notifies the driver of the situation and proceeds with calculating alternative solutions. It receives the available charging facilities within the range of the EV and it filters them based on their availability at the estimated time of EV arrival and the foreseen recharging duration. Using this subset of charging facilities as nodes EV backend calculates alternate routes to reach the original destination and presents them to the driver. The driver selects one and the system makes the booking of the charging facilities included in the route, while it cancels the reservations of the previously booked charging facilities. When reservations are in order the system guides the driver as a regular GPS. The whole monitoring and routing adaptation process is continuously running during the trip.

This use case will not be tested during the FABRIC project since there are no suitable testing facilities and the necessary network of charging infrastructure and it is studied in terms of feasibility for a future FABRIC-like system.

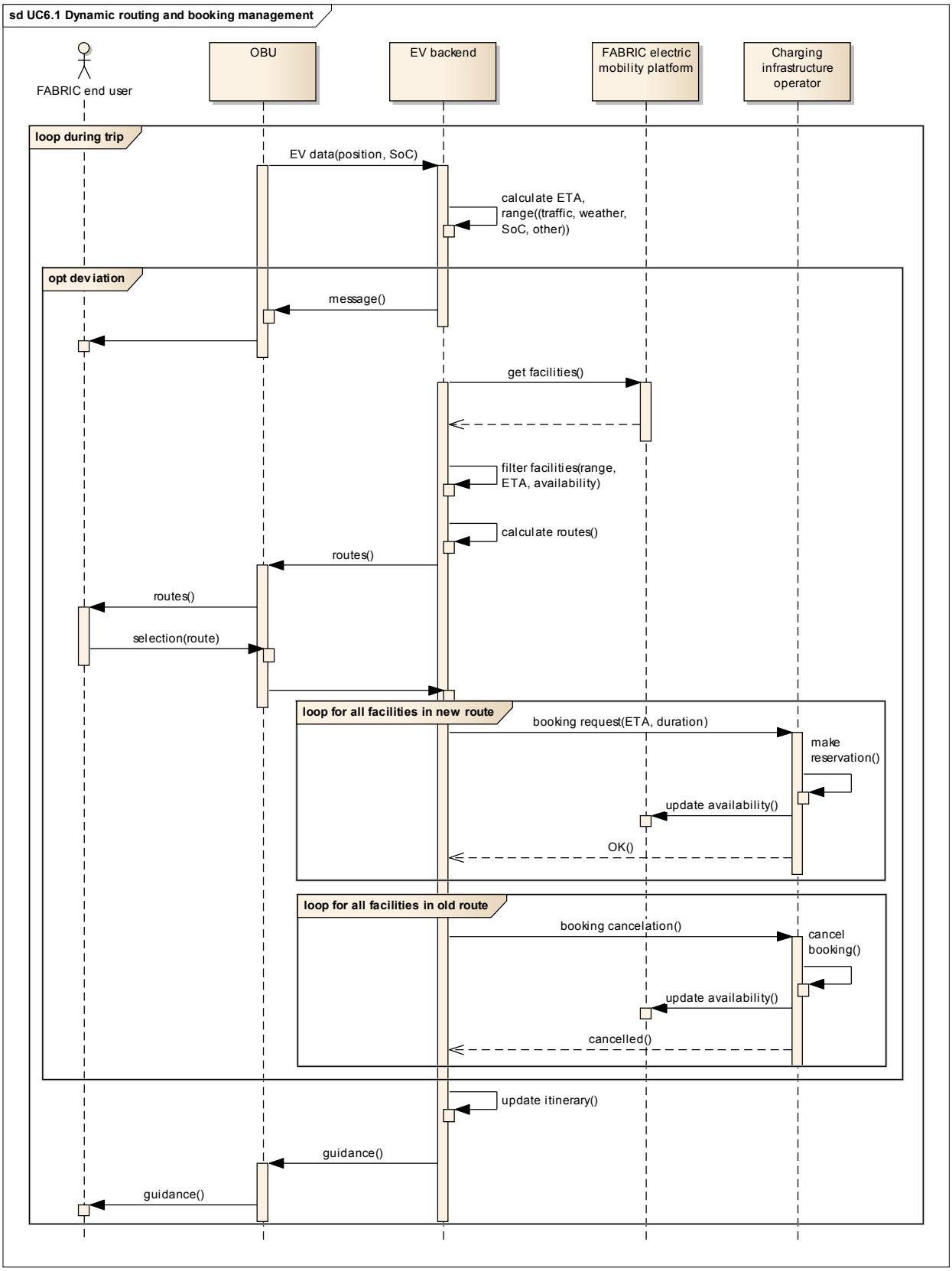


Figure 17: Dynamic routing and booking management

2.3.15 UC7.2 Charging management – dynamic and stationary

Figure 18 depicts the complex transactions among several FABRIC subsystems to enable EV charging while driving (static and stationary charging modes are also covered by this case). Initially the driver indicates the intention to recharge. This is communicated to the EVB along with current EV information necessary for the charging. EVB makes sure that the charging infrastructure is operational and available and validates the request. The charging assistance process is then followed leading the EV driver until the charging initiation. During charging the charging profile is being created and updated depending on real time information deriving from the EV and the grid. The process is being monitored and charging data are recorded. With the completion of charging data from the EV and the CI are transmitted to the EVB for processing, resolution of data mismatches (power transmitted vs power received vs battery charge) and cost to be billed estimation.

Note:
Regarding the measurement of power transfer (for billing purposes) the simplest solution would be to measure the power at the OBU and transmit the information to the system. This is similar to what is done for domestic consumption where the power meters are installed locally. However this introduces two risks: the first one is tampering with the data easily since the end-user has physical access to the vehicle (OBU). Hacking OBU in order to transmit inaccurate power transfer data is a very feasible scenario due to the level of access the end-user has to the OBU. The second risk is that the driver will have no incentive to reach optimum power transfer efficiency (accurate driving during charging) if he/she is billed based solely on the energy that has reached the vehicle (and not the energy transmitted by the infrastructure). This will lead to big differences between what is transmitted and what is received and losses for the charging company, DSO etc. This is not an issue with home consumption or wired power transfer in general since it is assumed that all of the transmitted power reaches the consumer with minimal loses. To address these issues a hybrid solution is envisioned where the power transfer is measured both at OBU and the infrastructure. The two values are then transmitted to FABRIC for comparison and processing. This gives flexibility to the companies on how to handle differences between the data from the vehicle and data from infrastructure, perhaps by introducing a cost formula that is a function of these two values. It is not in the scope of FABRIC to specify this formula (which will be tailored according to custom business plans at the commercialization phase) but to provide the technical means to gather the necessary data from both sources.

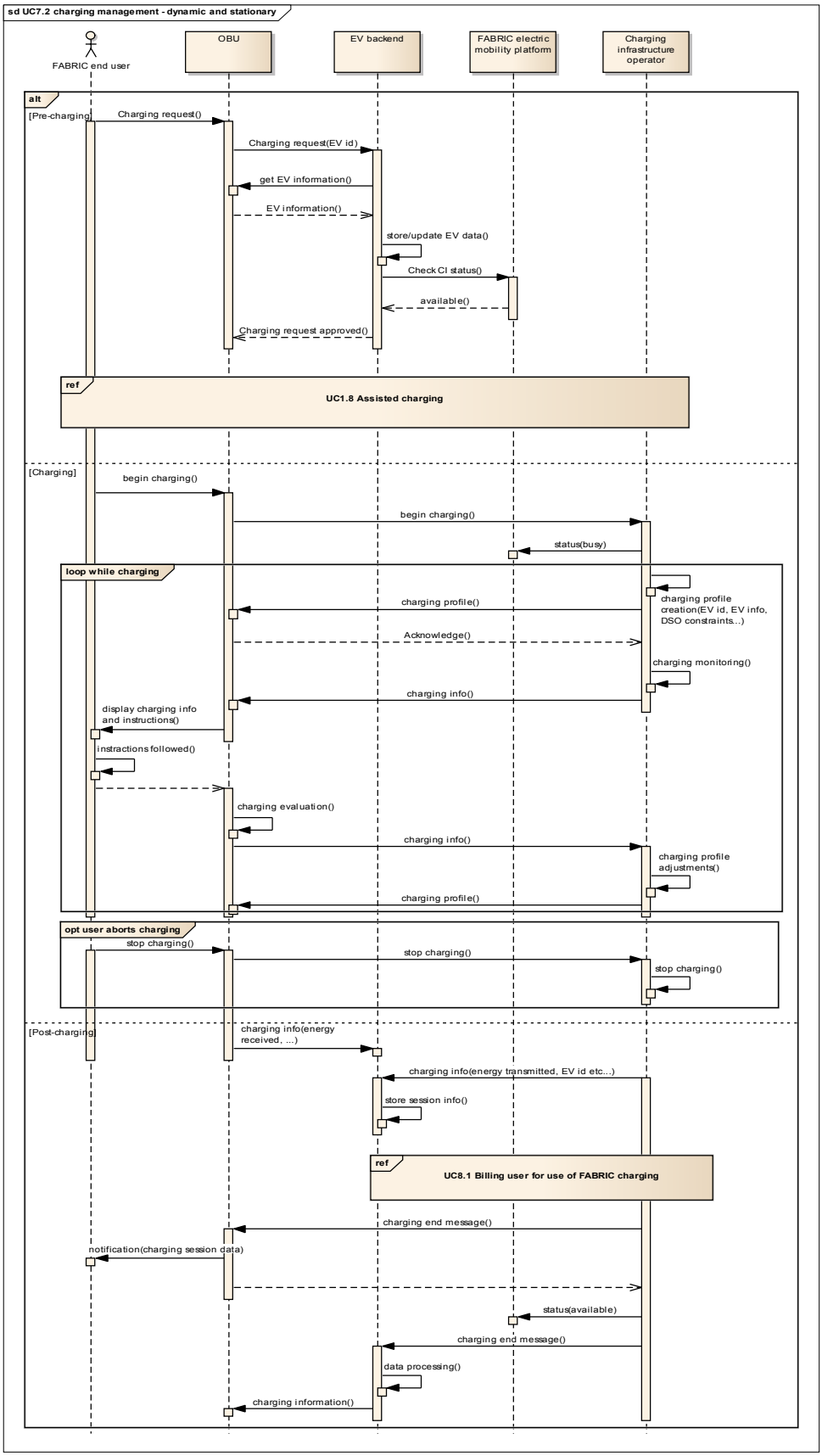


Figure 18: Charging management for dynamic and stationary charging.

2.3.16 UC8.1 Billing user for use of FABRIC charging

The billing process follows each successful charging session. Initially the charging infrastructure operator submits charging session data to the EVB. This includes the energy transferred measured from the primary (infrastructure) side, the id of the EV, timestamps of the session etc. FABRIC EVB also retrieves the corresponding information from the EV. A process to reconcile differences between the data deriving from the two sides may take place in order to estimate the amount of energy to be billed. However this depends on the custom commercial implementations of the system and their business planning. The energy can be priced using a cost formula which will depend on the cost factors imposed by various stakeholders and service providers and perhaps take into account penalties for improper or inefficient system usage. The cost information is forwarded to an external third party that realizes payment transactions based on the business model selected during implementation. Upon successful financial transaction, the receipt is provided to EVB for archiving in the user's account and to the charging operator or other stakeholder.

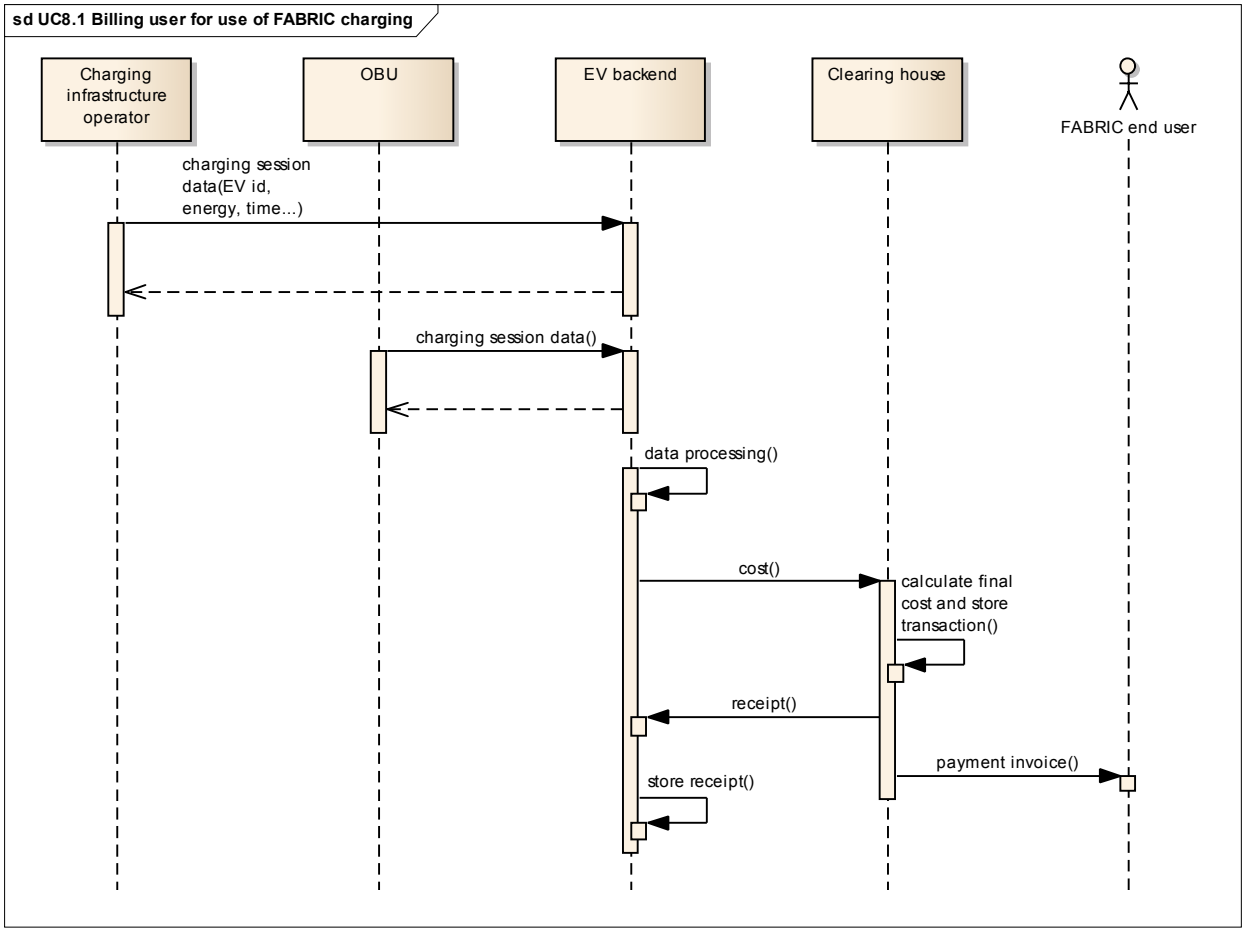


Figure 19: End-user billing.

Note:

The current paradigm with petrol stations and stores in general dictates that the financial transaction takes place at the point of sale. In this case, CIO should be the contact point with the clearing house entity and not the EVB. Such a solution has several drawbacks:

- The billing information of all end-users would be available to each CIO every time the CI was used. Dissemination of personal information to multiple recipients on a daily basis is a significant security risk and an invasion of privacy.
- Difference between energy transmitted to and energy received by the EV is certain to exist, especially during wireless power transfer at high speeds. Having a central strategy on how to address these differences and reach a final cost estimate based on several parameters cannot be implemented with a decentralized billing architecture.

On the other hand if billing is carried out centrally by the FABRIC EVB, monitoring, storing and management of billing processes is easier and with the proper measures more secure to implement. In addition the billing information is readily available to the user and stored in the EVB database without further communication with remote operators. Due to the nature of FABRIC services and the given ICT infrastructure, it is possible to leave current billing models that are usually built around the assumption of physical payment transactions and utilize a centrally managed and monitored, fully electronic payment model.

2.3.17 UC8.2 Booking charging infrastructure

Charging facility booking, especially when the charging infrastructure facilities are sparse, is important in order to avoid congestion and unavailability issues that will increase EV user anxiety. Reliable trip planning is feasible only if the EV is able to recharge with a high degree of confidence (this is not an issue with ICE cars since gas stations are installed very densely and refuelling takes only 2-3 minutes so station availability is always high). The EV may need to charge several times during a trip in the worst case scenario (in reality, during daily urban transits which is the vast majority of transits, refuelling once every day or even every three days or less during the night is enough – tesla motors model S boasts a 470km range). Due to the complexity of the infrastructure booking it is foreseen that this functionality will take place automatically by the EV backend based on route and infrastructure availability information. In addition, in case of rerouting during a trip, the user should not have to deal with the task of manual booking which is time consuming and very distracting process. At most, the users should only provide confirmation on very high level booking decisions made by the EV backend, like overall route cost which is similar to the functionality of regular navigators with the difference that now there is the charging cost information to consider in addition to route length and estimated traveling time.

The sequence diagram is shown below. The EV backend initiates a booking request providing the facility ID, the EV data and the booking period. FABRIC platform routes the request to the appropriate facility, which checks its availability and makes the booking. Then it sends back confirmation, FABRIC platform updates its charging facility database and sends a confirmation message to EV backend. The sequence is easily extendable to include manual booking just by adding one more step: the initiation of the booking request by the OBU to the EV backend.

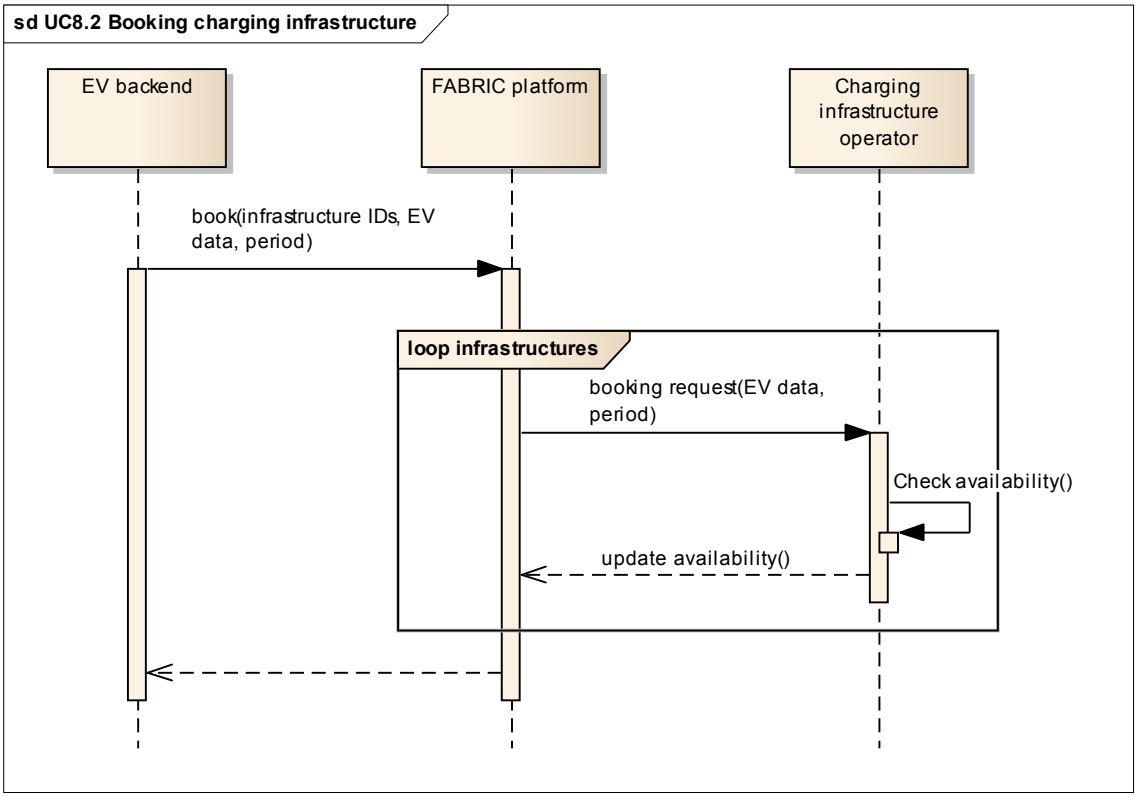


Figure 20: Charging infrastructure booking.

2.4 System components

2.4.1 FABRIC On-Board Unit (OBU)

The OBU is a computer that is installed in the FEV to support remote bi-directional communication with FABRIC and execute the FABRIC applications and in order to provide services to the end-user that enable dynamic, wireless FEV charging. The OBU needs to be integrated with existing systems in the vehicle, be connected to the CAN in order to receive information from vehicle sensors and ECUs, and also connect to the FEV charging equipment. The OBU subsystem needs to satisfy basic requirements from interface and hardware perspective, as listed below, in order to achieve the objectives of the FABRIC project.

Requirement	Technical means
Communication with FABRIC infrastructure (FABRIC EV backend)	DSRC/ITSG5 antenna 3G/LTE antenna
Communication with FABRIC charging infrastructure operator	
Communication with FABRIC RSU	
Communication with CAN-bus and Battery Management System (BMS)	CAN-bus interface BMS interface
Ability to host and execute FABRIC applications & services	PC/Tablet

Ability to store FEV and driver/owner information	Secure database
Ability to monitor and control charging process	Interface with WPT module
Interaction with driver through HMI	Tablet or OEM interface
Communication of OBU PC with OBU HMI in case they are located on separate machines	Ethernet or WiFi

The basic vehicle architecture that enables wireless charging is illustrated in Figure 21. Some HW components have to be integrated with the existing FEV equipment (high voltage battery, inverter and traction motor). One of the components to be added is the on-board vehicle ITS station (ITS-S) that contains an Application Unit, a Communication Unit and the HMI device.

An in vehicle gateway is also needed to collect the data (battery SOC, instantaneous power consumption, …) from the OEM CAN-bus network, processing it and feeding it to the on-board ITS-S. In the case of wireless charging (static and while driving) a wireless power transfer (WPT) device, containing a high frequency caption coil and a diode rectifier, is connected on the high-voltage (HV) DC bus with the existing HV components.

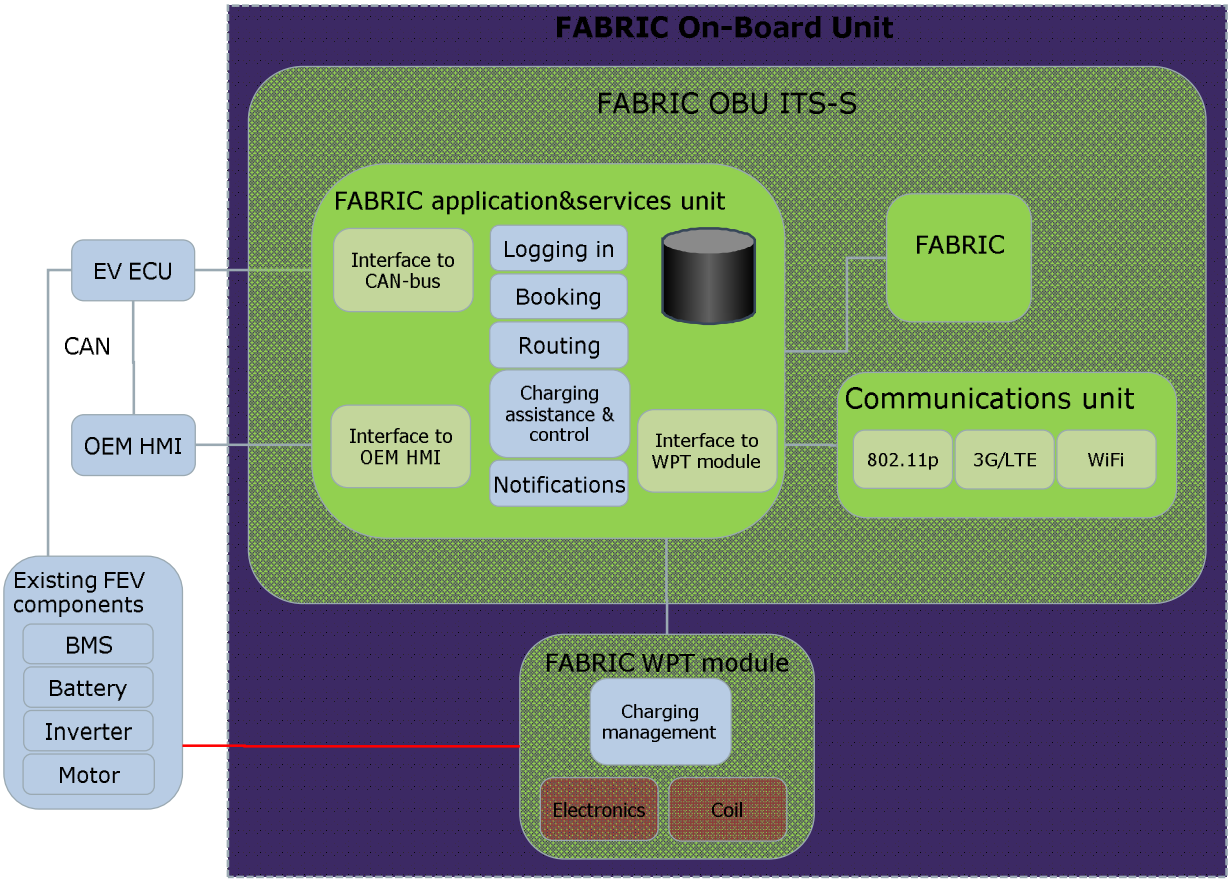


Figure 21: FABRIC OBU high level architecture.

The FEV integrates an ITS station (FEV ITS-S) that hosts and executes the applications and services for FEV users and the supporting communication capabilities. In addition it may include a FABRIC-specific HMI device in case the FEV OEM HMI is not capable of supporting the interaction requirements of FABRIC. The FEV ITS station is designed based on standardized ITS reference architecture in [7] in order to facilitate interoperability with future systems but also ICT designs in other electromobility projects such as eCo-FEV. In that way, already developed and tested components can be reused without additional spending of resources. As illustrated in Figure 21 FABRIC OBU includes three physical components: an Application and Services Unit (FASU), a Communications Unit (FCU) and a Human Machine Interface (FHMI) device (FABRIC OBU HMI can be considered part of the application and services unit). According to the information exchange needs and application requirements, these components are connected with each other, with other existing FEV systems and with external communication networks. For this reason, several antenna systems are installed in OBU.
A short description of FEV ITS-S and the main interfaces is provided in Table 4.

Table 4: FABRIC OBU subsystems description.

FABRIC OBU Subsystem	Short description
FASU (FABRIC Applications and Services Unit)	The FASU implements applications and facilities layer of the standardized ITS station. It is connected with in vehicle systems CAN via an in vehicle-gateway (interface), in order to receive in vehicle data, e.g. battery status information, vehicle sensor information, range estimation etc. Furthermore, FASU is connected with FCU, in order to send and receive messages from and to other FABRIC subsystems via the communication capacities provided by FCU. Finally, FASU should be connected with the OEM HMI device of the FEV, in order to present application processing results and notifications to the end-user. FASU should also receive from HMI end-user inputs and feedback. In case the OEM HMI cannot satisfy the interaction requirements of FABRIC applications and services, a FABRIC-specific HMI is foreseen as an add-on device.
FABRIC Communications Unit	FCU implements the networking & transport layer and access layer of the ITS station. It provides communication capacities to other FABRIC systems i.e. RSU, FABRIC EV backend, FABRIC charging infrastructure operator via wireless communications. It should be highlighted that, for communication between FEV and charging infrastructures, the required communication capacities will be supported by FEV on board charging device. Therefore, this communication is not included in the FCU. The FCU is connected with FASU (e.g. via Ethernet) in order to send and receive application and facilities layer messages to other FABRIC subsystems. The FCU includes at least ITS-G5/DSRC and 3G/LTE and WiFi communication capacities.

Based on FABRIC high level functional architecture and analysis of use case sequence diagrams as presented in section 2.3, it is possible to define the functional architecture of the FASU and FCU respectively, by specifying their main functional components. These functional

components are interacting with each other, either via a physical interface or via Application Programming Interface API in order to realize the FABRIC applications and services to FEV user. The functional architecture of the FEV ITS-S FASU is illustrated in Figure 22. This functional architecture is defined based on ITS station reference architecture as defined in [7].

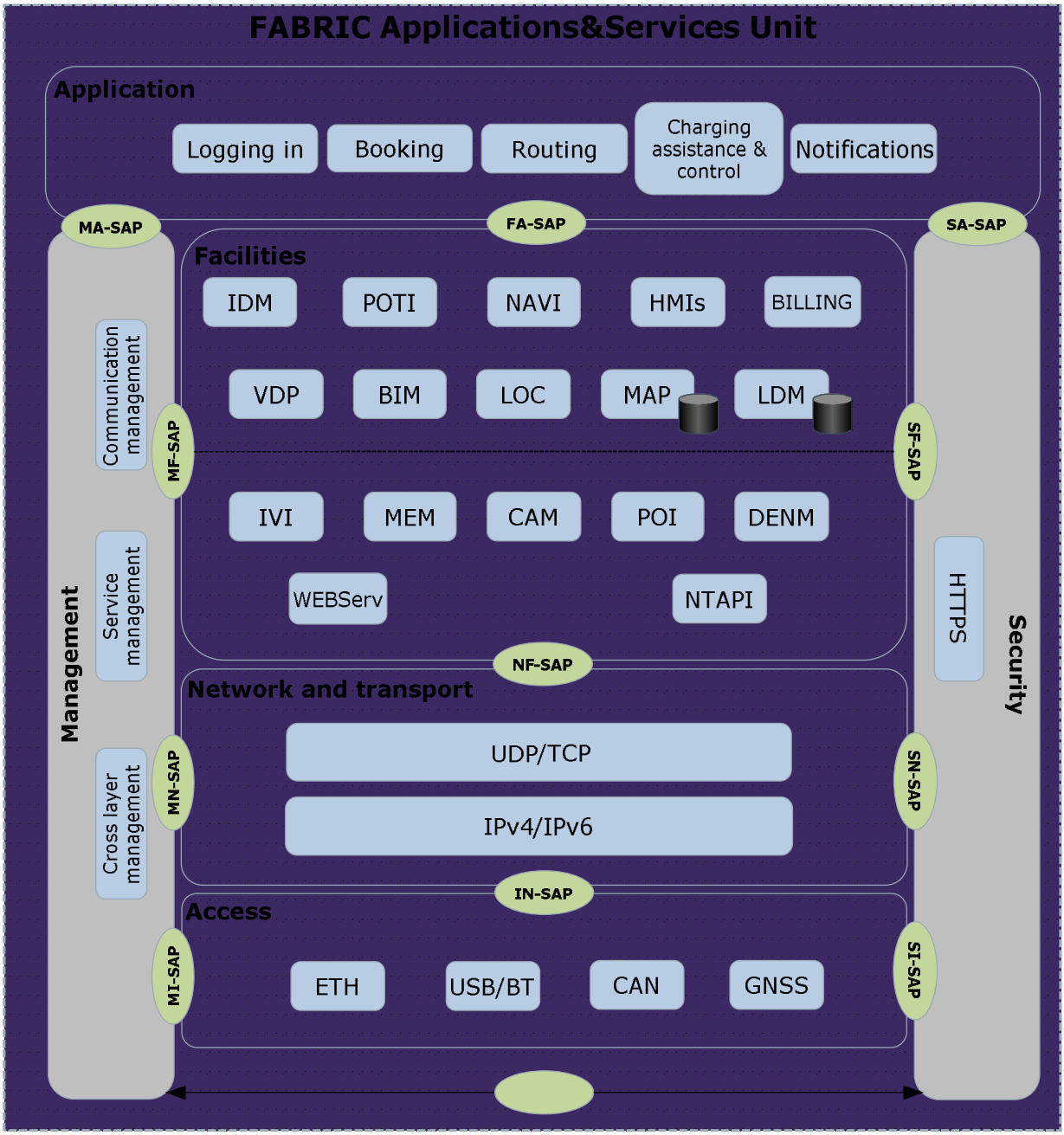


Figure 22: FABRIC OBU ITS-S Applications and Services Unit (FASU) functional architecture.

In the table below the components of the FASU are briefly described.

Table 5: OBU FASU functional components description.

Functional component name	Description
Application layer	FABRIC set of applications for the end-user, accessible by the FEV OBU, that enable the use cases.
Logging in	An application that facilitates the connection of a registered end-user to the system in order to access the FABRIC applications and ensure billing of the right person.
Routing	The application comprises two parts: 1. It provides an HMI interface to the end-user providing route planning and rerouting functionalities. After the route is set, the second part of the application is activated. 2. The application provides real time routing assistance (navigation and POI information. POIs include charging facilities).
Booking	The application facilitates the booking of charging infrastructures by the end-user. Depending on the type of charging different modes of infrastructure booking will be available. For example for static charging it is possible to make a booking for a specific duration at a specific time. However for dynamic and stationary charging the "booking" of the infrastructure will be in the form of a simple "request to charge" or "consent to charge" functionality (push of a button) when the FEV is in the vicinity of the charging infrastructure. This is because the duration of dynamic or stationary charging is very small compared to the potential ETA delay and in that way the nature of these types of charging should be considered opportunistic and not planned.
Charging assistance and control	This application facilitates the charging process by providing information to the end-user on how to approach the infrastructure, how to initiate charging and how to achieve maximum efficiency. It also gives charging abortion capability to the end-user at all times prior and during charging. This application will support all three wireless charging modes (static, stationary and dynamic) and provide different assisting information and options depending on the charging mode.
Notifications	This application uses the HMI to provide information to the end-user for various functionalities and travel phases. It is an information hub that receives input from several in-vehicle applications (e.g. routing) and from FABRIC backend (e.g. information regarding availability of charging infrastructure and billing).
Facilities layer	This layer contains components that support the FASU OBU applications
IDM	This component manages the identity information of FEV and the end-user. This information is required to match the FEV/user profile with registered or supported FABRIC services, with a billing contract, infrastructure booking and authentication/authorization functionalities.

	The identity may be temporarily updated to satisfy anonymization and privacy protection requirements.
POTI	This is the component that provides real time FEV location and time information. It is necessary for location based applications and services such routing and the actual charging process. A GNSS receiver is typically used for the acquisition of the vehicle location. This type of position detection has 6-10m margin or error. In FABRIC, it will be necessary to have much more accurate and fast position estimation for the charging assistance application. For this reason GNSS data may be augmented with data from road side and vehicle sensors. A possible solution is for the vehicle to receive the accurate and fixed position coordinates of transmitters installed at charging pads or any other road side unit, as it passes over the pad or next to the RSU.
NAVI	This is a component that supports the Routing application. It calculates the route between two points based on the end-user's preferences and/or FABRIC restrictions and information. It also facilitates turn-by-turn navigation functionality and location based information.
HMIs	HMIs is a gateway facilitating bi-directional communication between the application layer and the HMI.
BILLING	This component is in charge of triggering the billing and payment data exchange with the EV backend after the charging has ended. The billing transactions take place between the FABRIC backend and an external clearing house.
VDP (Vehicle data provider)	This component provides a gateway to the vehicle CAN-bus in order to receive in vehicle data which is required for the application and facilities layer processing. Data such as vehicle sensor data and charging system data may be provided via CAN-bus to this component and then routed to the appropriate FASU applications.
BIM	This component manages the FEV battery status information received from FEV battery and charging device. It may provide current or historical battery status information to FABRIC backend or to charging assistance application. Alternatively, this component may include simple data processing functionalities to aggregate the battery information.
LOC	This component provides location referencing information additional to the geographical coordinates, enabling the matching of FEV position to road topology. Multiple location referencing methods may be used. A commonly used location referencing method between FEV, RSU and backend system will enable the receiver of the information correctly estimate the position of the sender within the road network. This component can be considered a sub-component of the POTI component in case charging pad and/or RSU position data are used to augment the accuracy of GNSS.
MAP	Map database being used by FEV applications. Openstreetmap [8]

	is used for FABRIC project for testing purposes.
LDM (Local Dynamic Map)	Embedded database that includes dynamic (or static) information at the vicinity of the FEV e.g. received messages from RSUs in neighborhood. Furthermore, it may also store information of FEV such as its position, speed and vehicle sensor information etc. LDM is updated periodically during driving. It provides an interface to applications, allowing the retrieval of data required for application processing.
CAM	Standardized Cooperative Awareness facility that generates transmits and receives Cooperative Awareness Message (CAM). The received CAMs update the LDM. CAM is standardized by ETSI [9].
DENM	Standardized Decentralized Environmental Notification basic service that generates, transmits and receives Decentralized Environmental Notification Message (DENM). The received DENMs update the LDM. DENM is standardized by ETSI [10].
POI	Standardized Point of Interest basic service that receives Point of Interest Message (PoI). The received POIs may update the LDM or directly go to applications that request the information. POI for FEV charging station is standardized by ETSI [11]. Other types of POIs may be defined in FABRIC to include and describe various types of charging facilities.
MEM	Component that routes other types of messages as required by the information flow shown in chapter 2 of this document.
WEBServ	Component that implements web service functionalities (e.g. SOAP, REST) and related higher layer protocol (e.g. HTTP).
NTAPI	Component that provides an API for data exchange between FASU and Communication Unit.
Networking and Transport layer	This layer hosts the communication means to transfer information between the FASU and the Communications Unit (CU) and the HMI (in-vehicle)
TCP/UDP	TCP/UDP transport protocol used for communication between FASU and CU/HMI.
IPv4/IPv6	Network layer protocol used for communication between FASU and CU/HMI.
Access layer	Access technologies for communications between FASU and CU/HMI
ETH	Ethernet connection.
USB/BT	USB (wired) or Bluetooth (wireless) connections.
CAN	CAN-bus connection with in-vehicle systems and sensors.
GNSS	Interface to GNSS receiver.
Management layer	Management functions for FASU operation and cross layer
Service management	Functionalities that manage the FASU operations, e.g. configuration, FASU status management, software management etc. It processes received Service Announcement Messages (SAM) from road side or from

	backend, and interacts with applications to access to services using communication means as included in SAM.
Communication management	Functionalities that interact with NTAPI to determine the communication stack being used for message transmission from OBU to external networks.
Cross layer management	Functionalities that manage the communication between FASU and other FEV systems e.g. CU, HMI, CAN-bus etc.
Security layer	Security functions.
HTTPS	Secure communication for HTTP protocol-based communications.

The functional architecture of the FEV ITS-S Communications Unit (CU) is illustrated in Figure 23.
This functional architecture is defined based on ITS station reference architecture as defined in [7]. It includes functionalities of access and networking & transport layer.

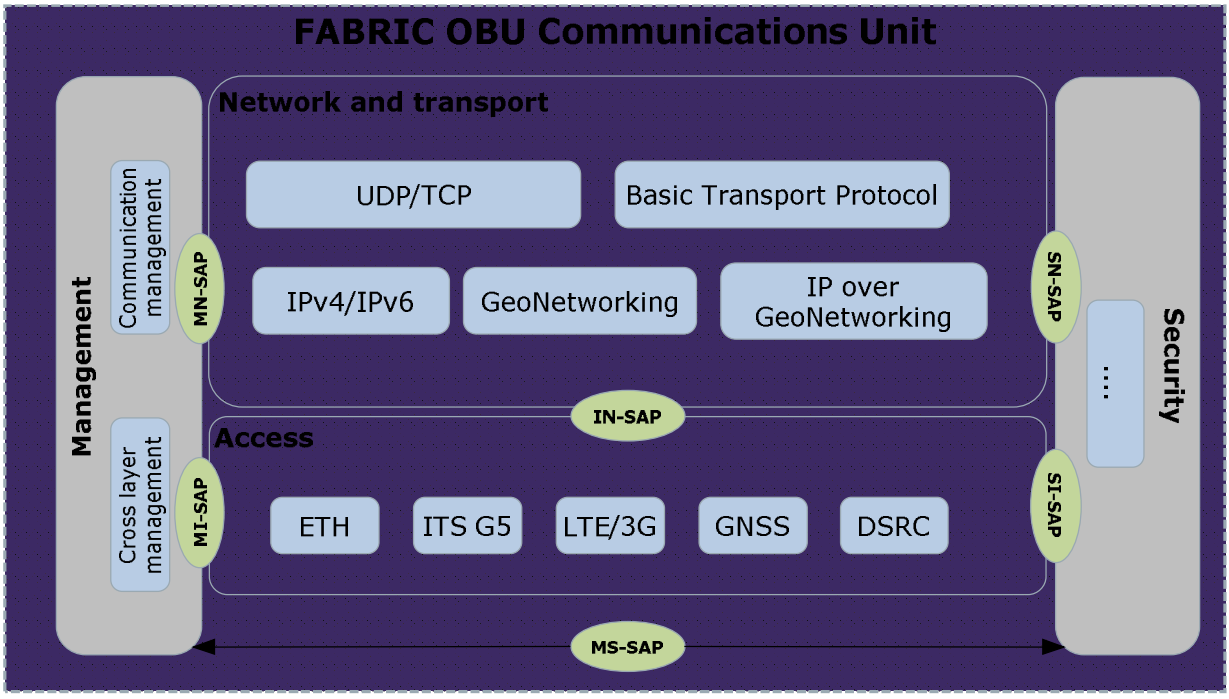


Figure 23: FABRIC OBU Communications Unit functional architecture.

Table 6: FABRIC OBU Communications Unit functional components description.

CU functional component name	Description
Networking and Transport layer	Communication facilities for the CU
Basic Transport Protocol	Basic Transport Protocol is used for GeoNetworking protocol stack. It is standardized by ETSI [12].
GeoNetworking	Standardized geolocation-based networking protocol and networking functionalities. It is standardized by ETSI [9].

IP over GeoNetworking	Functionalities that enable the transmission of IPv6 packets over GeoNetworking protocol stack.
TCP/UDP	TCP/UDP transport protocol used for communication between FASU and CU/HMI.
IPv4/IPv6	Network layer protocol used for communication between FASU and CU/HMI.
Access layer	Access technologies for communications between FASU and CU/HMI
ETH	Ethernet connection between FASU and CU.
ITS G5	IEEE 802.11p based ITS G5 technologies at 5.9 GHz as standardized by ETSI [13]. It provides direct ad hoc communications between FEVs and between FEV and RSUs.
LAN/3G	Cellular communication technologies for communication between FEV and FABRIC off-board systems (platform and EV backend) or other infrastructure systems.
GNSS	Interface to GNSS receiver.
DSRC	IEEE 802.11p based DSRC technologies at 5.8 GHz for communication with electronic toll-like systems that may be used for road operator access control systems for dynamic charging lanes or communication with RSUs.
Management layer	Management functions for FASU operation and cross layer
Communication management	Functionalities that interact with FASU to determine the communication stack being used for message transmission from OBU to external networks.
Cross layer management	Functionalities that manage the communication between CU and other FEV systems e.g. FASU.

2.4.2 FABRIC EV backend subsystem

FABRIC EV backend is envisioned as the gateway between FABRIC and the FEV. It will handle all communications with the FEV and the end-users and in that way reduce the load for the core FABRIC electric mobility platform. By splitting the EV backend from the central FABRIC platform it is possible for OEMs to manufacture their own EV backend and integrate them with FABRIC using a FABRIC-provided API.

The FABRIC EV backend subsystem needs to satisfy the following basic requirements from interface and hardware perspective in order to achieve the objectives of the FABRIC project:

- Communication with the FEV.
- Communication with FABRIC electric mobility platform.
- Communication with CIO.
- Communication with RSU.
- Communication with the clearing house.
- Communication with end-users via web interface.
- Servers to install the platform, its applications, the communications SW infrastructure and secure databases that will store user, FEV and system information.

A high level functional architecture of the FABRIC EV backend subsystem is illustrated in Figure 24. FABRIC EV backend connects with FEV and other infrastructure systems via Internet domain. A special case may be the connection with the electric mobility platform via intranet or even the hosting of the two subsystems in the same server. On the other hand, FABRIC EV backend functionalities may be implemented in more than one physical entity i.e. backend servers. The detailed implementation framework will be decided in WP25 of the FABRIC project.

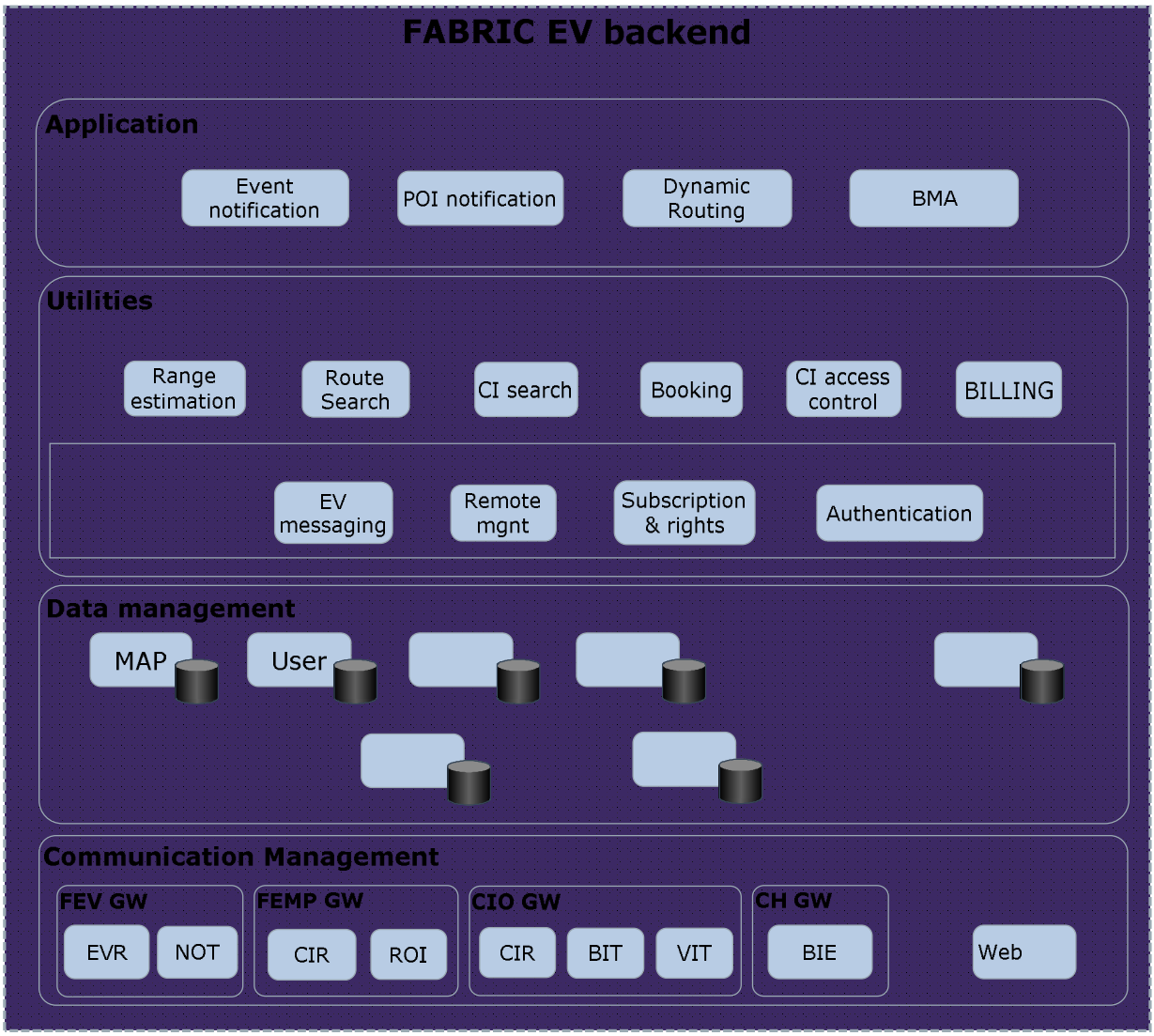


Figure 24: FABRIC EV backend functional architecture.

Table 7: FABRIC EV backend functional components description.

Functional component name	Description
Application layer	This layer includes the high level applications for FABRIC EV backend.
Event notification	Application to monitor events, deriving from the FABRIC electric

	mobility platform or other sources, such as traffic accidents/congestions, changes in the charging infrastructure availability status etc. and notify the end-user about it.
POI notification	Application to notify about nearby charging facilities, filtered based on the EV charging characteristics and the users' preferences. Other POIs such as parking lots could be included.
Dynamic routing	Application to provide navigation assistance to the EV user towards a destination or a charging facility based on the use cases.
BMA	Application to provide Battery Management Assistance to the EV.
Utilities layer	This layer includes utilities and components that support the operation of the high level applications.
EV messaging	Component to dispatch EV messages to relevant functions/applications.
Remote management	Component to construct and generate notification messages to EVs or to RSUs.
Subscription & rights	Component to manage user subscription process and manage the user's access rights.
Authentication	Component to authenticate user and vehicles.
Range estimation	Component to calculate the remaining EV range based on real time traffic information, battery State of Charge information and potentially other information. In case no special algorithm for this task is developed, this component could retrieve the range estimation information from the vehicle ECU.
Route search	Component to calculate route using digital map database based on predefined criteria. It may provide route guidance information according to the calculated route.
CI Search	Charging infrastructure search component selects relevant and available charging facilities from the CI database according to criteria such as EV charging characteristics, user preferences over the mode and duration of charging, charging facility operating characteristics, EV range etc.
Booking	Component to manage the charging facilities bookings and cancellations depending on the type of charging facility.
CI access control	Component to authorize the use of a charging facility for a specific EV at a specific time based on the EV ID, the bookings and the status of the charging facility.
Billing	Component to initiate and manage the billing process and handle the communication with the clearing house.
Data management layer	This layer includes the components and databases to store and manage the various data that are necessary for the applications and their components.
User	Database and management functions to store, access and process end-user data such as user id, user name, password, user profile, billing information, address, contract information etc. and also logs information about the user login sessions and activity for security purposes.
MAP	Maps database and services.

CI info	Database and management functions to store and access charging facilities' data such as id, name, address, position, nominal operating capacity etc. Dynamic data such as availability status and operating limits will be updated in near real-time either by pull or push methods.
EV	Database and management functions to store and access vehicle information such as id, type, supported charging modes, charging and battery characteristics etc.
VRM	Database and management functions to manage Vehicle Relationship Management data.
Probe	Database and management functions to manage dynamic EV data such as time, position, velocity etc.
BI	Database and management functions to manage EV battery status information.
Communication management layer	This layer includes the components that enable connection with other FABRIC subsystems and external actors such as the OBU, the clearing house etc.
FEV GW	Gateway to FEV.
EVR	EV information Retrieval: Interface to receive EV information data such as probe and battery data.
NOT	Notifications: Interface that enables messaging functionality from the backend to the EV.
FEMP GW	Gateway to FABRIC Electric Mobility Platform.
CIR	Charging Infrastructure info Retrieval: Interface to collect charging infrastructure status information from the FABRIC electric mobility platform.
ROI	Road Operator Info retrieval: Interface to collect road operator derived information from the FABRIC electric mobility platform.
CIO GW	Gateway to Charging Infrastructure Operator.
CIR	Charging Information Retrieval: Interface for information exchange with the CIO to receive charging related data (energy consumed, efficiency etc.) and send billing related information.
BIT	Billing Information Transmission: Interface with the CIO to transmit billing related information relevant to the CIO reimbursement.
VIT	Vehicle information Transmission: Interface with the CIO to transmit booking information and EV characteristics prior to charging.
CH GW	Gateway to Clearing House.
BIE	Billing Information Exchange: Interface with the clearing house to exchange information regarding payment for the charging.
Web serv	Web interface that enables the end-users to access their account in FABRIC and manage their personal information and the information for their EV. Pre and post trip FABRIC services could be provided to the end-users via this interface.

2.4.3 FABRIC Charging Infrastructure subsystem

The basic requirements for the wireless charging infrastructure of FABRIC are listed below.

- Communication with FABRIC electric mobility platform
- Communication with EV charging device (secondary coil)
- Communication with the on-site power delivery
- PC to install charging equipment including the energy provision system and a control unit
- A charging operator that monitors and controls the operation of the charging facilities.

The architecture for the wireless charging facility is shown in Figure 25. The charging facility may consist of one charging pad per station in case of static charging mode or many charging pads installed in series in case of dynamic or stationary charging modes. From the architectural point of view, the operation in all modes is basically the same so it is not necessary to draft different architectures for each mode. What changes is the duration of charging, the control algorithms and the interfaces with the end-user, so the static and stationary modes can be considered as special cases of the dynamic charging.
The charging infrastructure comprises two main parts:

- The charging infrastructure (CI) that is installed on the road (probably under the pavement) which consists of the primary coils, the power control electronics, communications equipment and sensors. In order to be in-line with other electromobility projects and related standards, this part will be called EVSE which stands for Electric Vehicle Supply Equipment.
- The charging infrastructure operator (CIO), which is a backend system for the monitoring and control of the charging infrastructure, the collection and processing of data and communication with FABRIC electric mobility platform.

The following table provides a more detailed description of the charging infrastructure main parts.

Table 8: FABRIC Charging Infrastructure Subsystems description.

FABRIC Charging Infrastructure Subsystem	Short description
EVSE	The EVSE is composed of the HW components for the electric power transfer, and works in resonance with the compatible secondary coil device that is installed under the EV. One of the components of the EVSE is the charging station control unit which manages the V2G data exchange between the OBU and the charging infrastructure operator. EVSE is connected with charging infrastructure operator within a specific charging infrastructure operator network using IP communication.
Charging infrastructure operator (CIO)	Charging infrastructure operator is a backend system that manages the operation of the EVSE. It manages Authentication and Authorization tasks before the EV charging, monitors the charging process and

	collects energy consumption data for billing purposes. CIO is the communications hub with the FABRIC platform. It hosts a load balancing module that controls the energy supply to the EVSE based on high level grid restrictions. CIO also provides EVSE status and operating characteristics information to the FABRIC platform.
RSU	The RSU can be part of the EVSE (housed in the same box) or installed separately close to the EVSE. Two functionalities are foreseen for the RSU: the first is data exchange between the OBU and the EVSE; the second is EV presence detection above the RSU in order to trigger the wireless power transfer. The appropriate EV detection sensors will be defined in SP3. Due to the expected high vehicle velocity, EV detection and communication of the information to the EVSE needs to be in the order of microseconds.

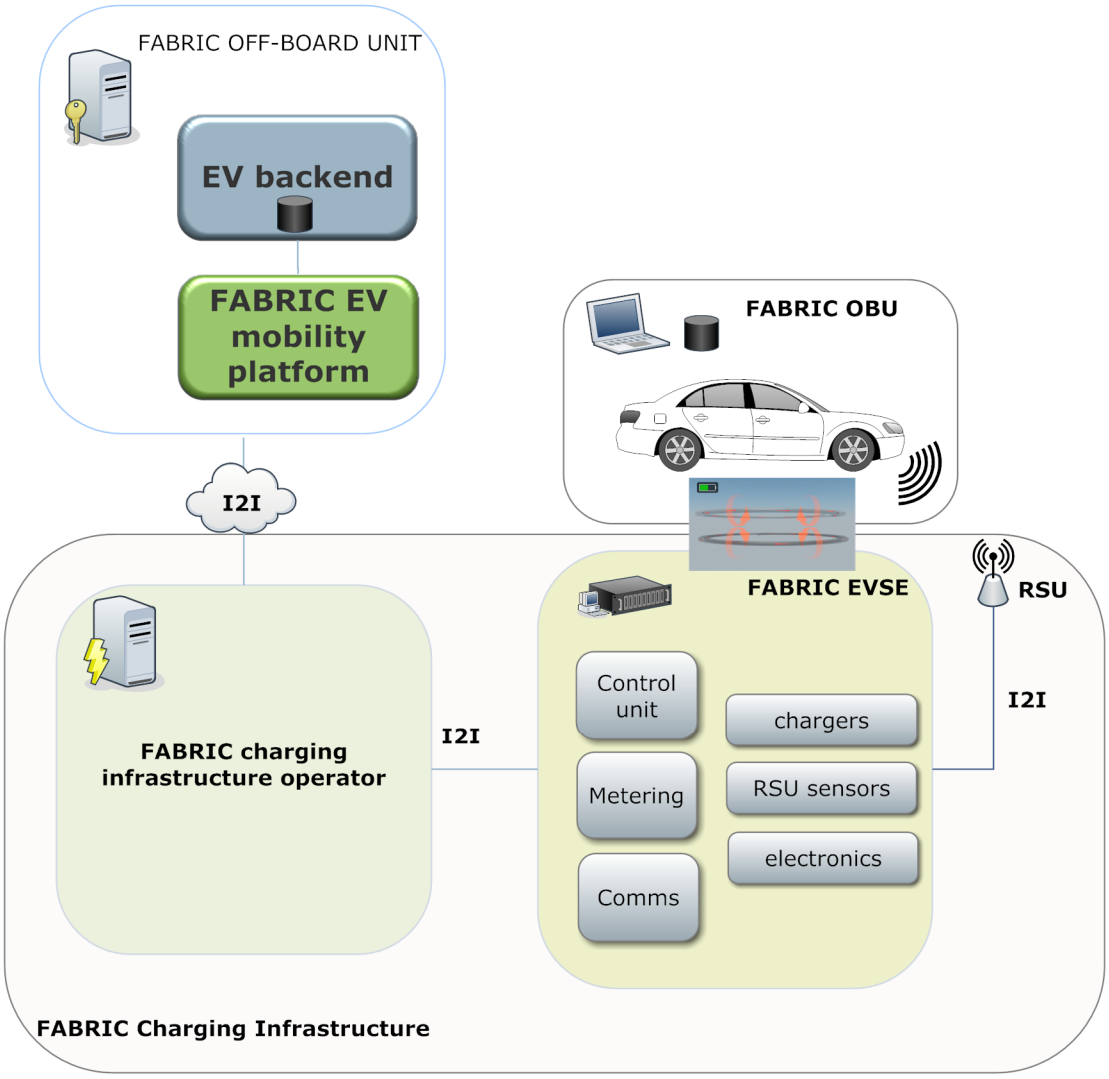


Figure 25: FABRIC Charging Infrastructure high level architecture.

Note:
The separation of the RSU from the charging pads can be expected for two reasons in a feasible FABRIC system:

1. An already existing third party RSU could be integrated in FABRIC to provide traffic or other data so this is a separate unit already.
2. Due to technical reasons the RSU (which may contain vehicle detection sensors) could be required to be installed a bit further than the CI: If the vehicle travels at 130km/h the contact time with the charging pad is less than 30ms. If the RSU is installed some meters before the CI it will detect the oncoming EV some ms before it reaches the CI and it will give time to the system to perform functions necessary for charging (e.g. calculate and transmit a charging profile to the CI, switch electronics etc) on time, so the EV/CI contact time will be used for the actual power transfer (optimizing the EV charging). These are hypothetical development scenarios at the moment of writing; however separating RSU from the CI increases the system designing flexibility.

2.4.3.1 FABRIC EVSE

FABRIC EVSE or charging infrastructure is the point where power transfer takes place between the EV and the electric grid. The EVSE comprises hardware parts such as the primary coil(s) (chargers) and the supporting switching and control electronics, metering hardware that measures the power consumed by the chargers, communications hardware that enables information exchange between the EVSE and the CIO, between the EVSE and the EV and between the EVSE and sensors that are installed on the road such as vehicle detection sensors or RSUs. The EVSE contains a software module, called Control Unit, which coordinates communications, monitors energy transfer and controls the operation of the chargers. The functional architecture of the EVSE Control Unit is illustrated in the figure below and a description of its functional components is presented in Table 9.

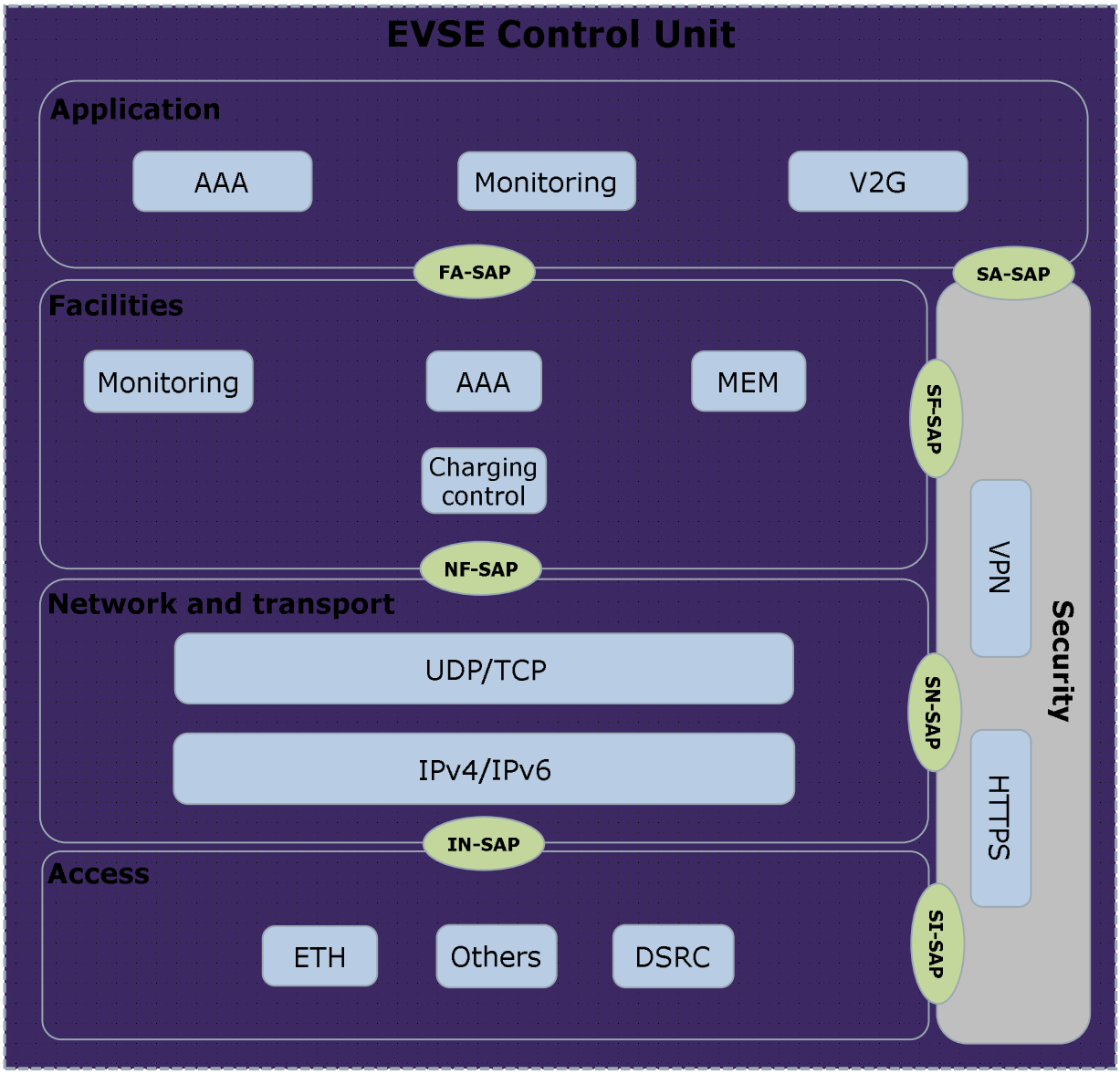


Figure 26: EVSE Control Unit functional architecture.

Table 9: EVSE Control Unit functional components.

Functional component name	Description
Application layer	EVSE applications
AAA	Authentication of the vehicle ID, Authorization for the specific vehicle to charge and Accounting for the charging session. This application is performed in collaboration with the charging infrastructure operator.
Monitoring	This application communicates with the charging infrastructure operator to send information about the operational and availability status of the EVSE.
V2G	This application manages the energy supply to EV based on the

	charging profile that the CIO transmitted to the EVSE for a specific vehicle.
Facilities layer	Functional components necessary for the EVSE applications
Monitoring	Provides a bidirectional communication gateway between the CIO and the charging infrastructure to allow collection of operating and availability data and the remote execution of commands by the CIO.
MEM	Messaging facility needed for information exchange between the EVSE and CIO as described in the sequence diagrams.
AAA	Component which communicates with CIO to enable AAA services.
Charging control	Facility that provides control and management of the EVSE during charging.
Networking & Transport layer	This layer includes the components that support the communication between CIO and EVSE.
TCP/UDP	TCP/UDP transport protocol used for communication between CIO and EVSE.
IPv4/IPv6	Network layer protocol used for communication between CIO and EVSE.
Access layer	Access technologies for communications between CI and CIO.
ETH	Ethernet connection between EVSE and CIO.
Other	Connection to the power electronics of the EVSE.
ITSG5/DSRC	Connection to the OBU of the EV.
Security layer	Security functions.
VPN	VPN connection to CIO.
HTTPS	Secure HTTP connection between EVSE and OBU.

2.4.3.2 FABRIC Charging Infrastructure operator

The Charging Infrastructure Operator (CIO) subsystem is the backend of the charging infrastructure. The charging infrastructure in case of static charging is one charging pad but in case of stationary and dynamic charging the infrastructure consists of many charging pads. In that way, the charging infrastructure operator can be considered an aggregator of many charging stations. The CIO communicates with a set of charging station control units, for gathering monitoring and status information, and triggering specific actions, (such as booking). It implements the Server-side of the AAA (Authentication, Authorization, Accounting) for the charging process. On the other hand it communicates with the FABRIC electric mobility platform for reporting the status of the charging facilities (monitoring) and providing accounting information.
The functional architecture of the CIO unit is illustrated in Figure 27. Short description of functional components is presented in Table 10.

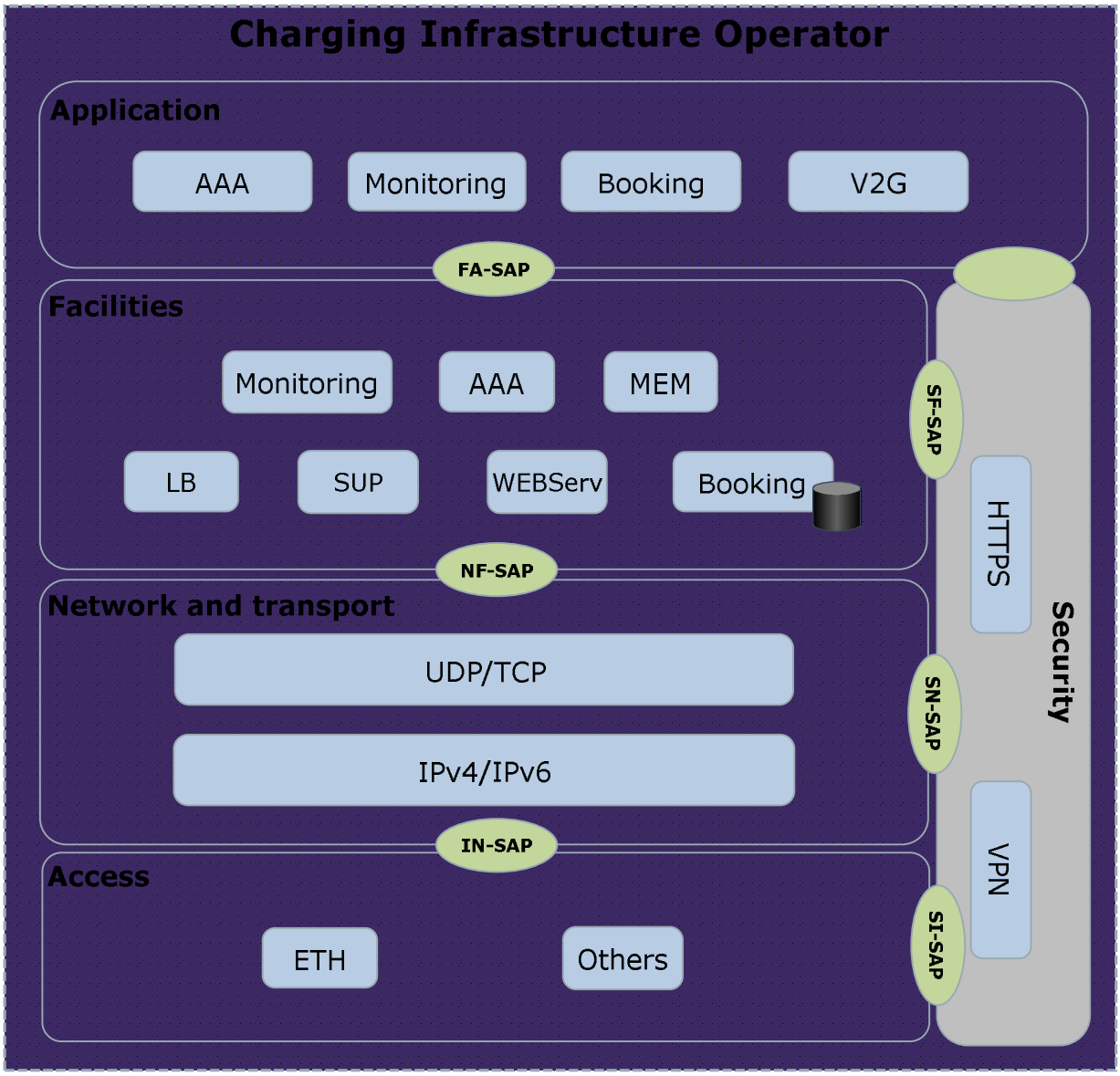


Figure 27: FABRIC Charging Infrastructure operator functional architecture.

Table 10: FABRIC Charging Infrastructure operator functional components description.

Functional component name	Description
Application layer	Charging Infrastructure applications
AAA	Authentication of the vehicle ID, Authorization for the specific vehicle to charge and Accounting for the charging session. This application is performed in collaboration with the charging infrastructure control unit.
Monitoring	This application communicates with the charging infrastructure Control Unit to gather information about the operational

	(metering) and availability status of the latter one and reports them to FEMP and EVB.
Booking	This application reserves the charging facility for a specific EV for a specific period and time in case of static charging. In case of stationary and dynamic charging this application with only provide authorization to access the facility in near-real time upon the EV's request to charge as it approaches the facility. The authorization will be done taking into account various parameters, such as facility availability, facility operating characteristics and compatibility with the EV charging equipment, grid restrictions etc.
V2G	This application manages the energy supply to the charging infrastructure based on grid restrictions and demand response algorithms. It contains a load balancing module that extends the load balancing done in other projects for static charging, in order to cover stationary and dynamic charging of many vehicles in parallel.
Facilities layer	Functional components necessary for the CIO applications
Monitoring	Provides a bidirectional communication gateway between the CIO and the charging infrastructure to allow collection of operating and availability data and the remote execution of commands by the CIO.
MEM	Messaging facility needed for information exchange between the CIO and the other FABRIC units as described in the sequence diagrams.
AAA	Component which accesses the booking database and the monitoring data to enable AAA services.
Booking	A module which communicates with EVB to receive booking information. The information is stored in a database for the charging facility reservation. A component that handles the incoming booking requests based on CI availability is also included. In case the EV misuses the booking the information is also communicated to EVB for further actions.
SUP	A module that receives information from FEMP regarding the supply limits based on DSO restrictions. It could either be CI specific limitation or aggregated supply limit. In the latter case the module will distribute the aggregated supply to the CIs it supervises/controls.
LB	A module that balances the demand from EV charging to the supply limits of the CI and creates custom charging profiles per EV based on grid restrictions, EV characteristics and charging preferences.
WEBServ	Facility that implements web service interface for communication with FABRIC EMP.
Networking & Transport layer	This layer includes the components that support the communication between RSU AU and CU.
TCP/UDP	TCP/UDP transport protocol used for communication between CIO and CI Control Unit and FABRIC EMP.
IPv4/IPv6	Network layer protocol used for communication between CIO and

	CI Control Unit and FABRIC EMP.
Access layer	Access technologies for communications between CI and CIO.
ETH	Ethernet connection between CI and CIO.
Others	Wired or wireless connections with FEMP and EVB
Security layer	Security functions.
HTTPS	Secure communication for HTTP connections.
VPN	VPN to CI Control Unit.

2.4.3.3 FABRIC Road Side Unit (RSU)

The RSU subsystem is placed at road side, it may provide services to EVs following the ITS paradigm and communication capacities to connect EVs with the road side CI. In the scope of FABRIC feasibility and demonstration, two scenarios of RSU deployment may be envisioned:

1. The RSU is controlled by road IT infrastructure operators (e.g. traffic management center) and provide traffic information to road users. It receives dynamic traffic information either directly from the road side sensors, or from services providers (e.g. traffic management center or private service provider such as PoI service provider) then broadcasts the information to road users in its vicinity. This creates a secondary communication channel between the FABRIC off-board unit and the EVs, in parallel to the primary communication channel that is via the EV backend. This secondary communication channel can also transmit information to vehicles that are not logged into FABRIC depending on their vicinity to the RSU.
2. The RSU is mounted to charging infrastructure and provide communication capacities for information exchange between FEV and charging infrastructure before and during the charging. In this case the RSU may be equipped with vehicle detection sensors in order to trigger the charging process.

The RSU subsystem needs to satisfy basic requirements from interface and hardware perspective, as listed below, in order to achieve the objectives of the FABRIC project.

- Communication with Road operators and/or FABRIC electric mobility platform (Cellular).
- Communication with OBU. Since FABRIC will support primarily dynamic charging, very short communication delay is a primary requirement and because of that ITSG5 or DSRC/WAVE technologies will be used.
- Optional communication with road side equipment (existing interfaces of road side equipment).
- Communication with charging infrastructure (preferably Ethernet for low latency and security reasons).
- Hardware for hosting the FABRIC applications and supporting communication interfaces.

The RSU is designed based on standardized ITS reference architecture as illustrated in [7]. This RSU includes two physical components: an Application Unit (AU) and a Communication Unit (CU). AU and CU provide similar functionalities as in OBU.
According to the information exchange needs and application requirements, these components are connected with each other, with road side infrastructures (e.g. road sensors, charging

infrastructures) and with external communication networks. For this reason, several antenna systems are installed in RSU.
The functional architecture for the AU of the RSU is shown below.

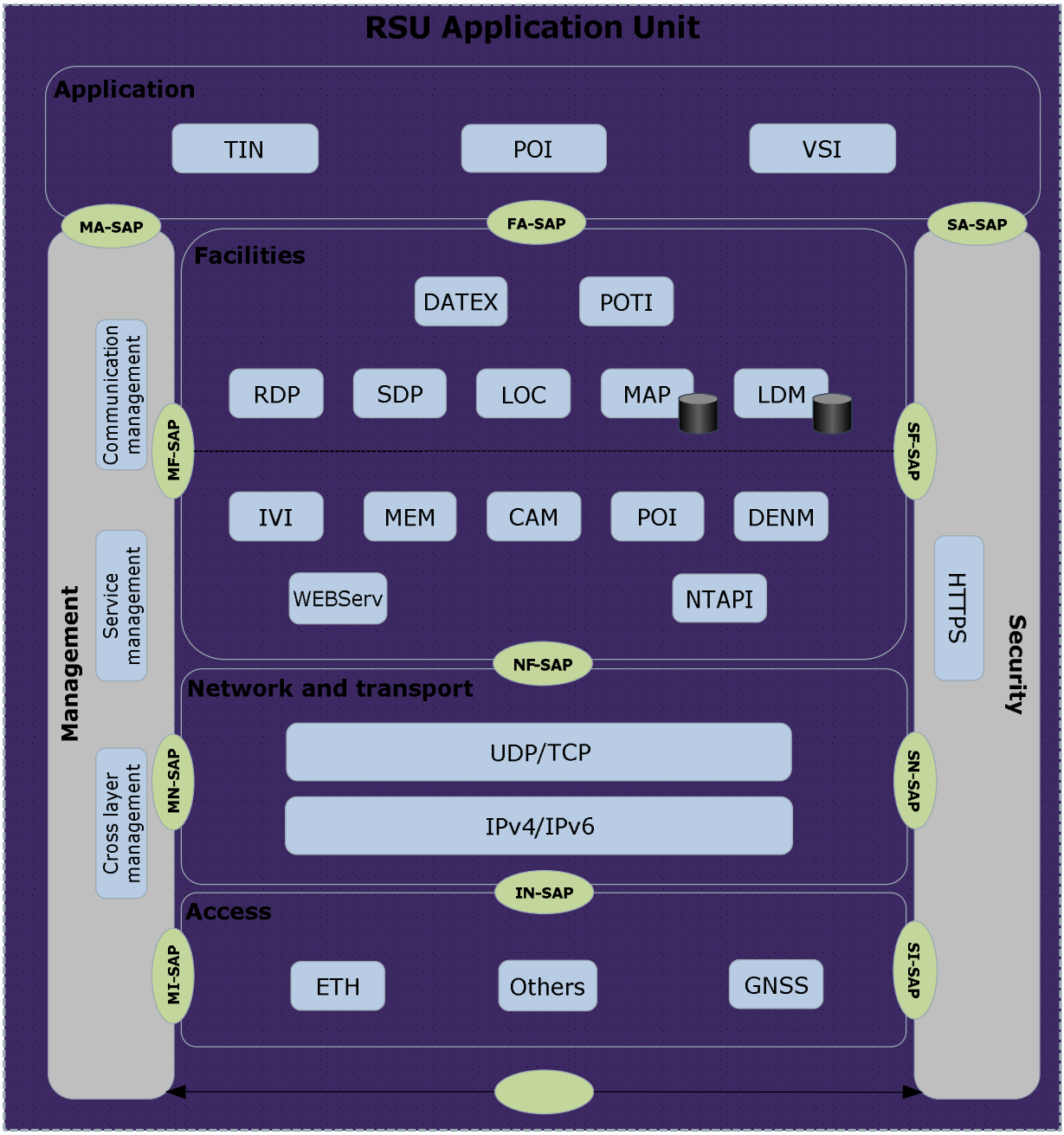


Figure 28: FABRIC RSU Application Unit functional architecture.

A short description of functional components are provided in the following Table

Table 11: FABRIC RSU Application Unit functional components.

Functional component name	Description
Application layer	This layer includes the high level applications for FABRIC RSU.
TIN	Traffic Information Notification provides real time traffic information from RSU to FEVs. The real time traffic information is received from road traffic operator, from FABRIC electric mobility platform or from road side sensors or equipment that are connected directly to RSU.
POI	RSU broadcasts PoI notification to road users such as charging facilities information and status.
VSI	RSU broadcasts dynamic or static road side signage information for in vehicle presentation. This information could include custom signs that will guide the driver through the charging procedure.
Facilities layer	This layer includes the components that support the RSU applications.
DATEX	This facility provides gateway functionalities to support DATEX II standard-based traffic information reception from road and traffic operators.
POTI	This facility provides real time geographical position and time information of the RSU, in order to enable location based applications and services. This component can be used to increase the accuracy of the OBU GNSS regarding the position of the vehicles.
SDP	Sensor Data Provider component provides an interface with road side sensors such as an EV detection sensor, in order to receive information from those sensors.
RDP	Road equipment Data Provider provides an interface with road side equipment e.g. traffic lights, which could be used to control access to the charging lane in case of dynamic charging or control traffic to allow for longer charging duration in case of stationary charging at intersections.
LOC	LOC component provides location referencing information additional to the geographical coordinates, enabling the matching of position to road topology. Multiple location referencing methods may be used. A commonly used location referencing method between FEV, RSU and backend system will enable the receiver of the information correctly estimate the position of the sender within the road network. In FABRIC, the location referencing information being used may be the fixed position of the charging pads.
MAP	Map database being used by FEV applications.
LDM	Embedded data base that includes dynamic (or static) information at the vicinity of RSU e.g. received messages from FEVs or other RSUs in neighbourhood. Furthermore, it may also store information of the RSU such as its position, sensor information etc. LDM is updated periodically. It provides an interface to applications, allowing the retrieval of data required for application

	processing.
CAM	Standardized Cooperative Awareness facility that generates transmits and receives Cooperative Awareness Message (CAM). The received CAMs are sent to LDM for update. CAM is standardized by ETSI [9].
DENM	Standardized Decentralized Environmental Notification basic service that generates transmits and receives Decentralized Environmental Notification Message (DENM). The received DENMs are sent to LDM for update. DENM is standardized by ETSI [10].
POI	Standardized Point of Interest basic service that generates and transmits Point of Interest Message (POI). POI for FEV charging station is standardized by ETSI [11]. The standard may be updated in FABRIC to include the characteristics of dynamic and stationary charging modes. Other types of POIs may be defined in FABRIC.
IVI	Facility that generates the In Vehicle Information message to provide road side signage information.
MEM	Facility that transmits and receives other types of messages as required by the information exchange presented in the information flow sequence diagrams.
WEBServ	Facility that implements web service functionalities (e.g. SOAP, REST) and related higher layer protocol (e.g. HTTP).
NTAPI	API for data exchange between AU and CU.
Networking & Transport layer	This layer includes the components that support the communication between RSU AU and CU.
TCP/UDP	TCP/UDP transport protocol used for communication between AU and CU.
IPv4/IPv6	Network layer protocol used for communication between AU and CU.
Access layer	Access technologies for communications between AU and CU.
ETH	Ethernet connection between AU and CU.
GNSS	Interface to GNSS receiver.
Management layer	Management functions for AU and cross layer operations.
Service management	Functionalities that manage the AU operations, e.g. configuration, AU status management, software management etc. It may receive service announcement messages (SAM) from backend, in order to discover the provided services types as well as the method and communication path to access to service. It may also generate SAM to inform FEV about the provided services by RSU and the communication means that enables the service access.
Communication management	Functionalities that interact with facilities and applications to decide the communication stack being used for message transmission from RSU to external networks.
Cross layer management	Functionalities that manage the communication between AU and other systems.
Security layer	Security functions.
HTTPS	Secure communication for HTTP connections.

The functional architecture of the RSU Communications Unit is the same as the one defined for the OBU Communications Unit.

2.4.4 FABRIC Electric Mobility Platform (FEMP)

FABRIC Electric Mobility Platform is the core module of FABRIC. It is the central hub that offers access to the system for all external actors namely the Road Operator, the Energy Retailer and the Distribution System Operator. FEMP hosts a repository that contains the current state of all charging infrastructures and it is a central access point for all subsystems that need to have operational status information, avoiding in that way many-to-many connections that introduce increased security risks and complexity.
FEMP's main functionalities are the following:

- Provides access point to DSO in order to manage energy supply to FABRIC-supervised CIs. This is beneficial for grid stability during emergencies since it makes direct load shaping possible.
- Provides access point to RO in order to manage CI availability in case or scheduled or unforeseen events such as accidents. A feasible scenario is an automated procedure originated by the RO traffic control centre using DATEXII protocol that sets CIs offline in case of accidents.
- Provides access point to ER(s). This is how FABRIC acquires the price information for the energy consumed during charging. The simplest case involves one ER and a set price. In the most complex scenario many retailers could bid in an auction like system for the forecasted demand. Tariff can be dynamically changed to indirectly shift charging towards low demand (or high supply) periods.
- Provides access point to FABRIC human operators. They can perform maintenance operations, see usage statistics, send messages to operators and the EVs etc. The functionalities offered depend on the custom implementations.

FEMP can reside in the same machine as the EVB. This will allow for fast, secure and reliable communication and local sharing of databases. However, the reason these two modules are not fused is to offer flexibility in future feasible implementations: Several OEMs may develop their own EVBs to communicate with the OEM OBUs. In that way, the EVB could also be located in a separate data centre than the core module FEMP. In this case the communications between FEMP and OEM EVBs must be strongly standardized to ensure seamless interoperability. In addition communications must be secure and reliability (system availability) should be ensured via redundant communication channels.
In Figure 29 the functional architecture and the components of FEMP are depicted. Then in Table 12 a more detailed description of each component is offered.

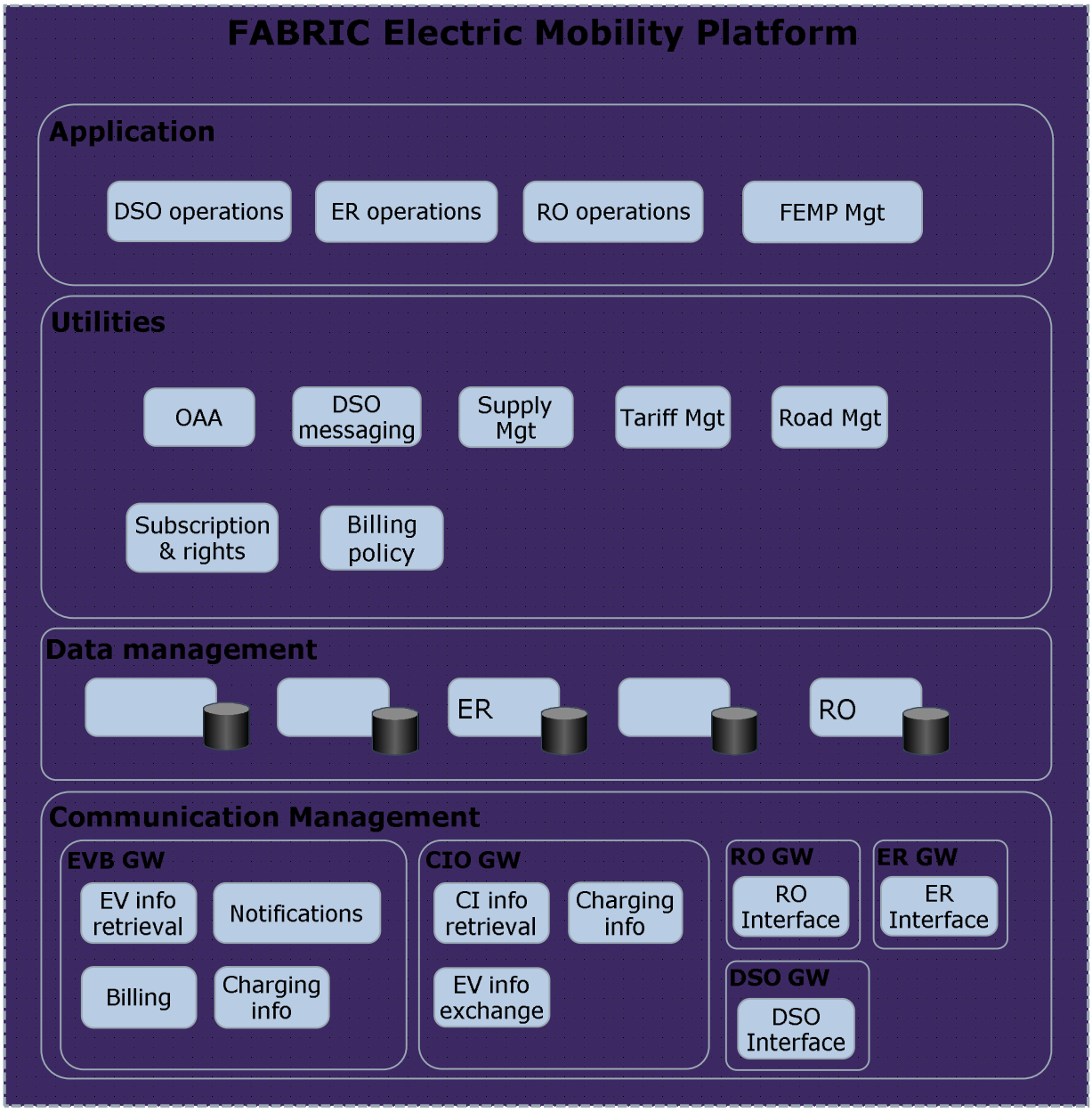


Figure 29: FEMP functional architecture.

Table 12: FEMP components description

Functional component name	Description
Application layer	This layer includes the high level applications for FABRIC Electric Mobility Platform.
DSO operations	This application receives input and requests from the DSO and it communicates replies and messages from FABRIC. It enables the DSO to login to the system and to view the current status of the Charging Infrastructures supervised

	by FABRIC. It connects with the OAA utility to guarantee secure access and it also stores session information to the OPs database for security purposes. Finally it receives information from the DSO regarding supply to the CIs and forwards it to the supply management module of FEMP.
ER operations	This application provides the means to the energy retailer(s) to set the price of energy supply (energy tariff). In the simplest case where there is only one ER (fixed contract) tariff information will be communicated to FABRIC tariff mgt utility and used for billing the end-user. In the more complex case where several ERs compete, the tariff information may go to an auction module in FEMP. The ER is notified via the application about the result of the bidding.
RO operations	This application receives input from the RO and it communicates replies and messages from FABRIC. It enables the RO to login to the system and it connects with the OAA utility to guarantee secure access also storing session information to the OPs database for security purposes. It allows ROs to change the availability status of CIs that are under their supervision due to scheduled or unscheduled events.
FEMP Mgt	This application provides the means to a human operator to manage the parameters of FEMP and also set global parameters affecting the whole FABRIC system. One such functionality is the specification of parameters that define the billing cost as a function of the energy consumed, penalties, energy tariff etc.
Utilities layer	This layer includes utilities and components that support the operation of the high level applications.
OAA	This utility performs Authentication and Authorization of persons that access FABRIC via the operators' interfaces. This is done by crosschecking the submitted credentials with ones stored in OPs database. Several security measures such as limited number of login retries can be implemented to enhance security.
DSO messaging	This module routes messages from FABRIC to DSO. The messages originator could be a module, a system or a human operator. Messages could be free text, standardized ones or replies to actions.
Supply Mgt	This module receives supply restrictions from the DSO. This could be a matrix containing 24h supply schedule for every CIO (CI aggregator) or CI or totals for all FABRIC-supervised CIs. The module can either route the supply information to the CIOs or (feasible scenario) it could contain algorithms to dispatch the CI loads to the available supply based on several optimization parameters. However this is an custom implementation issue.

Tariff Mgt	This module receives energy supply tariff information from the ER. The tariff is then stored to the CI info database. Complex scenarios can be envisioned such as dynamic tariff modulation based on demand forecasts or the existence of many competing ERs. In the latter case, the module could host an auction platform where the ERs could make their bidding based on a forecasted aggregated load from all CIOs that are supervised by FABRIC. The module decides which is the most economic offer and updates the CI info database and the CIOs.
Road Mgt	This utility receives information from Road Operators that may affect the availability of charging infrastructure residing on the specific road segment. The information may include scheduled road maintenance or unscheduled events such as weather phenomena or accidents that prevent use of the road and the charging infrastructure. The utility updates the availability of the affected charging infrastructures in the CI info database and notifies the EVB NAVI utility to replan the routes that include the affected CIs. The event is stored in RO info database.
Subscription & rights	A utility to subscribe external operators to FABRIC and define their access level. Their rights to functionalities could be scalable, depending on their access level. FABRIC operators will be subscribed also via this utility.
Billing policy	This is a utility that provides the means for flexible billing depending not only on the energy consumed and the corresponding tariff (which can be dynamic) but also on penalties such as booking penalties, efficiency penalties etc and on other charges. The FABRIC operator sets the parameters via this utility and then the utility forwards the billing function to the EVB for use in calculating the final cost per charging session.
Data management layer	This layer includes the components and databases to store and manage the various data that are necessary for the applications and their components.
Ops	Database and management functions to store, access and process operators' data such as operator id, operator name, password, operator profile, organization information, address, contact information, access rights etc. In addition it can store information about an operator's connection to FABRIC sessions such as timestamp, duration and perhaps activities. This is for non-repudiation and security purposes.
CI info	Database and management functions to store and access charging facilities' data such as id, name, address, position, nominal operating capacity etc. Dynamic data such as availability status and operating limits will be

	updated in near real-time either by pull or push methods.
RO info	Database and management functions to access information deriving from road operators and RSUs such as weather and traffic information, road-works information etc.
ER info	Energy tariff related information storage.
Communication management layer	This layer includes the components that enable connection with other FABRIC subsystems and external actors such as the DSO, the energy retailer etc.
DSO GW	Gateway to DSO.
DSO interface	This module implements the server side access point to FABRIC for the DSO and realizes the communications as foreseen in the DSO operations application.
ER GW	Gateway to Energy Retailers.
ER interface	This module implements the server side access point to FABRIC for the ERs and realizes the communications as foreseen in the ER operations application.
EVB GW	Gateway to EV Backend.
EVR	EV information Retrieval: Interface to receive EV information data such as battery data, EV location, charging statistics, payment data etc.
Notifications	Interface that enables messaging functionality from the FEMP to the EVB and from there to the EV.
CIT	Charging Infrastructure info Transmission: Interface to transmit charging infrastructure status information (availability, operating characteristics, location etc.) to the EVB.
Billing	Interface to transmit billing formula as defined centrally in the FEMP to the EVB.
CIO GW	Gateway to Charging Infrastructure Operator.
CI info retrieval	Interface to receive information about availability status and operating characteristics of the Charging Infrastructure for storage in the FEMP CI info database and availability of this information to other FABRIC subsystems upon request.
RO GW	Gateway to Road Operators
RO interface	This module implements the server side access point to FABRIC for the RO and realizes the communications as foreseen in the RO operations application.
Web serv	Web interface that enables remote management of FEMP and overview of the system operation by FABRIC operators.

3. DATA SECURITY AND PRIVACY

The objective of this section is to identify the information flow through the FABRIC network and the information stored in various systems and to identify the vulnerabilities and risks involved in order to draft requirements for data security. Based on this analysis, problems in terms of attack models and their counteractions in terms of available security and privacy mechanisms are reported.
This will result in a list of recommendations that will guide the selection of specific currently commercially available security solutions to be used by the FABRIC platform in the application development workpackage (WP25). FABRIC is not a security-focused project and the resources allocated for security and privacy analysis are limited. In addition all of the "subsystem-specific" threats can be addressed once good practices and safety procedures that apply to ICT systems and ITS are in place and used. To ensure privacy and data security each subsystem developer in WP25 should conduct their own study and apply the appropriate techniques and security standards on a component level, something which is too detailed and low level for this document which provides a high-level overview of the system functionality.
The main sequential phases of the security and privacy analysis work were the following:

- Preliminary Information flow consideration (based on sequence diagrams in chapter 2 of this document).
- Personal sensitive data identification.
- Attacker models categorization and risk/threats analysis.
- Identification of the appropriate security solutions and components' recommendations.

The scope of the analysis carried out in the FABRIC project is not re-analyzing the security and privacy ITS requirements (since previous projects have done a very good work on this) but to emphasize and extend the existing security architectures and find the appropriate security solutions for the protection of sensitive data that are communicated, processed and stored within FABRIC. FABRIC can be considered primarily a power systems related project since it relates with power charging of electric vehicles and in that sense security measures that apply to current grid installations should be considered. However ICT plays an important role both for the communication with external actors and for the feasible vision of FABRIC which includes smart booking of charging and other infrastructures, intelligent routing and advanced V2V and V2I communications, which all pose significant risks. In that way, ITS security risk analysis and protection methods also apply in FABRIC.

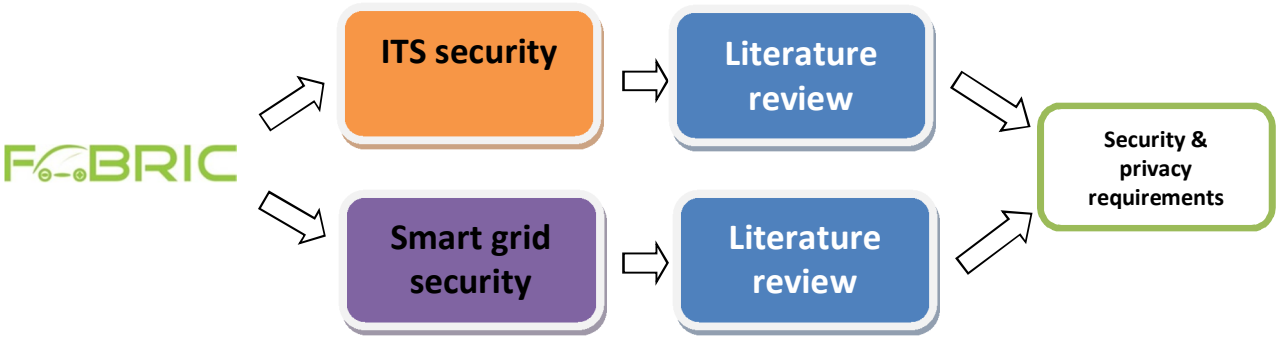


Figure 30: Methodology for the definition of security and privacy requirements

3.1 Benchmarking of relevant research projects

In the last decade, several research projects - both at national and at European level working on Field Operational Tests and V2X communication have dealt with vulnerability of cooperative systems. Such projects have studied solutions able to ensure security and privacy of cooperative transport systems: they cover several domains including cryptographic protection, ID management, privacy support, plausibility checks and in-vehicle security.
Below a summary of the research projects and standardization organizations that are relevant to the ICT/ITS part of FABRIC, as well as the relevance of their achievements to FABRIC, is illustrated in the following table:

Table 13: Research projects and relevance of their achievements to FABRIC

Project description	Objectives	Relevance to FABRIC
PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) The goal of PRESERVE is to bring secure and privacy-protected V2X communication closer to reality by providing and field testing a security and privacy subsystem for V2X systems. PRESERVE will combine and extend results from earlier research projects, integrating and developing them to a pre-deployment stage by enhancing scalability, reducing the cost level, and addressing open deployment issues. It aims at providing comprehensive protection ranging from the vehicle sensors, through the on-board network and V2V/V2I communication, to the receiving application. As a result, PRESERVE will present a complete, scalable, and cost-efficient V2X security subsystem that is close-to market and will be provided to other FOT projects and interested parties for ongoing testing. **Duration:** 2011 – to date http://www.preserve-project.eu	• Create an integrated V2X Security Architecture (VSA) and design, implement, and test a close-to-market implementation termed V2X Security Subsystem (VSS). • Prove that the performance and cost requirements for the VSS arising in current FOTs and future product deployments can be met by the VSS, especially by building a security ASIC for V2X. • Provide a ready-to-use VSS implementation and support to FOTs and interested parties so that a close-to-market security solution can be deployed as part of such activities. • Solve open deployment and technical issues hindering standardization and product predevelopment.	• On board vehicle security regarding information flow from the sensors to the OBU. • V2X Security Architecture for the information exchange between the vehicle and infrastructure or other vehicles. • Cheap and scalable security Application Specific Integrated Circuit (ASIC) for V2X.
OVERSEE (Open Vehicular Secure platform) OVERSEE's expected impact can be defined as developing an open platform for innovative automotive applications with "significant improvements in safety, security and comfort of transport". On longer term OVERSEE will contribute to the worldwide effort for "significant improvements in energy efficiency and emissions reduction" by the reduction of the amount of ECUs in vehicles and hence the reduction of vehicle weight. OVERSEE's research will be concentrated on improving security and dependability of Intelligent Vehicle Systems by developing an execution platform for protected simultaneous execution of multiple applications. Additionally this will offer the potential for favorable prices of innovative automotive applications and therefore the expansion to new emerging markets. **Duration:** 2010 – to date	• Efficient resource virtualization that meets the stringent real-time and security requirements. • Trusted access to security services protected by a vehicular hardware security module. • Flexible trusted dynamic administration of application deployment. • Monitoring capabilities based on a trusted point of control and observations (PCO).	• Security policies that ensure privacy and restrict access to the networks according their needs. • OVERSEE-developed Hardware Security Module (HSM) which provides security services over a standardized programming interface as well as validation support.
PRECIOSA (Privacy enabled capability in co-operative systems and safety applications)	• Define an approach for the privacy evaluation of co-operative systems	• Privacy policies. • Security architecture.

The goal of PRECIOSA is to demonstrate that co-operative systems can comply with future privacy regulations by demonstrating that an example application can be endowed with technologies for suitable privacy protection of the location related data of individuals. PRECIOSA will contribute to common pan-European architecture with these objectives. • Trust models and ontologies for privacy. • Communication verifiable architecture. • Data storage privacy and verifiable architecture. • Validated guidelines for privacy verifiable co-operative systems. **Duration:** 2008 - 2010	in terms of communication privacy and data storage privacy. • Define a privacy aware architecture for cooperative systems which involves suitable trust models and ontologies, a V2V privacy verifiable architecture, and a V2I privacy verifiable architecture, and which includes the architecture components for protection, infringement detection, and auditing. • Define and validate guidelines for privacy aware co-operative systems. • Investigate specific challenges for privacy.	• Guidelines for privacy verifiable cooperative systems.
EVITA (E-safety vehicle intrusion protected applications) Secure and trustworthy intra-vehicular communication is the basis for trustworthy communication among cars or between cars and the infrastructure. Therefore, the objective of the EVITA project is to design, verify, and prototype architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle. By focusing on the protection of the intra-vehicle communication EVITA complements other e-safety related projects that focus on the protection of the vehicle-to-X communication. **Duration:** 2006 - 2011	• Design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle.	• Secure information storage and transmission between the sensors and the OBU inside the vehicle. • Hardware cryptographic engines. • Scalable security architecture.
PRE-DRIVE C2X (Preparation for Driving implementation and evaluation of C2X communication Technology) PRE-DRIVE C2X develops an integrated simulation model for cooperative systems that enables a holistic approach for estimating the expected benefits in terms of safety, efficiency and environment. This includes all tools and methods necessary for functional verification and testing of cooperative systems in laboratory environment and on real roads in the framework of a field operational test. PRE-DRIVE C2X is part of the COMeSafety architecture task force and transferred the COMeSafety architecture description into a detailed specification. PREDRIVE C2X put special focus on all key aspects related to security, privacy and identity management. **Duration:** 2008 - 2010	• Develops and verifies prototype communication platforms. • Prepares test centers and test scenarios. • Conducts simulation studies in order to predict the advantageous effect of CAR-2-X communication on road safety and traffic efficiency.	• Secure communication. • Identity management. • In-vehicle security. • Privacy. • Administrative processes.
Converge The CONVERGE partners prepare regulations for the Car2X systems network, how different traffic institutions should work together in the future according to their responsibilities and roles. Therefore the Car2X systems network establishes a completely new open communication-, services- and organization architecture that reflects communication technologies and technologies of IT security at state of the art. Not only the technology-overarching connecting of communication of vehicles with relevant information sources is taken into account, but also information providers will be included, which are responsible organizationally for the operation of cooperative		

systems of intelligent traffic - so-called IVS systems. These include the operators of traffic infrastructures, cellular networks and networks of traffic infrastructure - the so-called IRS networks - as well as vehicle manufacturers and IVS service providers. Through defined access points, they can be integrated into the open and secure system architecture. The ultimate goal is the decentralized and dynamic coupling of all systems and actors across national borders. http://www.converge-online.de?spid=en		
DRIVE C2X (Driving implementation and Evaluation of C2X communication technology in Europe) EU Integrated Project to deploy a set of cooperative ITS functions at 7 test sites in Europe in order to run Field Operational Tests (FOTs). Supports the development of standard compliant (EU mandate M/458) cooperative systems implementations as well as their integration into vehicles (cars and motorbike) and roadside infrastructure. A test methodology supports the assessment of cooperative driving based on FOT data as well as user feedback.	• Create and harmonise a Europe-wide field operational testing environment on cooperative systems. • Evaluate cooperative systems through impact assessment, technical evaluation and user acceptance. • Promote cooperative driving.	• Security Daemon (SecD) • Privilege Management Infrastructure Daemon (PMID) for ITS station registration and certificates issuing. • Native library for identity and credentials management. • OpenSSL based cryptography • Message formatting based on IEEE 1609.2 and RSA.
CraftITS		• CraftITS/ETSI TS 103 097 WebValidator for validation of software.
C2C-CC Pilot PKI www.sit.fraunhofer.de/de/angebote/projekte/c2x-pki/		• Prototype PKI developed by the C2C-CC
SeVeCom(Secure Vehicle Communication) SeVeCom addresses security of future vehicle communication networks, including both the security and privacy of inter-vehicular and vehicle-infrastructure communication. Its objective is to define the security architecture of such networks, as well as to propose a roadmap for progressive deployment of security functions in these networks. Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I) bring the promise of improved road safety and optimised road traffic through co-operative systems applications. To this end a number of initiatives have been launched, such as the Car-2-Car consortium in Europe, and the DSRC in North America. A prerequisite for the successful deployment of vehicular communications is to make them secure. **Duration:** 2006 – 2009	• Identification of the variety of threats: attacker's model and potential vulnerabilities; in particular, study of attacks against the radio channel and transferred data • Specification of architecture and of security mechanisms which provide the right level of protection. • The definition of cryptographic primitives which take into account the specific operational environment.	• Threats identification. • Security architecture. • Security Mechanisms. • Secure communication protocols. • Privacy.
simTD (Safe and intelligent mobility: Test field Germany) sim^{TD} is a large scale Field Operational Test (FOT) in Germany. It is the worldwide first field operational trial for car-to-x (C2X) technology that applies several hundred vehicles and roadside stations in a real-life environment in order to evaluate the entire spectrum of applications with regard to effects on traffic safety and traffic efficiency.	• Increased road safety and improved efficiency of traffic using of car-to-x communication • Definition and validation of a roll-out scenario for identified functions and applications for scientific questions through experiments and FOTs. • Consolidation of car-to-x functions for traffic efficiency, driving, safety and value-added services. • Definition, analysis and specification of functions to be developed and tested, as well the overall system. • Testing and validation. • Consolidation and harmonisation of	• Near-series security architecture for C2X communications. • Several concepts, protocols and cryptographic procedures that were used in simTD. • Strategies to protect driver's privacy based on pseudonyms • Security module.

	requirements from the perspective of feasibility, performance and compatibility.	
OpenSSL The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.		• Cryptography

Table 14: Commercial solutions for V2X communications

Commercial solutions for secure V2X communication	
Escrypt CycurV2X	CycurV2X is focused on providing a self-contained and complete security solution for V2X applications according to the latest standards while optimizing cost-efficiency in small to mid-volume markets. ESCRYPT's V2X security application encapsulates the IEEE 1609.2 draft security protocol handling and makes integration into existing applications, e.g. on-board units (OBU) and road-side units (RSU), easy. CycurV2X provides a highly optimized cryptographic engine to perform up to 400 signature generations/verifications over elliptic curves per second. Furthermore, it provides strong encryption/decryption of messages based on ECIES-AES-CCM as well as WAVE certificate handling.
NXP RoadLINK SAF5100	The SAF5100 is a flexible software-defined radio processor for car-to-car (C2C) and car-to-infrastructure (C2I) communication, helping to realize NXP's vision for a complete C2X (C2C+C2I) solution. Scheduled for mass production in the second half of 2014, the SAF5100 is also the first product to become generally available from the MK4 reference design for connected vehicles, following its unveiling in July by NXP and Cohda Wireless, a leading specialist in wireless communication for automotive safety applications. The SAF5100 processor is fully programmable and can support unique algorithms to improve reception in wireless communication. The SAF5100 can support multiple wireless standards as well as different OEM antenna configurations like 802.11p

	antenna diversity, providing OEMs with the flexibility to support emerging standards across multiple regions via firmware updates. It also provides best-in-class wireless link performance via the 802.11p firmware from Cohda Wireless, which is a fully integrated part of the solution. With a 12-mm x 12-mm LFBGA package, the SAF5100 has a very small PCB footprint which allows the 802.11p receiver to fit into confined spaces, and significantly reduces bill of materials (BOM) costs. The unique software-defined radio approach allows OEMs to deploy a global C2X solution based on a single hardware platform with end-of-line configurability by firmware download.
Cohda MK4	The MK4 is a complete solution incorporating Cohda's field-proven network layer, facilities layer and applications layer software products. It supports international standards including IEEE 1609 for US operation, ETSI TC-ITS for European use and the Japanese standard at 760 MHz (ARIB STD-T109). The MK4 also comes with an open and extensible Software Development Kit (SDK) that allows customers to configure and evolve Cohda applications to meet their own specific requirements.
Marben PANGAEA4	Marben PANGAEA is a CAR 2 CAR Day 1 Application Platform based on the Autotalks PLUTON V2X RF transceiver and CRATON V2X communication processor. It has full support of C2C Day 1 profile and provides all-packets verification, secure signing, tamper-proof storage and secure boot.

Table 15: Technical reports for security and privacy that are related to FABRIC

Technical reports	
Report	**Objectives**
ETSI (ETSI TR 102 893 V1.1.1) (2010-03) This technical report summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) operating in a fully	Preparation of a full TVRA (using guidelines from ISO 15408 and TS 102 165-1) for ITS covering Vehicle to vehicle, Vehicle to roadside infrastructure (network), Vehicle to roadside standalone unit and ITS integration with Internet communication scenarios.

deployed ITS.	
ETSI TS 102 731 V1.1.1 (2010-09) Intelligent Transport Systems (ITS); Security; Security Services and Architecture	Specifies mechanisms at the stage 2 level defined by ETS 300 387 [i.2] for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization.
ETSI TS 102 867 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2	Specifies the use of the mechanisms of IEEE 1609.2 within the ITS communications architecture defined in EN 302 665 to provide a stage 3 implementation for a subset of the security services defined in TS 102 731.
ETSI TS 102 940 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management	Specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in TS 102 731, it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in EN 302 665. The document also identifies the roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. These include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.
ETSI TS 102 941 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Trust and Privacy Management	Specifies the trust and privacy management for Intelligent Transport System (ITS) communications. Based upon the security services defined in TS 102 731 and the security architecture define in TS 102 940, it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in EN 302 665. The document identifies and specifies security services for the establishment and maintenance of identities and cryptographic keys in an Intelligent Transport System (ITS). Its purpose is to provide the functions upon which systems of trust and privacy can be built within an ITS.
ETSI TS 102 942 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Access Control	Specifies authentication and authorization services to avoid unauthorized access to ITS services. The document also specifies measures to ensure the required level of security and privacy for ITS

	message communication.
ETSI TS 102 943 V1.1.1 (2012-06) Intelligent Transport Systems (ITS); Security; Confidentiality services	Specifies services to ensure that that the confidentiality of information sent to and from an Intelligent Transport System (ITS) station can be maintained at a level that is acceptable to the users of the station.
ETSI TS 103 097 V1.1.1 (2013-04) Intelligent Transport Systems (ITS); Security; Security header and formats	Specifies security header and formats for Intelligent Transport Systems. These formats are defined specifically for securing G5 communication.
Draft ETSI TS 102 723-8 V1.0.0 (2013-07) Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer	Specifies interfaces between the ITS security entity and the ITS network and transport layers including interface services and service primitives which are extensible in order to achieve general applicability. Additionally, it specifies related procedures and common parameters.
NIST Interagency Report (IR) 7628: Guidelines for Smart Grid Cyber Security (2010-09)	NISTIR 7628 is a three-volume document with Volume 1 containing technical material for maintaining the security of the grid, including a reference architecture and high-level security requirements; Volume 2 addresses privacy issues, containing a discussion of potential privacy issues in smart grid compared to other networked systems; and Volume 3 contains analyses and references that support the document's contents.

3.2 FABRIC communication architecture

In Chapter 2 of this document there is a detailed depiction of the foreseen information flow between all the modules, on-board and off-board the vehicle, of the FABRIC system. In the figure below a high level architecture diagram is provided to identify the main physical blocks and the communication channels between them that are vulnerable to attacks.

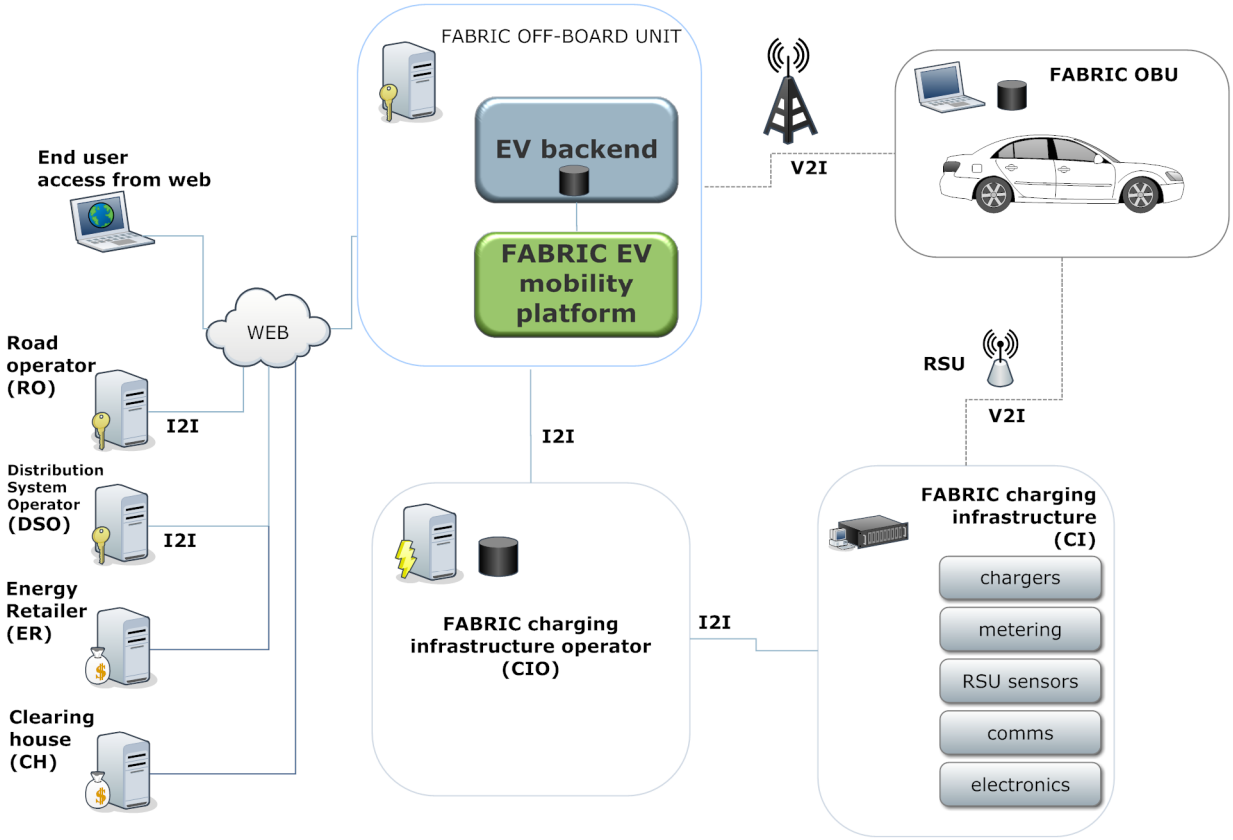


Figure 31: High level communications architecture diagram identifying main communication channels.

In Figure 31 the following logical interfaces are shown:

- OBU to communication infrastructures
- Communication infrastructure to FABRIC off-board unit and routed either to the EV backend or the FABRIC EV mobility platform
- Communication infrastructure to charging infrastructure
- Charging infrastructure to charging infrastructure operator
- Charging infrastructure operator to FABRIC off-board unit
- Web interfaces of external actors and end user to FABRIC off-board unit.

3.2.1 Communication technologies for FABRIC

For the communication of the nodes shown in the previous section, the following communication technologies can be used based on the State of the Art study on communications found in D33.1.

In Figure 32 the preliminary concept of FABRIC, as described in the Description of Work, is sketched.

According to the use cases in D43.1 and the sequence diagrams of Chapter 2 the following functionalities can be identified:

- Charging request to the infrastructure by the EV.
- Approval/denial of request.
- Automatic detection/identification of vehicle and identification of driver by RSU connected to the wireless charging modules.
- Driver assistance services provided by the infrastructure, regarding speed, alignment/lane departure.
- Traffic control services provided by the infrastructure (desired but not mandatory).
- V2V communication (desired but not mandatory).
- Infrastructure booking and booking management.
- Assisted navigation (desired but not mandatory).
- Charging status measurement and payment information provided by the infrastructure to the vehicle and/or driver.
- Energy management by the grid operator based on requested charge and the grid restrictions.
- Tariff definition by external actors.

Also offline functionalities include

- Registration of end users and vehicles.
- Registration of external actors to FABRIC.
- Logging in to the system for both end users and external actors.
- Account management.
- Billing services.

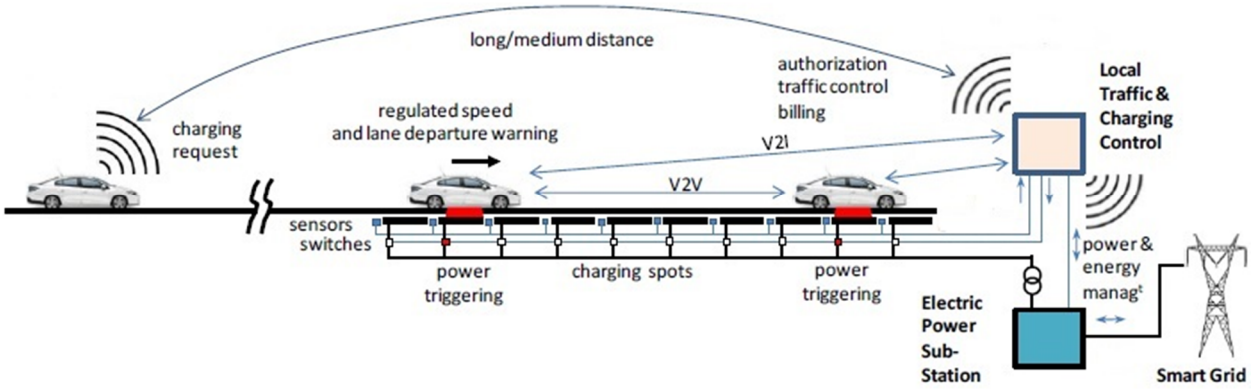


Figure 32: Schematic principle of the FABRIC ICT solutions related to the operation of an on-road-charging station. Several communication channels are depicted.

Based on the identified functionalities several long and short-range communications, both wireless and wired can be identified.

Specifically the following communication types should be included:

- V2I (FABRIC off-board unit) long-range communication (wireless)
- V2I (FABRIC charging infrastructure operator) long/medium-range communication (wireless)
- V2I (RSU) short-range communications (wireless)
- V2V short-range communications (wireless)
- I2I Grid operator to energy supplier communication (wired)
- I2I external actors to FABRIC (wired)
- I2I RSU (metering/control) to FABRIC charging infrastructure operator (wired)
- Infrastructure to driver nomadic device (mobile phone or other) (wireless)

Figure 33 provides a close up to the wireless charging concept that will be used in FABRIC test sites. In this figure we can see in more detail the infrastructure-side communications needed when the vehicle is in charging mode:

- Vehicle/driver identification.
- Vehicle position detection so as to energize a specific charging pad.
- RSU communication with charging infrastructure operator via the CI.

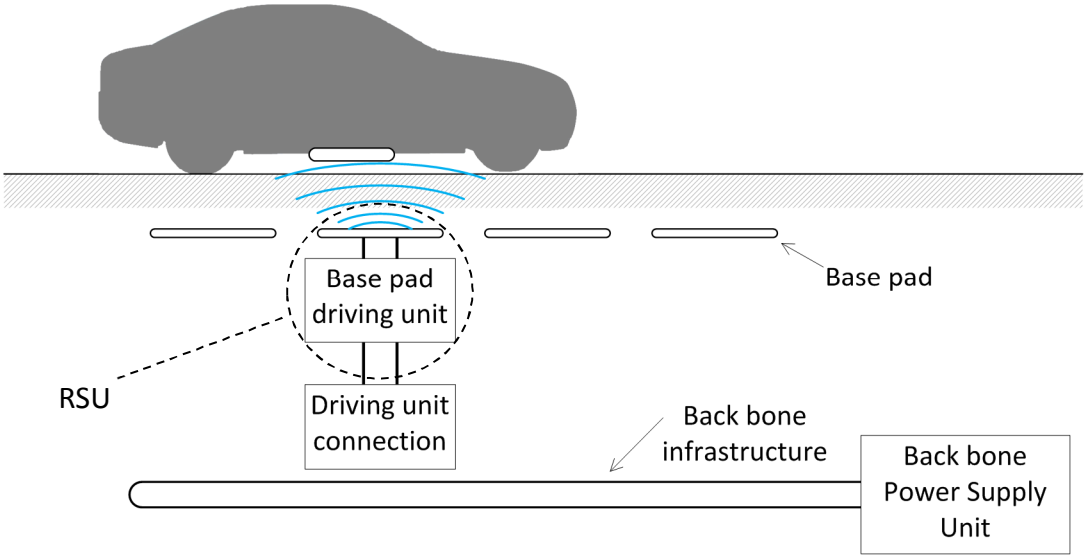


Figure 33: Draft concept of an installed charging spot system for wireless dynamic charging.

In Figure 34 a preliminary topology of the installed pads and their connection to the grid is depicted.

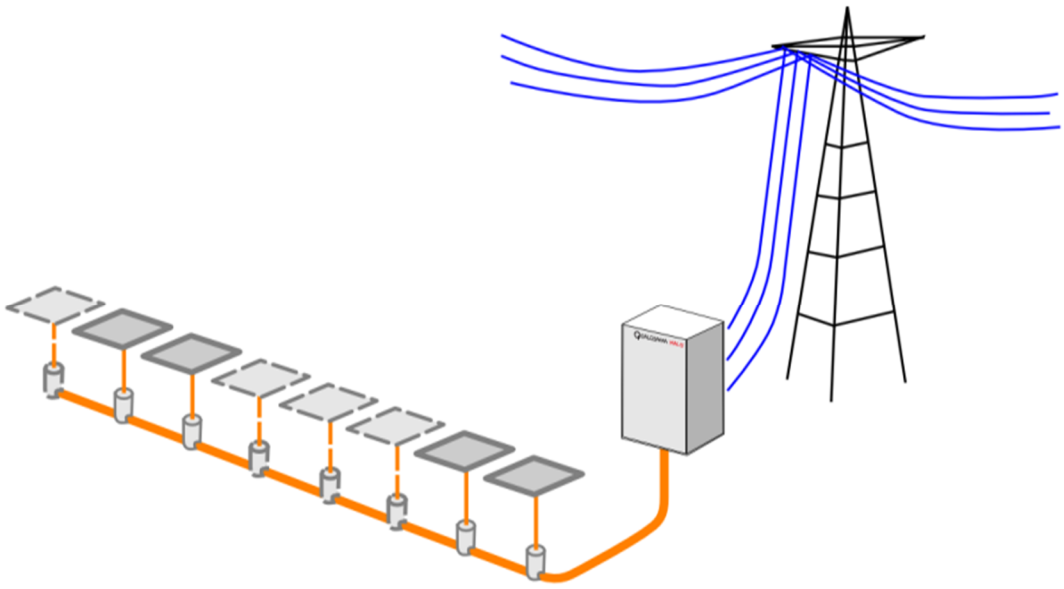


Figure 34: Topology concept of charging pads installation and connection to the grid for the FABRIC test sites. Wired communication channels are evident.

The following table provides a mapping of communication types to FABRIC functionalities.

Table 16: FABRIC communications to functionalities mapping

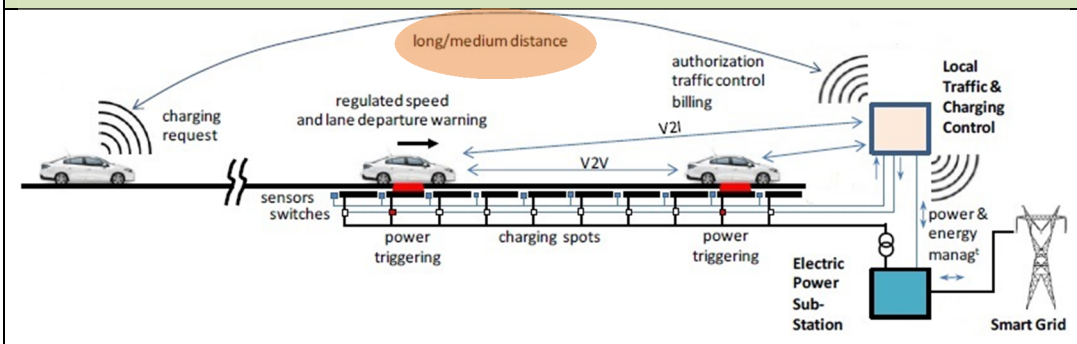
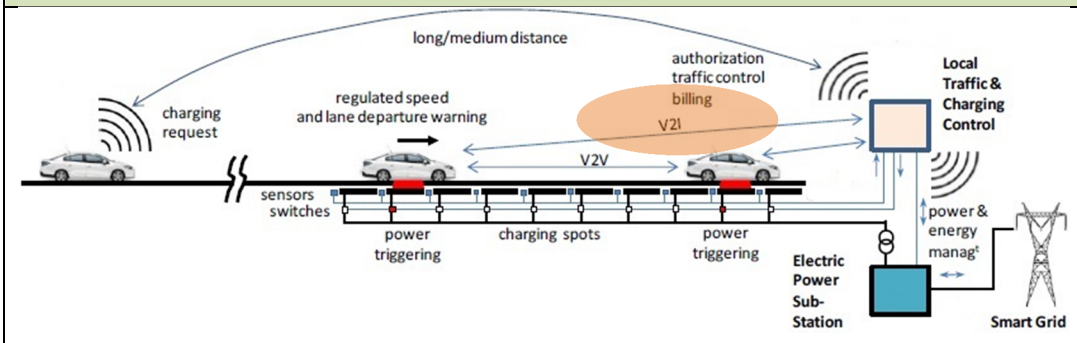
WIRELESS **WIRED**

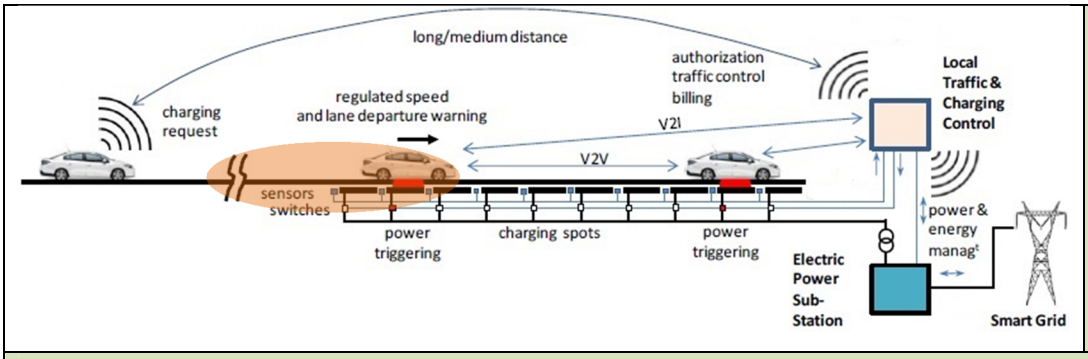
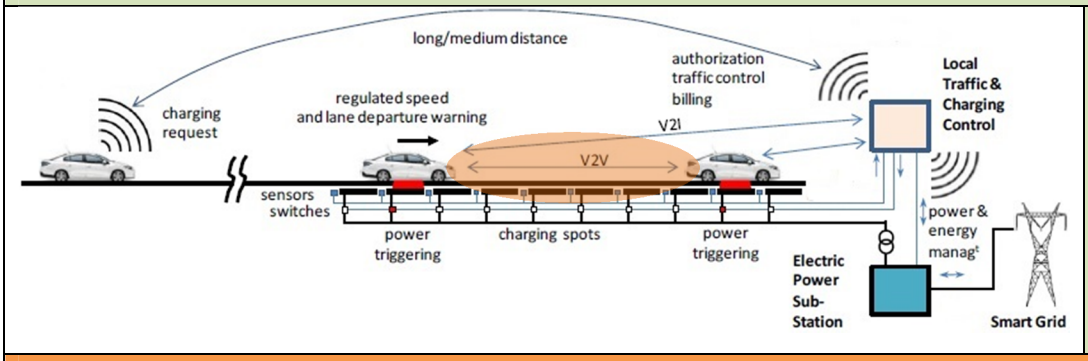
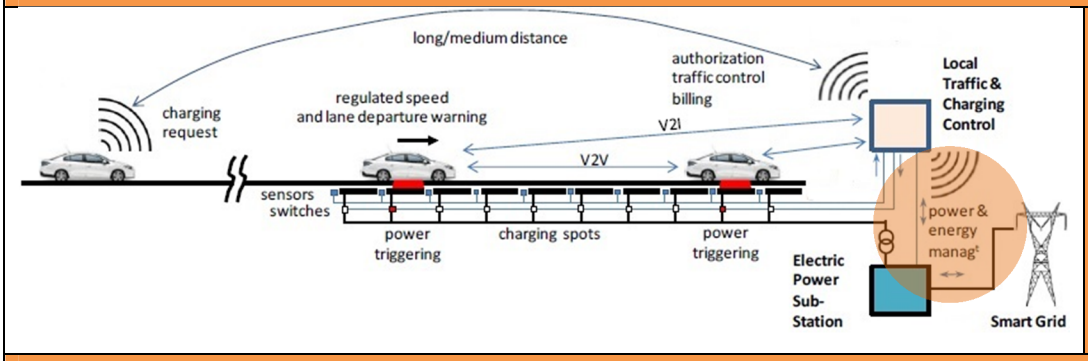
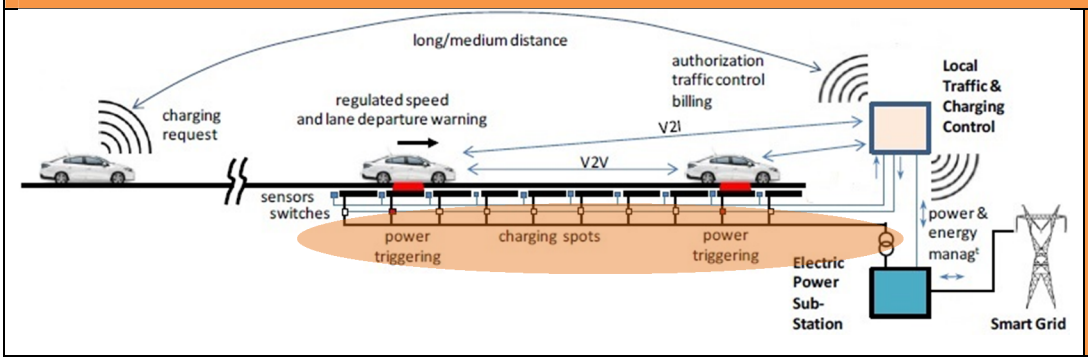
Logical interface	Example Functions
V2I (FABRIC off-board unit) long-range communication.	• Trip planning. • Navigation. • Infrastructure status updates. • Infrastructure booking. • Notifications from FABRIC. • Charging request to the infrastructure by the EV. • Charging authorization. • Information about available charging lanes and directions on how to reach them.
V2G (charging infrastructure operator) long/medium-range communication.	
V2I medium/short-range communications.	• Driver assistance services provided by the infrastructure, regarding speed, coil alignment/lane departure. • Local traffic and charging control services provided by the infrastructure. • Automatic detection of vehicle and identification of driver/EV by RSU connected to the wireless charging modules. • Charging management information exchange.
V2V short-range communications.	• Traffic report/control services provided by other vehicles.
Grid, road operator and energy supplier communication with the FABRIC platform.	• Energy supply restrictions by the DSO transmitted to FABRIC charging infrastructure. • Energy tariff information transmitted to FABRIC. • Charging data and billing information exchange.
RSU/charging pads to charging infrastructure operator.	• Automatic detection of vehicle. • Charging monitoring and metering. • Charging management and load balancing.

FABRIC to clearing house entity	• Billing and charging information exchange. • EV and driver information exchange.
End-user to FABRIC	• Charging statistics and billing information review. • User and EV profile management.

In the following table, the possible communication technologies and standards for the realization of these communications are presented in detail.

Table 17: FABRIC foreseen communications

Communication channel	Technology
V2I and V2G long range communication	
	3G, LTE
V2I medium range communication	
	LTE, ITS-G5, CALM
V2I short range communication	

	DSRC, MMWAVE, IR
V2V short range communication	
	DSRC, LTE, ITS-G5
I2I external actors to FABRIC communication	
	DSL, LTE
RSU/charging pads to charging infrastructure operator	
	PLC, DSL, Ethernet, WAN

3.2.2 V2V communications for a feasible future FABRIC implementation.

Current commercial wireless networks are designed primarily for point-to-point connectivity, and not for broadcast messaging. FEV re-charging spot notification however requires a capability of broadcasting potentially large amount of safety information to the geographically relevant on-board devices. In past nomadic device oriented research projects - such as the CoCar research project - this has been accomplished by having each device maintain a GPRS based connectivity to the application server, individually downloading the generated safety messages, and checking its geographic relevance against actual coordinates. This approach will not scale to larger deployments. In contrast, Mobility2.0 project [14] explores the capabilities of existing 5.9GHz geo-broadcasting communication capabilities by implementing the scenario of a FEV acting as a virtual Road Side Unit that broadcasts FEV-related information to other FEVs nearby. Among others, information useful to be transmitted in this way could be the charging spot notifications updates. Along this RSU direction, future electric vehicles are assumed to have 5.9 GHz DSRC communication capabilities.
Such architecture could be considered in future feasible deployments of a FABRIC system which entails V2V communications not only for broadcasting safety related information but also for real time negotiations over using the same charging infrastructure at the same time or for broadcasting information about changes regarding the charging infrastructure operational characteristics (e.g. lower than the nominal charging capacity due to DSO restrictions).
However V2V communications are not foreseen in the development and testing phases of FABRIC project.

3.3 FABRIC security analysis

3.3.1 Security and privacy prerequisites

An outline of the minimum security and privacy characteristics that should be taken into account when designing FABRIC communications and data storage architecture is presented in Table 18.

Table 18: Security and privacy prerequisites

Prerequisite		Description
Authenticity	ID authentication	Verification of the sender's unique ID
	Location authentication	Verification of the sender's claimed position
	Property authentication	Verification of the sender's properties
Access control		FABRIC has to define the user's rights such as whether the user can use two devices simultaneously etc (this might be the case where the user is a company operating a fleet).
Accountability		The process of auditing all changes to security parameters and applications. FABRIC has to be able to trace back the sender-

		receiver activity.
Availability		The ability to use information or resources as desired. FABRIC has to guarantee timely services.
Confidentiality		The act of keeping unauthorized users (or non-users) from accessing sensitive information. Only the FABRIC platform should be able to monitor and access information transmitted between sender and receiver and stored in FABRIC databases.
Integrity		The data state is the same as in the data source and has not been exposed to accidental or malicious alteration or destruction. FABRIC should be able to verify the integrity of the transmitted information.
Privacy	ID privacy	The identity of the users has to be protected and hidden.
	Jurisdictional access	Specific public authorities should be able to access the identity and location of the sender according to the legal procedures.
	Location privacy	The location of the sender has to be protected and hidden.

3.3.2 Attacker profiles

Before presenting the risk analysis carried out in the project, a classification of the attacker profiles is deemed appropriate. This is shown in Table 19. The source is [6] and it is deemed suitable for FABRIC since the system to be developed falls both in ITS and smart grid categories.

Table 19: Attacker profiles

Attacker type	Description
Nation states	State-run, well organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having an economic, military or political advantage.
Hackers	A group of individuals (hackers, phreakers, crackers, trashers, pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws. They range from inexperienced, amateur hackers that use hacking tools found in the internet, without understanding the hacking process, to experienced and professional hackers that have substantial expertise in the TCP/IP protocol suite and a deep knowledge of the workings of various operating

	systems. These types of hackers generally conduct attacks after doing research on the type of victim. They are often looking for high-visibility, high-profile, often well-protected victims whom they can hack to prove their hacking expertise. Professional hackers are also motivated by profit, so they often conduct corporate espionage.
Terrorists/cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized crime	Coordinated criminal activities including cyber-crimes. An organized and well-financed criminal organization.
Other criminal elements	Another facet of the criminal community, which is normally not well organized or financed. Normally consists of few individuals, or of one individual acting alone.
Industrial competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments in the form of corporate espionage.
Disgruntled employees	Dissatisfied individuals with the potential to inflict harm on the system network or related systems. This can represent an insider threat depending on the current state of the individual's employment and access to the systems.
Careless or poorly trained employees	Those users who, either through lack of training, lack of concern, or lack of attentiveness pose a threat to the system. This is another example of an insider threat or adversary.

3.3.3 Threat analysis

This section analyzes the main security threats to be taken into consideration while designing and developing a technological system and it applies to FABRIC.
In order to ensure a common understanding context with the reader, the following brief glossary describes the most important terms that are related to security:

Table 20: Threat analysis glossary

Term	Description
Asset	A resource of value to be protected from unauthorized access, such as the data in a database or on the file system, or a system resource.
Threat	A potential occurrence – malicious or otherwise – that may harm an asset.
Vulnerability	A system weakness that makes a threat possible.

Attack or exploit	An action taken to harm or gain unauthorized access to an asset.
Countermeasure	A safeguard that addresses a threat and mitigates the associated risk.

In the following table, the main threats are presented:

Table 21: Potential threats to a FABRIC system

Threat	Description	Applicable to
Denial of Service (DoS attack)	The attacker attempts to make the network resource unavailable to its intended users by flooding the web server with communication in order to keep it busy. The attack exploits the "availability" system requirement.	- Publicly accessible FABRIC interfaces.
Disclosure	The attacker acquiring sensitive information through unauthorized channels.	- FABRIC databases - Communication channels exchanging this type of info.
Manipulation/Injection of information (man in the middle attack)	The attacker intercepts and modifies data (in a syntactically valid manner) destined to another system. Data could also be destroyed (black hole).	- Vehicle - RSU
Masquerading	The attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.	- Vehicle - RSU
Replay attack	The attacker repeats or delays a valid data transmission.	- Vehicle - RSU
Eavesdropping/Traffic analysis (sniffing)	The attacker analyses and monitors the transported information between sender and receiver. The attacker can obtain sensitive information such as passwords, data, and protocols for performing specific actions.	- All communication channels in FABRIC
Repudiation	A threat action whereby an entity deceives another by falsely denying responsibility for an act.	- End-users - Operators
Viruses/malware	Malicious software used by hackers in order to obtain information or cause harm to a system.	- FABRIC platform - EV backend - Charging infrastructure operator - OBU
Trojan horses/keyloggers	Software used by hackers in order to obtain information or even control of the affected system without being noticed.	- FABRIC platform - EV backend - Charging infrastructure

		operator - OBU
Worms	Programs that propagate autonomously from computer to computer via network connections. Worms may have portions of themselves running on several different computers. Worms may carry malware and viruses.	- FABRIC platform - EV backend - Charging infrastructure operator - OBU
Password cracking	The use of specialized software to gain access to a system through an authorized user's account.	- FABRIC platform - EV backend - Charging infrastructure operator
Social engineering	The attacker takes hold of access credentials by using other than technological means e.g. by deceiving human operators into granting access or resetting credentials.	- FABRIC platform - EV backend - Charging infrastructure operator
Intrusion attacks	The use of various hacking tools to gain access to a system.	- FABRIC platform - EV backend - Charging infrastructure operator - OBU
Network spoofing	A system presents itself to the network as if it were another system.	- FABRIC platform - EV backend - External actor interfaces
Installation errors	Poor installation procedures may lead to errors and vulnerabilities.	- FABRIC platform - EV backend - Charging infrastructure operator
Known software weaknesses (security holes)	Misuse of known software weaknesses is the act of bypassing security controls in order to gain access, obtain information or upgrade privileges.	- FABRIC platform - EV backend - Charging infrastructure operator
Message saturation	The purpose of this type of attack is to saturate the connections inside the vehicle.	- Vehicle
Jamming of radio signals	The transmission of radio signals that disrupt communications by decreasing the signal to noise ratio.	- Vehicle - RSU
GNSS spoofing	The transmission of counterfeit GNSS-like signals that force the receiver to compute erroneous positions. The user believes	- Vehicle

himself to be in another location.

3.3.4 Countermeasures

The following table summarizes well known countermeasure strategies for the identified system threats. They can be considered as guidelines for the design and development of ICT in FABRIC or for a feasible commercial FABRIC-based system that can be deployed in a large scale.

Table 22: Countermeasures for the identified threats.

Threat	Countermeasures
Repudiation	• Implement a non-repudiation framework. • Include a source identity in each ITS message and operator message. • Maintain an audit log of the type and content of each message sent from and received by a sub-system. • Hardware-based protection of software and hardware configuration on ITS-S.
Viruses, Malware, Trojan horses, Worms	• Implement a Privileged Management Infrastructure (PMI) • Stay current with the latest operating system service packs and software patches. • Block all unnecessary ports at the firewall and host. • Disable unused functionality including protocols and services. • Harden weak, default configuration settings. • Install antivirus and keep it up-to-date. Automatic updates recommended. • Hardware-based protection of software and hardware configuration.
Password cracking	• Use strong passwords for all account types. • Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password. • Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications. • Audit failed logins for patterns of password hacking attempts.
DoS attacks	• Configure your applications, services, and operating system with denial of service in mind. • Stay current with patches and security updates. • Harden the TCP/IP stack against denial of service. • Make sure your account lockout policies cannot be exploited to lock out well known service accounts.

	• Make sure your application is capable of handling high volumes of traffic and that thresholds are in place to handle abnormally high loads. • Review your application's failover functionality. • Use an IDS that can detect potential denial of service attacks.
Impersonation	• Use a using statement to automatically revert impersonation. • Granularly impersonate only those operations that need it.
Eavesdropping	• Encrypt the transmission of personal and private data.
Replay attack	• Session Tokens: A pseudo random token should be issued to the user when the request comes from a legitimate user then this session token has to be submitted by the user whenever he sends the subsequent request thus the server can cross check this session token with the token stored at server side • Timestamps: This is another way of preventing a replay attack, in this synchronization of the time should be achieved using a secure protocol (UTC or GNSS). • Limit the session time: Enforce session time limits to invalidate state information and session IDs after a certain period of inactivity. • Deny concurrent logins: Disallow users from having multiple, concurrent authenticated sessions to the application.
Manipulation of information	• Performing of deep inspections throughout entire sessions. • Usage of packet-filtering devices. • Strong firewall rules for the inspection of data traffic. • Limit message traffic to V2I/I2V and implement station registration. • Digitally sign each message using a Kerberos/PKI-like token system. • Plausibility checks on incoming messages. • Information encryption.
Social engineering	• Train human operators to demand proof of identity over the phone and in person. • Define values for types of information, such as dial-in numbers, user names, passwords, network addresses, etc. The greater the value, the higher the security around those items should be maintained. • If someone requests privileged information, operators should find out why they want it and whether they are authorized to obtain it. • Verify information contained in e-mails and use bookmarked links instead of links in e-mails to go to company web sites.

	• Dispose of sensitive documents securely, such as shredding or incinerating.
Intrusion attacks	• Continuously monitoring of suspicious applications or suspicious network traffic.
Network Spoofing	• Filtering of incoming packets that appear to come from an internal IP address at the system perimeter. • Filtering of outgoing packets that appear to originate from an invalid local IP address.
Installation errors	• Strong installation procedures for the successful installation of software.
Misuse of known software weaknesses	• Keeping up-to-date with security and other patches available by official and trusted sources.
Message saturation	• Reduce frequency of beaconing and other repeated messages. • Add source identification (IP address equivalent) in V2V messages. • Limit message traffic to V2I/I2V and implement station registration.
Jamming of radio signals	• Implement frequency agility within the 5,9 GHz band. • Implement ITS G5A as a CDMA/spread-spectrum system or base ITS on 3rd/4th Generation mobile.
GNSS spoofing	• Limit message traffic to V2I/I2V and implement station registration. • Use INS or existing dead-reckoning methods (with regular - but possibly infrequent - GNSS corrections) to provide positional data. • Implement differential monitoring on the GNSS system to identify unusual changes in position.
Location tracking	• Use a pseudonym that cannot be linked to the true identity of either the user or the user's vehicle.

3.3.5 Security requirements

Based on the previously identified threats, that are relevant to the various subsystems and communication links of an envisioned FABRIC system, the following security requirements can be formulated. A large scale implementation of this system in the future is expected to respect the following requirements.

Table 23: FABRIC security requirements

Requirement ID	Security requirement
SP2_REQ_SEC_1	The platform will respect the common security targets.
SP2_REQ_SEC_2	There shall be security association between communication participants.

SP2_REQ_SEC_3	The platform must not require permanent online access to the backend systems.
SP2_REQ_SEC_4	Unique as well as anonymous authorisation shall be provided for end-users.
SP2_REQ_SEC_5	Integrity and authenticity of communications shall be ensured.
SP2_REQ_SEC_6	There shall be a central ITS authority, which impersonates the root of trust.
SP2_REQ_SEC_7	There shall be a public key infrastructure to establish security associations.
SP2_REQ_SEC_8	The ITS authority shall issue enrolment and authorisation credentials.
SP2_REQ_SEC_9	The ITS authority shall provide mechanisms to revoke security associations.
SP2_REQ_SEC_10	Security credentials shall contain immutable attributes reflecting access rights and privileges of a node.
SP2_REQ_SEC_11	Integrity and authenticity of aggregated data shall be preserved.
SP2_REQ_SEC_12	Secure user login to FABRIC applications.
SP2_REQ_SEC_13	FABRIC has to authorize applications before allowing their installation.
SP2_REQ_SEC_14	Safe exchange of personal data with third party applications.

FABRIC project aims to develop prototypes in order to assess the feasibility and efficiency of dynamic wireless EV charging. In that way, development of security mechanisms in the lifetime of the project is not a primary objective, while there are other R&D projects that specialize in security aspects of ITS. The requirements table above and the preceding threat analysis addresses the needs for a fully deployed and market ready solution, where security and privacy are of paramount concern since negligence in those areas they may lead even to health and safety hazards.

3.4 FABRIC privacy analysis

3.4.1 FABRIC personal information identification

Personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". This definition is meant to be very broad. Four dimensions of privacy are considered:

(1) personal information—any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural, locational, or social identity;
(2) personal privacy—the right to control the integrity of one's own body;
(3) behavioral privacy—the right of individuals to make their own choices about what they do and to keep certain personal behaviors from being shared with others; and

(4) personal communications privacy—the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because most data protection laws and regulations cover privacy of personal information. However, the other three dimensions are important privacy considerations as well; thus dimensions 2, 3, and 4 should also be considered in the Smart Grid context because new types of energy use data can be created and communicated. For instance, unique electric signatures for consumer electronics and appliances can be recognized and detailed, time-stamped activity reports within personal dwellings can be produced. Charging station information can detail whereabouts of an EV. This data did not exist before the application of Smart Grid technologies.

FABRIC personal data can be classified into two different types such as:

1. data regarding the driver and
2. data regarding the vehicle.

Driver and vehicle related personal data are described in Table 24.

Table 24: Identified private data for end-users and EVs in FABRIC

Driver/owner personal data	- Name - Contact information - Billing information - Vehicle information - Language preference, emergency contact information, licence plate number - FABRIC preferences - Current position and planned destination - Habitual routes, charging habits, preferred charging stations etc.
EV identity data	- Vehicle identification number (VIN), make, model, year, etc. - Information about the vehicle operation, diagnostic error codes, battery SoC, odometer and range information. - Location and speed of the vehicle. - Vehicle features. - Vehicle collisions history. - Traffic data received by the vehicle.

3.4.2 Privacy requirements

Privacy is strongly related to human users and their data as listed in Table 24. Vehicle and personal stations are the most popular targets for attack since they are used by the end-users and produce sensible data such as location, preferences and user/vehicle characteristics that could be intercepted and exploited for a later attack. With that in mind they should be the assets to be protected the most when designing a system.

In addition backend and infrastructure components that process, exchange and store personal data need to follow strict guidelines to guarantee the privacy of the users. FABRIC foresees

large scale integration of transportation with smart grids. A feasible EV-charging system in the near future will include bi-directional power flow between the EV and the smart grid. The EV could also be used to power the user's home. In that context, The Smart Grid will greatly expand the amount of data that can be monitored, collected, aggregated, and analyzed. This expanded information, particularly from energy consumers and other individuals, raises added privacy concerns. For example, specific appliances and generators may be identified from the signatures they exhibit in electric information at the meter when collections occur with great frequency as opposed to through traditional monthly meter readings. Data may also be collected from electric vehicles. Charging data may be used to track the travel times and locations for the EV owners. This more detailed information expands the possibility of intruding on consumers' and other individuals' privacy expectations. This new situation demands a more careful analysis of the collected data and their impact on privacy deterioration, and special procedures should be drafted on how to classify, collect, process and store each kind of information.
The following table lists the privacy requirements for a feasible FABRIC system in deployment phase.

Table 25: Privacy requirements.

Requirement ID	Privacy requirement
SP2_REQ_PRIV_1	Privacy of mobile nodes shall be preserved through anonymous or pseudonymous communications.
SP2_REQ_PRIV_2	Public identifiers of a mobile node shall be changed in regular intervals.
SP2_REQ_PRIV_3	All public identifiers must be variable and shall follow the joint ID change.
SP2_REQ_PRIV_4	During safety critical situations node ID changes shall be suspended.
SP2_REQ_PRIV_5	An ID Management component shall trigger ID changes and provide unique IDs.
SP2_REQ_PRIV_6	One-to-one communication channels should not be interceptable by third parties
SP2_REQ_PRIV_7	Aggregated data is confidential and shall be protected from unauthorized access.
SP2_REQ_PRIV_8	Before sharing data with backend services, mobile nodes should apply additional anonymisation measures.
SP2_REQ_PRIV_9	Compliance with EU Directive 96/46/EC4 is mandatory.
SP2_REQ_PRIV_10	Provide users with a clear and understandable privacy policy notice.
SP2_REQ_PRIV_11	Provide users with data privacy settings modification functionality.
SP2_REQ_PRIV_12	Lawful lifecycle of stored private information.
SP2_REQ_PRIV_13	Stored sensitive data should be encrypted.

In [6] privacy protection recommendations can be found. Even though these are focused on Smart Grids in general, they are applicable to an EV charging system such as FABRIC. The recommendations are the outcome of a Privacy Impact Assessment that takes into account the American Institute of Certified Public Accounts (AICPA) Generally Accepted Privacy Principles

(GAPPs), the Organisation for Economic Cooperation and Development (OECD) Privacy Principles, and information security management principles from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) *International Standard ISO/IEC 27001.*
The following points summarize the PIA recommendations (that can also be considered requirements during the system design) as presented in the draft *NIST Smart Grid High-Level Consumer-to-Utility Privacy Impact Assessment.* FABRIC or a future FABRIC-like system is considered to be a part of the "Smart Grid" and in that way the following recommendations apply to it as well.

- **Assign privacy responsibility**. Each organization collecting or using Smart Grid data from or about consumer locations should create (or augment) a position or person with responsibility to ensure that privacy policies and practices exist and are followed. Responsibilities should include documenting, ensuring the implementation of, and managing requirements for regular training and ongoing awareness activities.
- **Establish privacy audits**. Audit functions should be modified to monitor all energy data access.
- **Establish law enforcement request policies and procedures**. Organizations accessing, storing, or processing energy data should include specific documented incident response procedures for incidents involving energy data.
- **Provide notification for the personal information collected**. Any organization collecting energy data from or about consumers should establish a process to notify consumer account inhabitants and person(s) paying the bills (which may be different entities), when appropriate, of the data being collected, why it is necessary to collect the data, and the intended use, retention, and sharing of the data. This notification should include information about when and how information may or may not be shared with law enforcement officials. Individuals should be notified before the time of collection.
- **Provide notification for new information use purposes and collection**. Organizations should update consumer notifications whenever they want to start using existing collected data for materially different purposes other than those the consumer has previously authorized. Also, organizations should notify the recipients of services whenever they want to start collecting additional data beyond that already being collected, along with providing a clear explanation for why the additional data is necessary.
- **Provide notification about choices**. The consumer notification should include a clearly worded description to the recipients of services notifying them of (1) any choices available to them about information being collected and obtaining explicit consent when possible; and (2) explaining when and why data items are or may be collected and used without obtaining consent, such as when certain pieces of information are needed to restore service in a timely fashion.
- **Limit the collection** of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.

- **Obtain the data** by lawful and fair means and, where appropriate and possible, with the knowledge or consent of the data subject.
- **Review privacy policies and procedures**. Every organization with access to Smart Grid data should review existing information security and privacy policies to determine how they may need to be modified. This review should include privacy policies already in place in other industries, such as financial and healthcare, which could provide a model for the Smart Grid.
- **Limit information retention**. Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfill the purposes that have been communicated to the energy consumers. When no longer necessary, consistent with data retention and destruction requirements, the data and information, in all forms, should be irreversibly destroyed. This becomes more important as energy data becomes more granular, more refined, and has more potential for commercial uses.
- **Consumer access**. Any organization possessing energy data about consumers should provide a process to allow consumers access to the corresponding energy data for their utilities account.
- **Dispute resolution**. Smart Grid entities should establish documented dispute resolution procedures for energy consumers to follow.
- **Limit information use**. Data on energy or other Smart Grid service activities should be used or disclosed only for the authorized purposes for which it was collected.
- **Disclosure**. Data should be divulged to or shared only with those parties authorized to receive it and with whom the organizations have told the recipients of services it would be shared.
- **Associate energy data with individuals only when and where required**. For example only link equipment data with a location or consumer account when needed for billing, service restoration, or other operational needs. This practice is already common in the utility industry and should be maintained and applied to all entities obtaining or using this data as the Smart Grid is further deployed.
- **De-identify information**. Energy data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymized by removing personal information elements wherever possible to ensure that energy data from specific consumer locations is limited appropriately. This may not be possible for some business activities, such as for billing.
- **Safeguard personal information**. All organizations collecting, processing, or handling energy data and other personal information from or about consumer locations should ensure that all information collected and subsequently created about the recipients of Smart Grid services is appropriately protected in all forms from loss, theft, unauthorized access, disclosure, copying, use, or modification. While this practice is commonly in effect in the utility industry, as other entities recognize commercial uses for this information, they too should adopt appropriate requirements and controls. In addition, given the growing granularity of information from Smart Grid operations, the responsibility for these existing policies should be reviewed and updated as necessary.

- **Do not use personal information for research purposes**. Any organization collecting energy data and other personal information from or about consumer locations should refrain from using actual consumer data for research until it has been anonymized and/or sufficiently aggregated to assure to a reasonable degree the inability to link detailed data to individuals. Current and planned research is being conducted both inside and outside the utility industry on the Smart Grid, its effects upon demand response, and other topics. The use of actual information that can be linked to a consumer in this research increases the risk of inadvertent exposure via traditional information sharing that occurs within the research community.
- **Keep information accurate and complete**. Any organization collecting energy data from or about consumer locations should establish policies and procedures to ensure that the Smart Grid data collected from and subsequently created about recipients of services is accurate, complete, and relevant for the identified purposes for which they were obtained, and that it remains accurate throughout the life of the Smart Grid data within the control of the organization.
- **Policy challenge procedures**. Organizations collecting energy data, and all other entities throughout the Smart Grid, should establish procedures that allow Smart Grid consumers to have the opportunity and process to challenge the organization's compliance with their published privacy policies as well as their actual privacy practices.
- **Perform regular privacy impact assessments**. Any organization collecting energy data from or about consumer locations should perform periodic PIAs with the proper time frames, to be determined by the utility and the appropriate regulator, based upon the associated risks and any recent process changes and/or security incidents. The organizations should consider sending a copy of the PIA results for review by an impartial third party and making the results of the review public. This will help to promote compliance with the organization's privacy obligations and provide an accessible public record to demonstrate the organization's privacy compliance activities. Organizations should also perform a PIA on each new system, network, or Smart Grid application and consider providing a copy of the results in similar fashion to that mentioned above.
- **Establish breach notice practices**. Any organization with Smart Grid data should establish policies and procedures to identify breaches and misuse of Smart Grid data, along with expanding or establishing procedures and plans for notifying the affected individuals in a timely manner with appropriate details about the breach. This becomes particularly important with new possible transmissions of billing information between utilities and other information between utilities and other entities providing services in a Smart Grid environment (e.g., third-party service providers).

4. CONCLUSIONS

This document is the first (public) version of deliverable D24.1 “ICT functional architecture and specifications” which is the outcome of FABRIC WP24 entitled “Architecture and system specifications”. The second (confidential) version of the deliverable will be available on M15 (March 2015) which is when the WP24 ends and it will also contain the detailed system specifications, complementing the information provided here.

The present document includes the results of T2.4.1 “Architecture definition” and T2.4.3 “Data security and privacy”. It comprises two parts: the first one defines the functional architecture of FABRIC or a feasible FABRIC-like system that can be implemented in the future. This approach is followed because FABRIC is a feasibility research project and the architecture definition should consider probable implementations that go beyond the strict boundaries of the system that will be developed and tested in FABRIC project. In that way, infrastructure booking, routing and billing have been considered although these are not foreseen to be tested at the project test sites. In addition alternative implementation architectures for some functionalities (such as accounting and energy tariff specification) were briefly discussed and the proposed architecture is open enough to allow freedom during the development and the commercial implementation. In those cases specific architectural components (such as the algorithm that will calculate the final charging cost) may be defined by the business model during actual commercial system deployment.

To define the functional elements that form the whole system, initially the use cases and user requirements in terms of functionality were analysed and translated into UML sequence diagrams that depict the information flow among the main subsystems identified in [1] and [2]. The information flow provides the means to analyse in more detail which components are necessary to realize the functional requirements. The physical components will be defined based on the work of WP23 (technical benchmarking) and WP42 (Technical feasibility of ICT and charging solutions) and developed in WP25 (Design of ICT applications and development of components). Future work in FABRIC SP2, 3 and 4 should therefore take account of this deliverable and follow the proposed architecture; or consult with the authors of this deliverable if any deviation to this architecture is considered desirable or justifiable.

In order to contribute towards interoperability with the various charging systems currently under research and development, effort has been put to create synergies with other electromobility projects through common partners and mainly with eCo-FEV project. Eco-FEV’s research and development objective is the creation of the ICT infrastructure to enable seamless EV charging which also covers dynamic charging to some extent. By exploiting already available knowledge and ICT development, adapting and extending it where necessary FABRIC avoids reinventing the wheel and helps towards the definition of a standardized and modular ICT architecture for electromobility.

The second area covered in this document relates to user data privacy and system security. The threats that a system such as FABRIC will face do not differ greatly from the ones for ITS in general. The user identity, the EV location and sensitive data such as billing and personal information should be stored, handled and transmitted securely throughout the system. In addition system availability and data reliability should be ensured to avoid attacks aimed at the infrastructure which could also compromise the grid security. Attacks that are specific to the FABRIC system, such as identity theft in order to avoid payment or charging someone else, OBU

hacking to provide false information for the same reasons, malicious attacks aiming at reducing the system efficiency etc are just “application scenarios” that can be addressed if the root vulnerabilities are addressed and this is being done in many European projects that focus primarily to the security aspects of ICT systems and ITS. FABRIC is not focused on ITS security thus in this deliverable the user privacy and data security requirements are analysed and directions are given to developers on where to look for specialized security solutions that are available in the market as products, standards, APIs or still in research and development phase.

5. REFERENCES

[1] FABRIC IP Deliverable D43.1 “FABRIC final use cases”.
[2] FABRIC IP Deliverable D22.1 “User needs, system concept and requirements for ICT solutions”.
[3] FABRIC IP Deliverable D33.1 “Review of existing solutions”.
[4] eCo-FEV project website: http://www.eco-fev.eu.
[5] FABRIC IP Deliverable D32.1 “Technical and user requirements”.
[6] NIST IR 7628 “Guidelines for Smart Grid Cyber Security”, September 2010.
[7] ETSI EN 302 665 V1.1.1：Intelligent Transport Systems (ITS); Communications Architecture.
[8] www.openstreetmap.org/
[9] ETSI TS 102 636-4-1 V1.1.1 (2011-06) Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality.
[10] http://www.w3.org/2002/ws/, 3WC, Web Services Activity.
[11] ETSI TS 101 556-1 V1.1.1 (2012-07) Intelligent Transport Systems (ITS); Infrastructure to Vehicle Communication; Electric Vehicle Charging Spot Notification Specification.
[12] ETSI TS 102 636-5-1 V1.1.1 (2011-02), Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol.
[13] ETSI ES 202 663 V1.1.0: 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.
[14] Mobility 2.0 project website http://mobility2.eu/