



# I.ICT-2011-285135 FINSENY

## D1.11 version 1.0

## *Security Elements for the FINSENY Functional Architecture*

**Contractual Date of Delivery to the CEC:** *March 30th, 2013*

**Actual Date of Delivery to the CEC:** *March 30th, 2013*

**Author(s):** Lionel Besson, Steffen Fries, Andreas Furch, Henryka Jormakka, Fabienne Waidelich, Maria Martin-De-Vidales-Ramirez

**Participant(s):** Siemens AG, Thales, VTT, Atos Research & Innovation

**Workpackage:** WP1, Task 1.6 Security

**Estimated person months:** (resources spent on the deliverable)

**Security:** PU

**Nature:** **R**

**Version:** 1.0

**Total number of pages:** 134

Abstract:

Deliverable D1.11 presents all FINSENY security elements, especially including the energy domain specific security elements needed for the FINSENY scenarios. These are described as enablers, constraints, general elements countermeasures, or controls. Scenario specific security elements needed for FINSENY are also analyzed. It represents a direct continuation of deliverable D1.10 [181] and therefore fully includes its structure and content.

Keyword list:

Threat and risk analysis, security, risk assessment, interfaces, security requirements, scenario, use case, system analysis, authentication, authorization, privacy, confidentiality, trust domain, availability, reliability, functional architecture, security enablers, security standards, security elements, FINSENY, FI-WARE

Disclaimer:

*Not applicable.*

# Executive Summary

D1.11, titled “Security Elements for the FINSENY Functional Architecture” is a direct continuation of deliverable D1.10 [181] and therefore fully includes the structure and contents of it. D1.11 is thus as well based upon a threat and risk analysis which led to the definition of a set of security requirements that can be applied to all scenario work packages and a scenario specific security requirement. All FINSENY security requirements that are shortly repeated in chapter 3 of this deliverable justify the reason of defining a set of security elements that are described as enablers, constraints, general elements, countermeasures, or controls in chapters 4 and 5. In particular, chapter 5.2 explicitly states which security requirements are supported or met by which security control. Chapter 6 of this deliverable then takes a closer look at some of the energy scenario specific security elements needed for FINSENY. Chapter 7 finally shows an example of how the functional architectures of the FINSENY scenario work packages 2 to 6 may be extended by the security elements. This example is based upon the SGAM framework which is used by the scenario work packages as well.

**Assessment & Assessment Scope**

As IR 1.4 has been built upon the use cases of all FINSENY scenario work packages (WP2 to WP6) to derive its set of security requirements, deliverable D1.11 implicitly incorporates all these use cases as well. The following list shows the scenarios that have been analyzed within FINSENY work packages 2 to 6:

- Distribution network (WP2)
- Microgrid (WP3)
- Smart Buildings (WP4)
- Electric Mobility (WP5)
- Electronic Market Place for Energy (WP6)

**Findings**

As already mentioned, the main findings of the deliverable are the security elements that may be integrated into the FINSENY functional architecture as well as the domain specific considerations regarding selected security services needed for the FINSENY scenarios. Apart from this, deliverable D1.11 also explicitly considers usage of generic security enablers from the FI-WARE project as well as relevant security standards and constraints from a privacy perspective that should be taken into account for the security architecture.

**Recommendations**

Deliverable D1.11 presents all FINSENY security elements, especially including the energy domain specific security elements needed for the FINSENY scenarios. It is recommended to use the FI-WARE generic security enablers as described in the document and to take the domain specific security considerations into account as well when realizing testbeds within phase 2 of the project.

# Authors


| Partner | Name | Phone / Fax / e-mail |
|---|---|---|
| **Siemens AG** | **Steffen Fries** | |
| | | Phone: +49 89 636 53403 |
| | | Fax: +49 89 636 48000 |
| | | E-mail: steffen.fries@siemens.com |
| **Siemens AG** | **Andreas Furch** | |
| | | Phone: +49 89 636 56837 |
| | | Fax: +49 89 636 48000 |
| | | E-mail: andreas.furch@siemens.com |
| **Siemens AG** | **Fabienne Waidelich** | |
| | | Phone: +49 89 636 42735 |
| | | Fax: +49 89 636 48000 |
| | | E-mail: fabienne.waidelich@siemens.com |
| **Thales** | **Lionel Besson** | |
| | | Phone: +33 1 46 13 24 90 |
| | | Fax: +33 1 46 13 26 86 |
| | | E-mail: Lionel.BESSON@thalesgroup.com |
| **VTT** | **Henryka Jormakka** | |
| | | Phone: +358 40 511 6275 |
| | | E-mail: Henryka.Jormakka@vtt.fi |
| **Atos Research & Innovation** | **Maria Martin-De-Vidales-Ramirez** | |
| | | Phone: +34 91 214 9057 |
| | | E-mail: maria.martin-de-vidales-ramirez@atosresearch.eu |

# Table of Contents

# Table of Figures

## Table of Tables



## List of Abbreviations

| **Abbreviation** | **Definition** |
|---|---|
| A&A | Authentication and Authorization (Access Control) |
| APDU | Application Protocol Data Unit |
| API | Application Programming Interface |
| BAN | Building Area Network |
| BCP | Business Continuity Plan |
| BDSG | Bundesdatenschutzgesetz/German Data Protection Act |
| BES | Bulk Electric System |
| CGA | Cryptographically Generated Address |
| CIM | Common Information Model |
| CoAP | Constrained Application Protocol |
| CUC | Control Use Case |
| DB | Database |
| DCC | Data and Communications Company (UK) |
| DER | Distributed Energy Resources |
| DMS | Distribution Management System |
| DMZ | Demilitarized Zone |
| DNO | Distribution Network Operator |
| DNS | Domain Name Service |
| DNS-SD | DNS Service Discovery |
| DNSSEC | Domain Name System Security Extensions |
| DPA | Data Protection Act (UK) |
| DPIA | Data Protection Impact Assessment |
| DSA | Digital Signature Algorithm |
| DSO | Distribution System Operator |
| DTLS | Datagram Transport Layer Security |
| ECC | Elliptic Curve Cryptography |
| ECHR | European Convention on Human Rights |

| | |
|---|---|
| eID | Electronic Identity |
| eMarket4E | Electronic Market for Energy |
| ERGER | European Regulators Group for Electricity and Gas |
| ESCO | Energy Service Company |
| EV | Electric Vehicle |
| EVSE | Electric Vehicle Supply Equipment |
| FAN | Field Area Network |
| FERC | Federal Energy Regulatory Commission |
| FEV | Full Electric Vehicle |
| FoIA | Freedom of Information Act (UK) |
| FoISA | Freedom of Information Scotland Act |
| GCP | Global Customer Platform (Deutsche Telekom AG) |
| GE | Generic Enabler |
| GID | Generic Interface Definition |
| HAN | Home Area Network |
| GUI | Graphical User Interface |
| HIP | Host Identity Protocol |
| HRA | Human Rights Act (UK) |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | HTTP Secure |
| HW | Hardware |
| IAM | Identity and Access Management |
| ICS | Industrial Control System |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| IPsec | Internet Protocol Security |
| IS | Information Security |
| ISO | International Standardization Organization |
| ITIL | Information Technology Infrastructure Library |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Message Authentication Code |
| MGCC | Microgrid Control Center |
| NDP | Neighbour Discovery Protocol |
| NAT | Network Address Translation |
| NIST | National Institute of Standards and Technology |
| OCTAVE | Operationally Critical Threat,Asset, and Vulnerability Evaluation |
| PHEV | Plug-in Hybrid Electric Vehicle |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PPL | Privacy Policy Language |
| PUF | Physical Unclonable Function |
| RBAC | Role Based Access Control |
| RIPA | Regulation of Investigatory Powers Act (UK) |
| RSA | Rivest, Shamir, Adleman, cryptographic algorithm allowing signature and encryption |
| SAML | Security Assertion Markup Language |
| SANS | SysAdmin, Audit, Network, Security |

| | |
|---|---|
| SCADA | Supervisory Control and Data Acquisition |
| SEND | Secure Neighbor Discovery |
| SG | Smart Grid |
| SGAM | Smart Grid Architecture Model (based on the outcome of the European SGCG) |
| SGCG | Smart Grid Coordination Group |
| SGTF | Smart Grid Task Force |
| SKiP | Security Knowledge in Practice method |
| SLA | Service Level Agreement |
| SLP | Service Location Protocol |
| SLPv2 | Service Location Protocol version 2 |
| SM | Smart Meter |
| SMIP | Smart Metering Implementation Programme (UK) |
| SMS | Short Message Service |
| SQL | Structured Query Language (DB access) |
| SSL | Secure Socket Layer (kind of TLS) |
| SSO | Single Sign On |
| SW | Software |
| TCP | Transmission Control Protocol |
| T & R | Threat & Risk (Analysis) |
| TS | Technical Specification |
| TSO | Transmission System Operator |
| TNO | Transmission Network Operator |
| TLS | Transport Layer Security |
| USDL | Unified Service Description Language |
| USDL-SEC | USDL Linked Data Vocabulary for Security |
| V2G | Vehicle to Grid |
| XML | eXtensible Markup Language |

# 1. Introduction

This document builds upon a threat and risk analysis of the FINSENY target use cases conducted in the WP1 Security Task. The goal of this document is the definition of the security architecture elements addressing the threats and security requirements identified by the threat and risk analysis. This is done by providing appropriate countermeasures described in the form of security elements. Especially a first integration of Generic Enablers is being in focus in cooperation with the FI-WARE project. The security architecture elements build the base for the design of a scenario specific security architecture. Note that the security architecture strongly depends on the functional architecture of the underlying use cases. The security elements provided here may be seen as a catalog of security countermeasures targeting the Smart Grid domain.

## 1.1 General target system overview

WP1 security task analyzed the use cases of all FINSENY scenario work packages (WP2 to WP6) to derive all of their relevant threats and risk levels that in turn led to a full set of security requirements, listed in section 3. This document (FINSENY deliverable D1.11) addresses all these threats and requirements. Thus D1.11 implicitly incorporates all FINSENY scenarios and their use cases as well. The following lists the scenarios that were analyzed by work packages 2 to 6 together with short motivations used by FINSENY. More detailed information can be found deliverables D2.1 to D6.1 ([186], [187], [188], [174] and [175]).

- Distribution network (WP2)
  Advanced automation, control and management of Distribution Networks is needed to meet the increased use of distributed energy generation.
- Microgrid (WP3)
  Distributed generation supports the establishment of Microgrids aggregating and controlling their own supply and demand side resources.
- Smart Buildings (WP4)
  Efficient energy management in Smart Buildings requires use of communication network infrastructure as well as provision of the necessary interfaces.
- Electric Mobility (WP5)
  Charging points are required from the energy infrastructure, which implies interaction between the energy, transport and communication infrastructures and vehicle information systems.
- Electronic Market Place for Energy – eMarket4E (WP6)
  Smart Energy Grids result in a transformation of the European energy market. New players are appearing and the roles of incumbent players are changing.

## 1.2 Objectives

The scope of this deliverable is a definition of security architecture elements based on the threat and risk analysis. These security architecture elements can be used by the subsequent deliverable Dx.3 to specify the security architecture within the functional architectures originating from the scenario work packages WP2 to WP6.

## 1.3 Interactions with other FINSENY Work Packages

Since the security architecture elements cannot be seen as independent from a specific use case or from dedicated security requirements, D1.11 has a relation to different documents. It is assumed that most of the security measures will not be use case specific in terms of the applied technology. The technology is rather expected to be domain specific (resulting in a domain specific enablers described in this document) or general (resulting in the application of FI-WARE Generic Enablers). The security measures needed in the different WP specific functional architectures will use security architecture elements defined in D1.11. The following figure shows the different definitions in the context of certificates, derived from the threat and risk analysis. As shown, it is necessary to define the context of a certificate, which is use case specific. As certificates are used in merely all use cases, the underlying protocols for utilizing these

certificates are outlined in D1.11, while the general infrastructure for certificate provisioning is provided in FI-WARE.

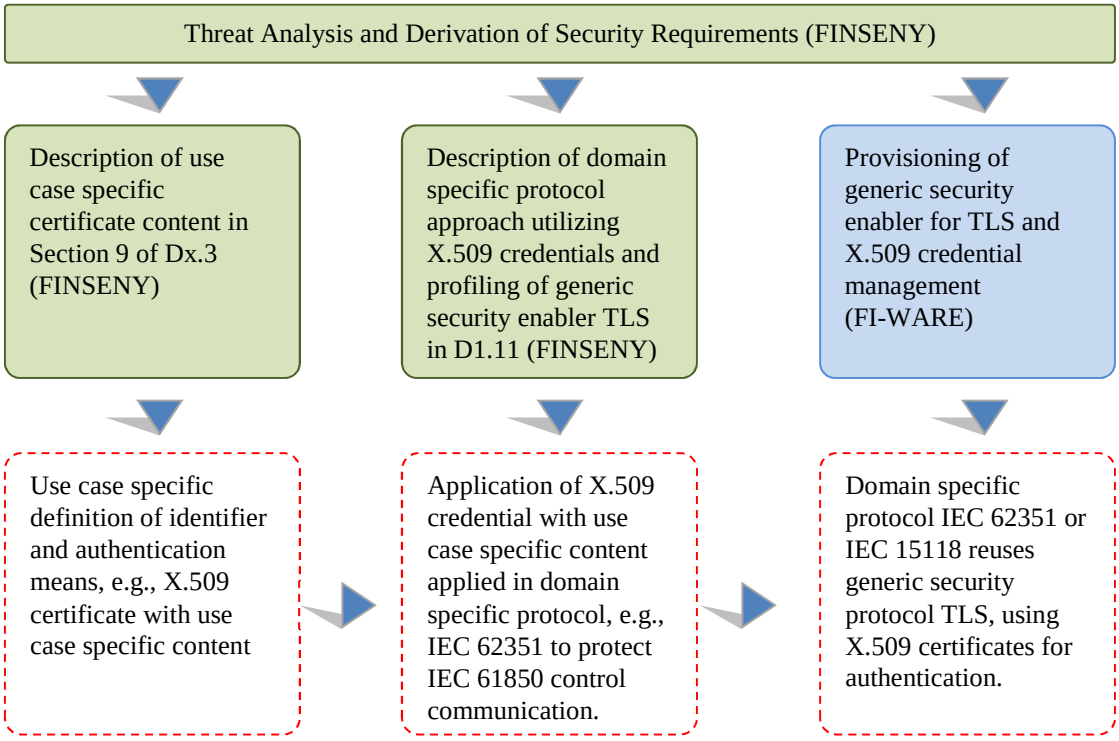


**Figure 1: Interdependency of FINSENY documents**

As seen in the figure above, WP specific security, security architecture elements from D1.11 and the generic enabler from FI-WARE in conjunction provide to the use case specific security solution.

## 1.4 Document structure

The document is structured in the following way:

- Chapter 1, “Introduction”, gives a short overview of the document together with important hints.
- Chapter 2, “Overview of Target System Functional Architectures”, summarizes information about the functional architectures of the FINSENY scenario specific work packages. Additionally an overview of applicable technical communication standards used within the scenarios is given.
- Chapter 3, “Security Requirements”, shortly summarizes the security requirements found by the FINSENY threat and risk analysis. They determine the set of security elements that are described in the following chapters.
- Chapter 4, “Existing Security Enablers and Constraints”, describes generic security enablers that can be used from the FI-WARE project as well as relevant security standards and constraints from a privacy perspective that should be taken into account for the security architecture. Security elements from a general perspective are handled as well.
- Chapter 5, “Security Countermeasures”, concludes the main chapters by showing a list of security countermeasures and controls that can be used to support or meet the security requirements. An analysis which security requirements are supported or met by which security control is also included.
- Chapter 6, “Security Architecture Elements”, then takes a closer look at some of the energy scenario specific security elements needed for FINSENY.

- Chapter7, “FINSENY Functional Architecture including Security” finally shows an example of how the functional architectures of the FINSENY scenario work packages 2 to 6 may be extended by the security elements.
- The document closes with a conclusion in chapter 8 and a list of references in chapter 9.

# 2. Overview of Target System Functional Architectures

In the following sections, we give an overview of the functional architectures of the different scenario work packages (WP2-6). The information is extracted from the DX.3 deliverables ([184], [185], [183], [182] and [180]), and addresses the following scenarios:

- Distribution network,
- Microgrid,
- Smart buildings,
- Electric mobility, and
- Electronic market place for energy.

In order to better understand these scenarios as part of the overall picture and to identify the interfaces between the work packages, the Functional Architecture task leaders of scenario work packages WP2-6 joined the FINSENY architecture group and derived the FINSENY high-level picture which is depicted in Figure 2.

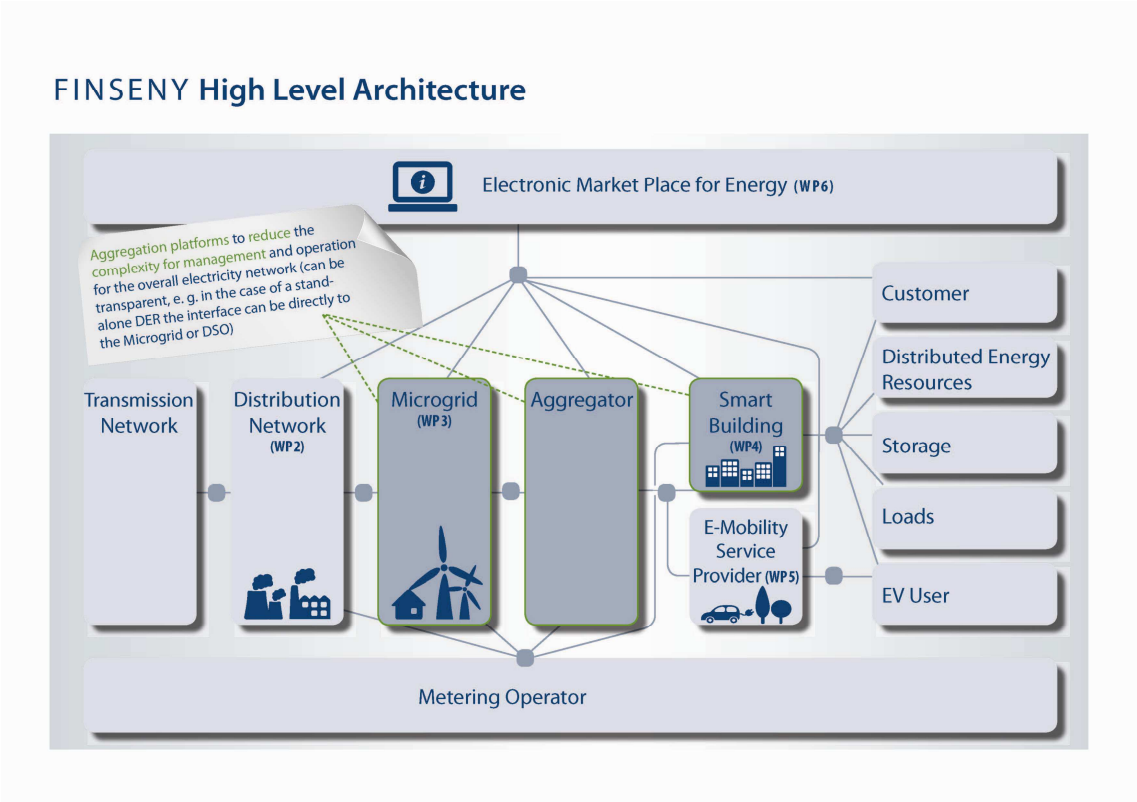


**Figure 2: High level view of FINSENY functional architecture**

The FINSENY high-level picture shows part of the electrical energy conversion chain ranging from the Transmission network, Distribution Network, Microgrid, Aggregator, Smart Building or E-Mobility Service Provider to the customers and their appliances (DERs, Storage, Loads or EVs). From a business perspective the interaction between the various stakeholders takes place on the Electronic Market for Energy.

We address the WP-specific functional architecture in the following subsections.

## 2.1 Distribution Network (WP2) functional architecture

The building blocks identified in all of the WP2 use cases grouped according to SGAM architecture are shown in Figure 3. The component infrastructure presented in the figure gives an overall view of the interconnections of all components and actors in the distribution system, while the identified five communication network clouds (denoted as “Comm. Networks”) are needed for information exchange

enabling monitoring, control and operation purposes. The critical communication requirements for different actors and their actions depend on the functionality of the actions and are presented in [184].

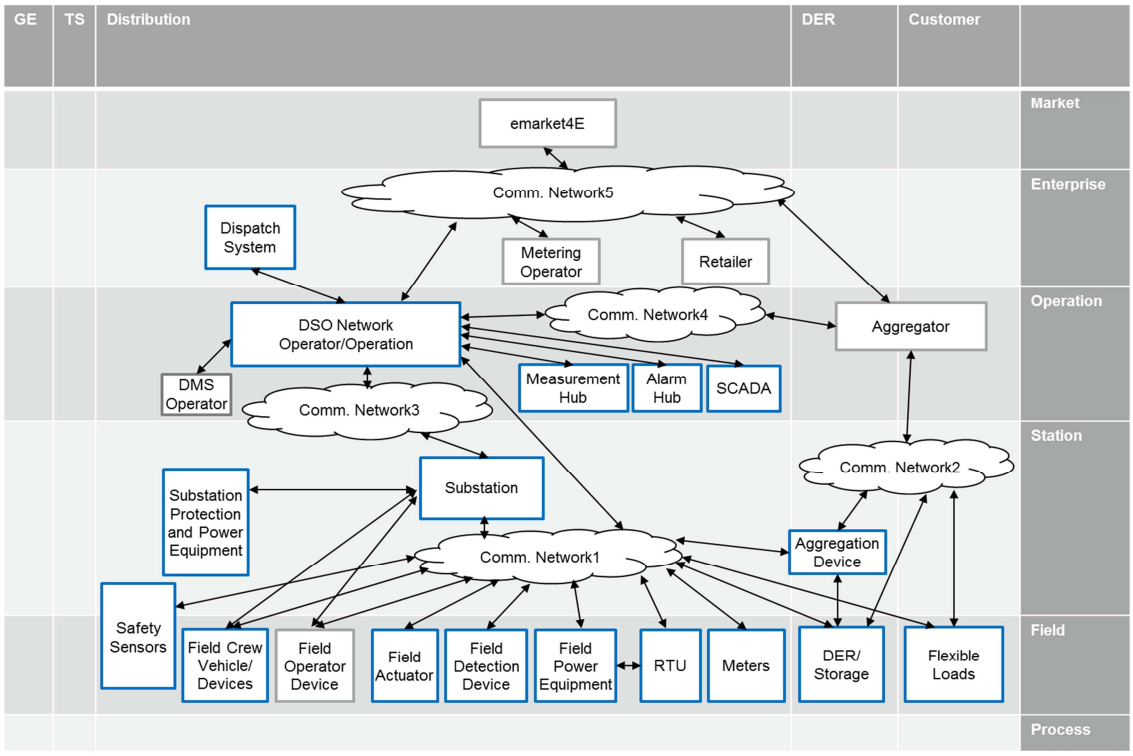


**Figure 3: Component infrastructure for the distribution system**

## 2.2 Microgrid (WP3) functional architecture overview

WP3 applied a thorough analysis to a selection of ICT-prone Control Use Cases from deliverable D3.1, following the SGAM methodology.

The following figure is an example of the drill down process applied to auto configuration CUC.

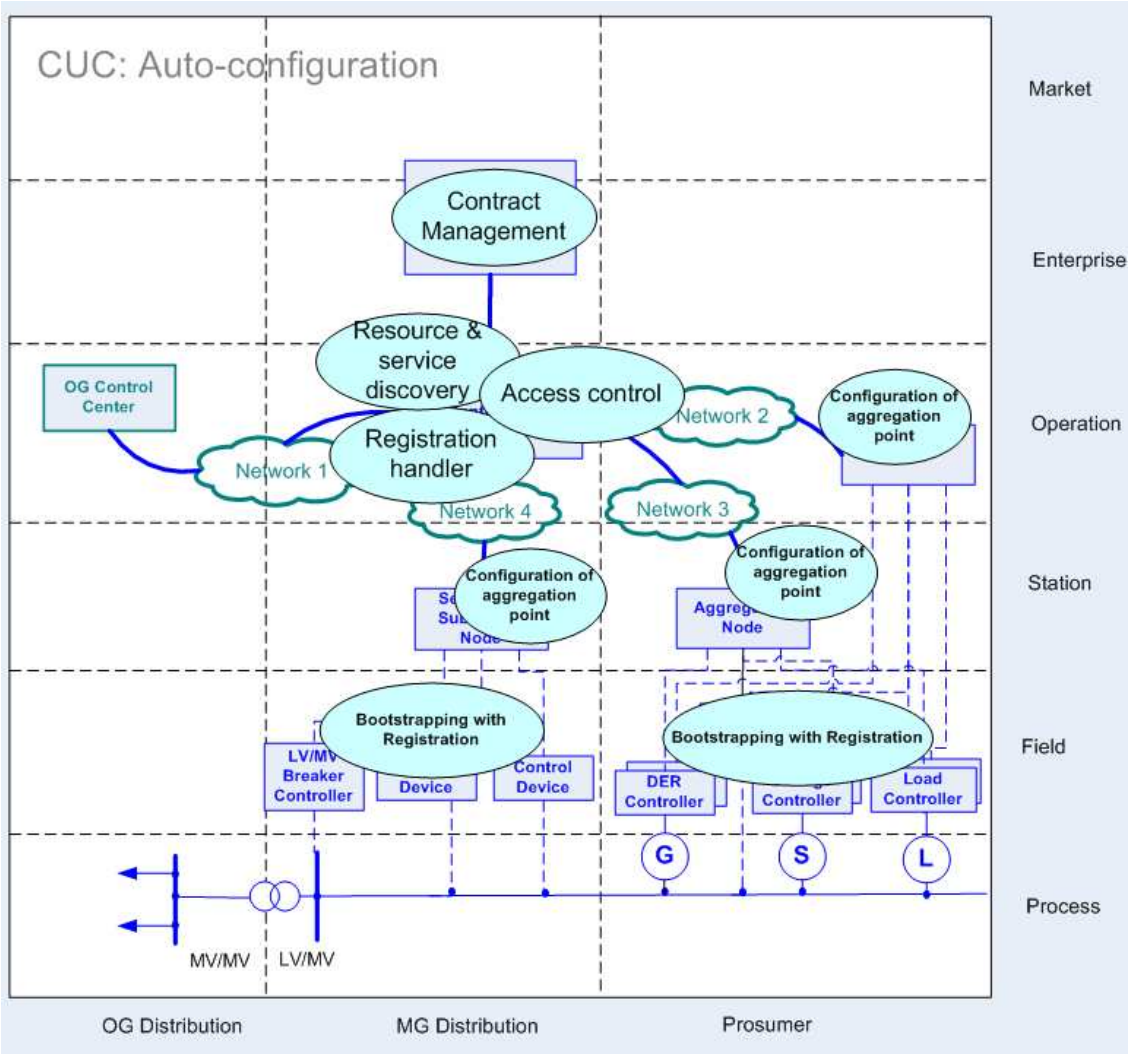


**Figure 4: Auto-configuration CUC drill down process**

Based on this drill down process and the harmonization of the functional layer of the different use cases, the functional architecture of the Microgrid Control Center was derived.

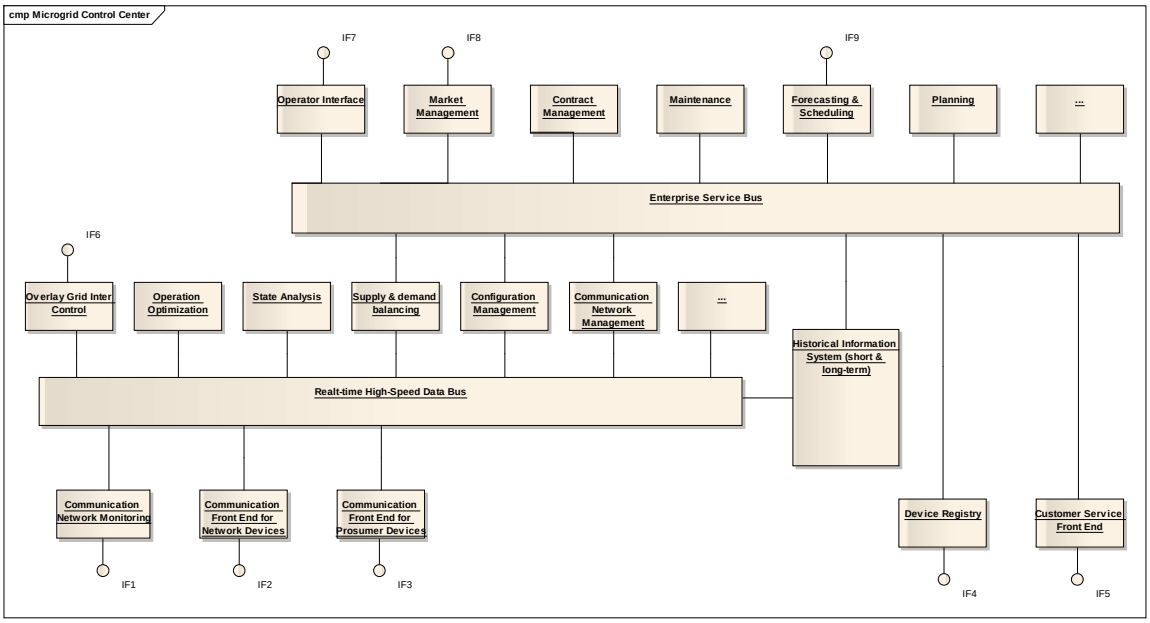


**Figure 5: Microgrid Control Center functional architecture (Building blocks and interfaces)**

20 functional components have been identified, as well as 9 interfaces to external components (noted IF1 to IF9). These interfaces connect devices from the station level to the MGCC, but also with other control centers, operators, service providers and other market roles.

## 2.3 Smart Buildings (WP4) functional architecture overview

WP4 performed a SGAM drill-down process of Smart Building use cases. Five topologies where taken into account, representing the home domain, residential domain, office/public building, data centre and hotels domains.

The overall matching of the Smart Building functional architecture to SGAM framework can be seen in Figure 6. It is organized in four separate layers: application layer, shared services layer, building abstraction layer and devices layer.

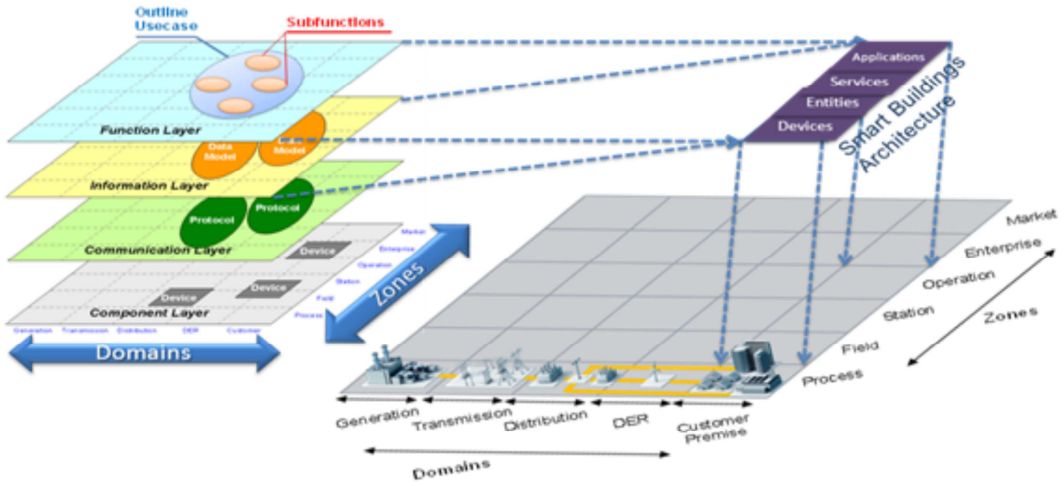


**Figure 6: WP4 matching of architecture to SGAM framework**

A more detailed decomposition of the architecture is presented in the following Figure 7: the main building blocks of the architecture are represented through examples of their instances and example instances of their mutual relationship.

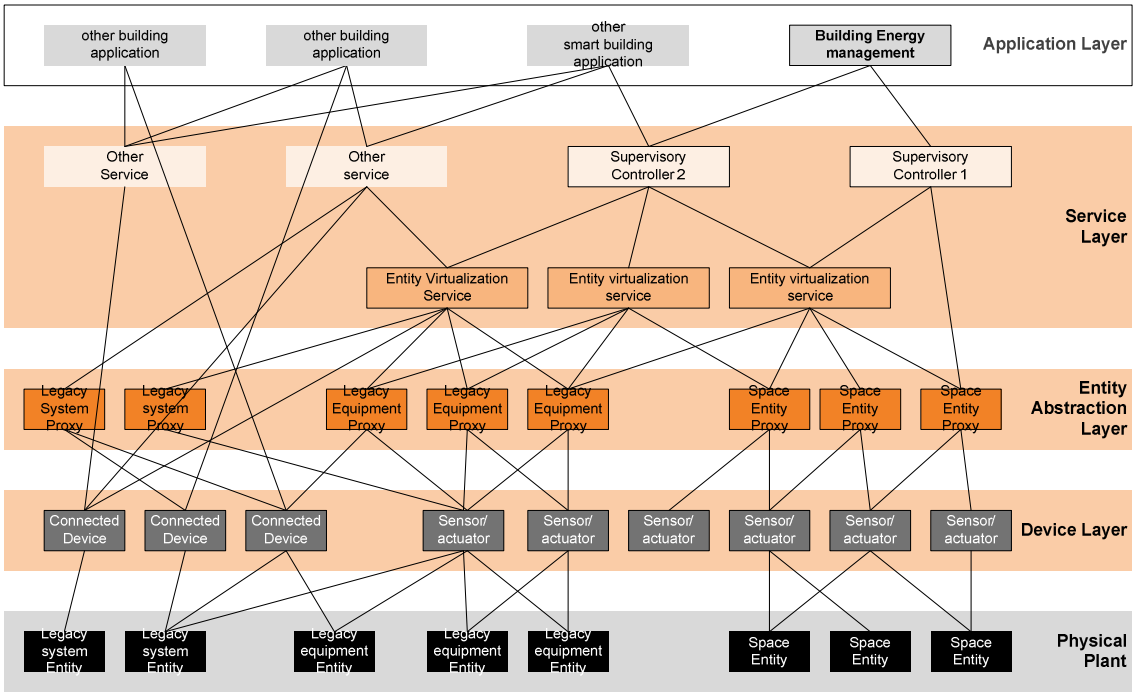


**Figure 7 : Generic functional building blocks of FINSENY Smart Building Architecture**

A more detailed view of the main high-level building blocks of the Smart Building architecture depicted above can be found in D4.3 [183].

## 2.4 Electric Mobility (WP5) - functional architecture overview

Electric Mobility addresses the incorporation of electric vehicles into the Smart Grid. This covers on one hand the usage of the electric vehicle as load but also as energy storage facility to feed back energy, when needed and possible. It also addresses the incorporation of renewable energy sources into the vehicle charging landscape. Using the electric vehicle besides its mobility feature as a dynamic and controllable energy load and energy source allows for a smooth integration into the Smart Grid.

WP5 has decided to reduce the number of use cases that are taken into account by the functional architecture. The remaining three use cases in scope comprise:

- ICT Enabled Demand Side Management,
- E-Roaming,
- V2G.

These use cases are further described in the deliverable D5.3 [182] and are also in the focus for the definition of trial candidates. The following figure from D5.3 shows the component layer according to SGAM which serves as a base for the above mentioned use cases:

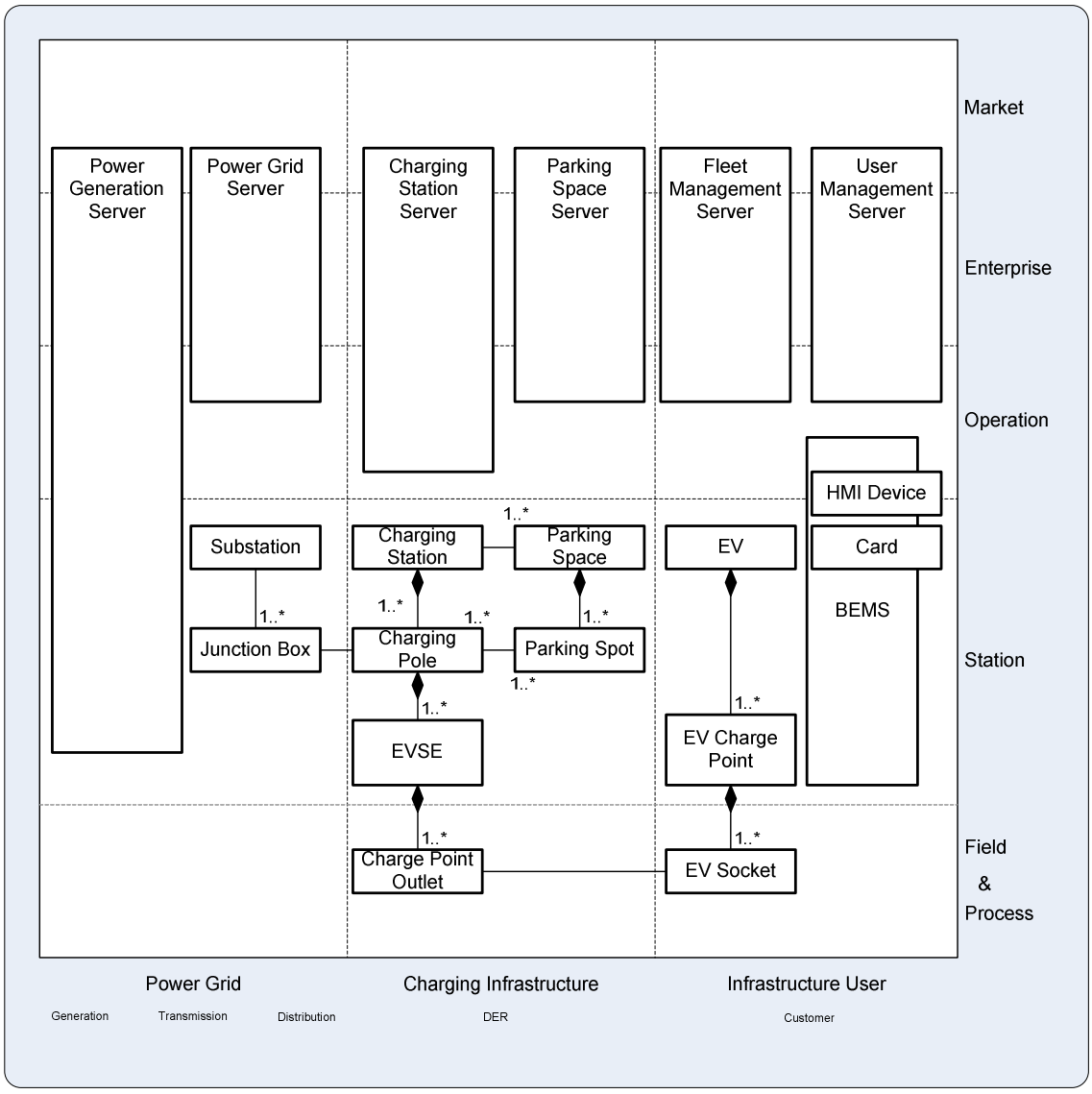


**Figure 8: Component Layer for the WP 5 use cases**

The following subsections provide an overview about the three use cases. Note that the current description of the deliverable for the functional architecture uses the SGAM model. Hence, the overview given here also concentrates on this mapping.

Note that the information about the different use cases has been summarized from the document describing the functional architecture for Electric Mobility in deliverable D5.3 [182].

### 2.4.1 ICT enabled demand side management

This use case describes a real use case trial addressing the management of electric vehicle charging systems. The trial is currently being developed as part of the FINESCE project, which is proposed for Phase II of the FI-PPP. Here, the focus is placed on the integration of renewable energy like wind power or solar power into the electric vehicle charging system. On the other hand the vehicle as dynamic load is addressed. Especially the possibility to use the renewable energy for charging electric vehicles is focussed.

Based on SGAM, the architecture has been defined on a rough component level as shown above as well as on a conceptual level as shown below (taken from deliverable D5.3 [182]).

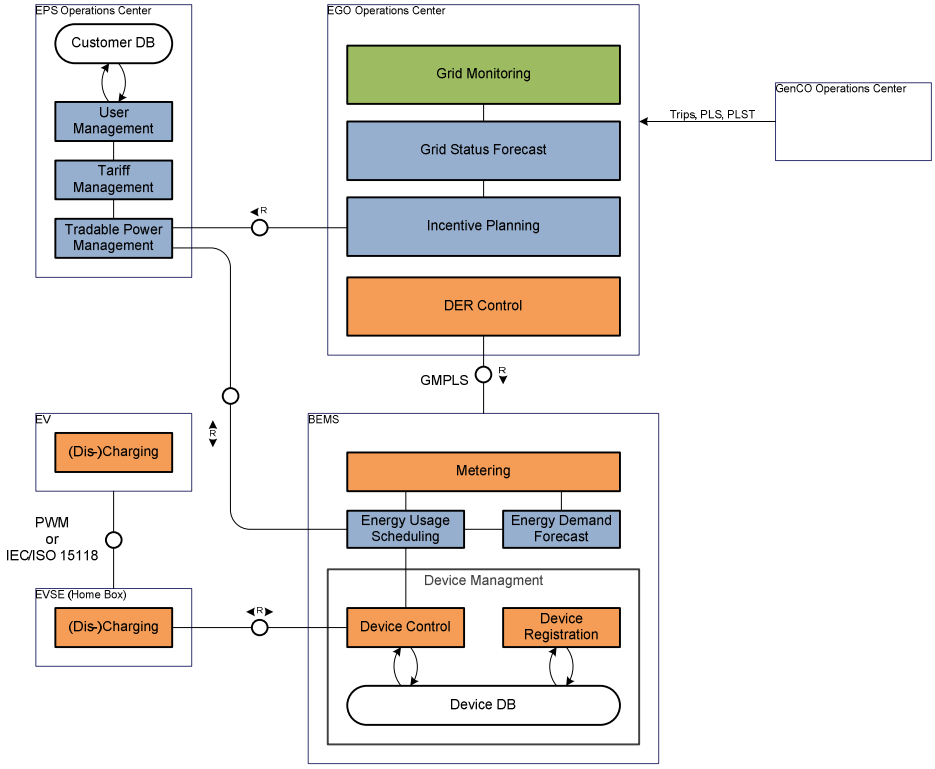


**Figure 9: ICT-Enabled Demand Side Management – Conceptual Architecture Modelling**

The figure above shows the basic functional architecture including main components and protocols on a conceptual level. Note that specific protocols like ISO15118 will be discussed later in the document.

### 2.4.2 E-Roaming

The second use case describes roaming in a similar view as the commonly known roaming for mobile phones. In contrast to roaming of mobile devices here the focus is placed on the energy provider (or mobility provider), who is in charge of providing the energy. This may be especially interesting in scenarios addressing car sharing or renting cars. Besides that, there is interest also for the private environment, i.e., if a car owner has a contract with a dedicated mobility provider, but wants to charge his electric vehicle at a charging point of a different mobility provider.

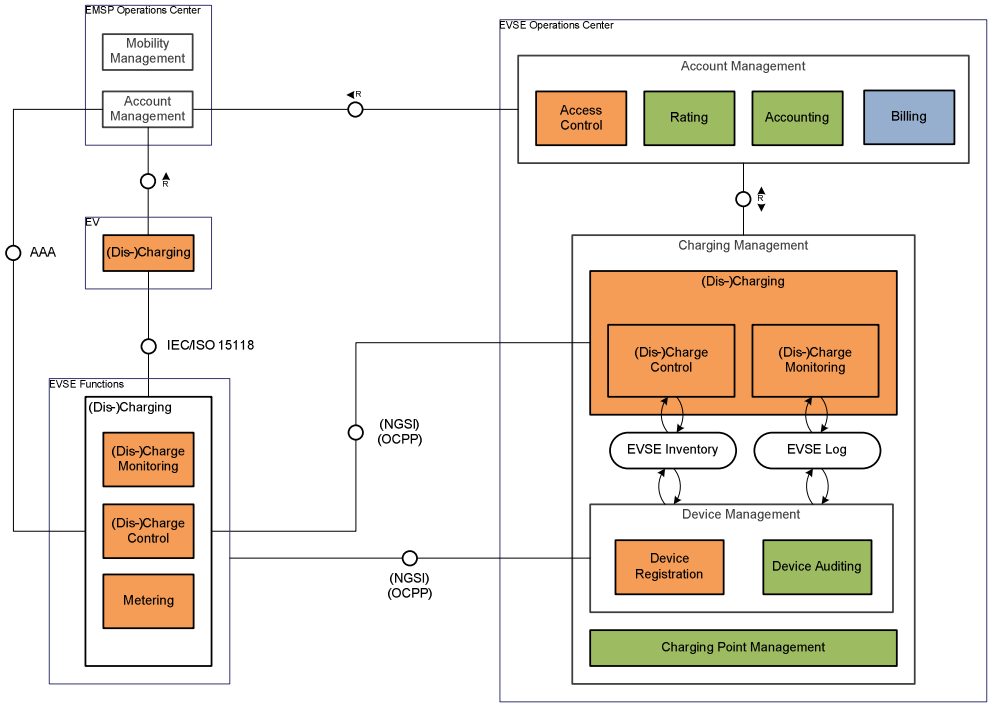


**Figure 10: E-Mobility conceptual architecture**

As in the mobile device case, there is a strong relation to services like authentication, authorization, and accounting. These services enable the clearing of energy transmissions and also the clearing for the connected payment for consumed energy. There are different platforms currently in preparation to enable a roaming platform for vehicle charging. To enable roaming between different mobility providers a unique identifier is seen as helpful. The focus of a potential trial relates therefore to the investigation of this roaming approach and the underlying business models and also potential technical realization options.

### 2.4.3 V2G

As outlined in deliverable D5.3 [182], tthe V2G use case investigates deeper in future application of electrical vehicles with the focus especially on the batteries in electric vehicles to support the power grid, e.g., by using them as variable energy storage. This approach has to consider different factors like grid frequency stability and voltage stability. The latter may be seen as a local issue, which ought to lead to a higher distribution grid penetration. Without control strategies EVs can be seen only as loads for the Smart Grid while V2G enables a bidirectional power flow by incorporating the electric vehicles as controllable loads as well as storage devices which can feed back power into the grid. Figure 11 shows the functional architecture based on SGAM (taken from D5.3 [182]).

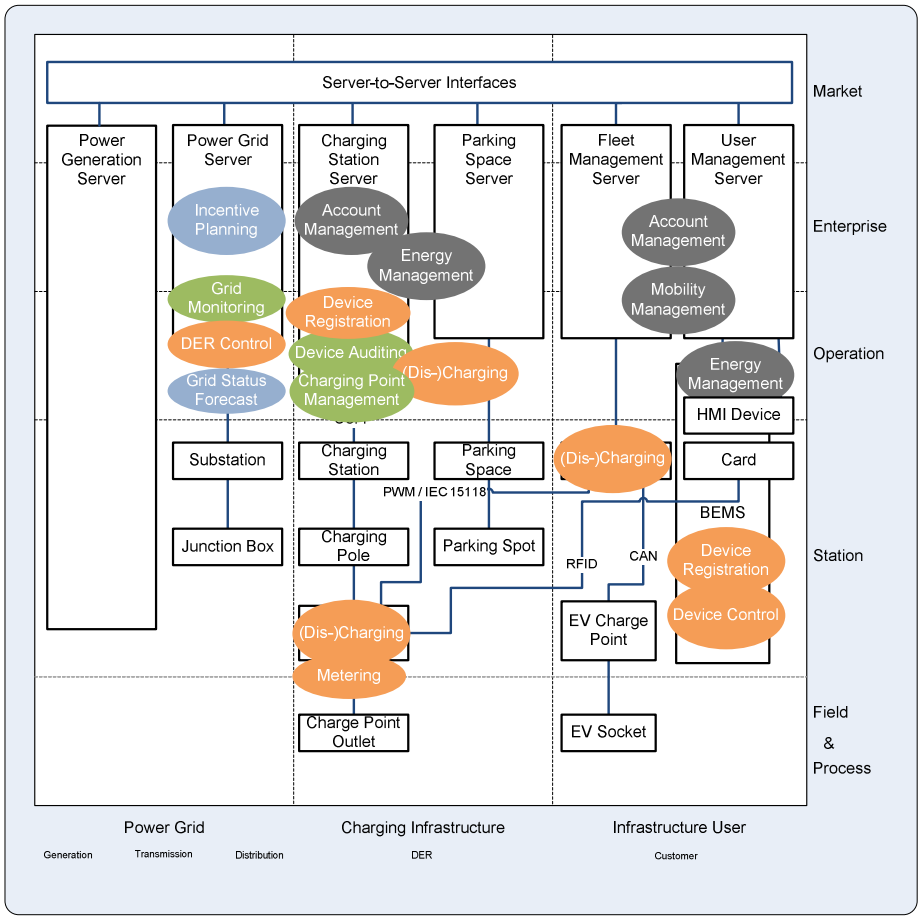


**Figure 11: V2G mapping to SGAM**

The V2G use case may be one way to support stabilization in the distribution network. Vehicles implementing V2G functionality can provide power to help balance loads by valley filling or peak shaving on a local scope. A potential trial may address macro as well as micro scenarios. The micro scenarios may be demonstrated by using a single EV supporting power consumption and feedback in conjunction with an EVSE including a power inverter. From a macro perspective this it may be investigated, how an arbitrary number of such enhanced electric vehicles can be used as a virtual power plant or a virtual electricity storage cloud.

## 2.5 Electronic marketplace for Energy (WP6) functional architecture overview

Concerning the WP6 functional architecture that describes the future electronic market place for energy (eMarket4E), the overviews as shown in Figure 12 and Figure 13 have been used by the work package (cf. [180]).

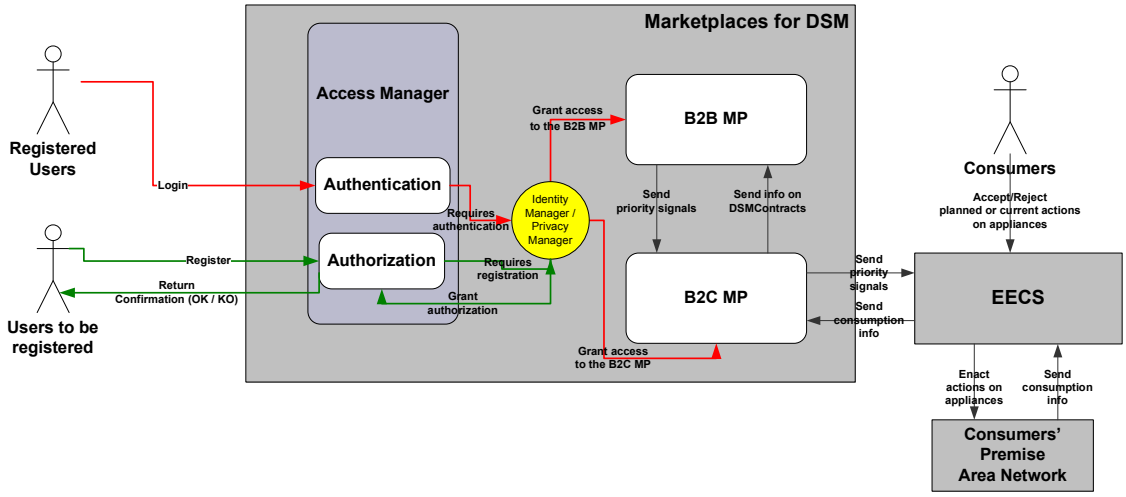


**Figure 12: "Marketplaces for Demand Side Management" high level functional architecture**

Additionally, the following purely security relevant information about the WP6 functional architecture is available from WP6 Functional Architecture task documents:

- HTTPS (on IPv6) is seen as an important building block of the SGAM communication layer (cf. [179]).
- "Authentication and access control" as well as "Data integrity at the Market Place" are seen as important (cf. [179]).
- Privacy of contract is needed (cf. [179]).

All of these issues are handled by the following chapters of this document.

Deliverable D6.3 [180] of WP6 details the functional architecture of the "Marketplaces for Demand Side Management" (see Figure 13 for an overview) which represents the trial candidate for experimentation identified within WP6. Section 9 of D6.3 [180] contains the work package specific security considerations that have been found out during a joint work between WP1 security task team and WP6 and whilst it references this deliverable for security elements that are not WP6 specific. Please note that this deliverable nevertheless contains a discussion of security elements regarding transaction security that have been identified as a WP6 specific security requirement.

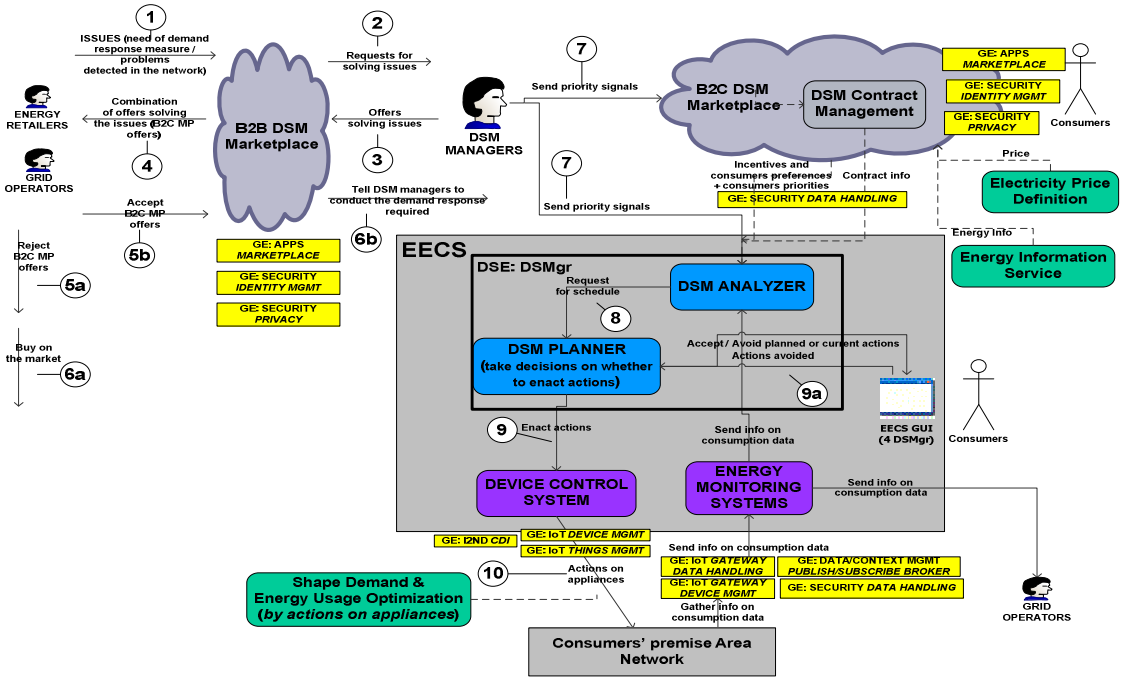


**Figure 13: Marketplaces for Demand Side Management - High Level Architecture**

## 2.6 Applicable technical communication standards

This section contains technical communication standards, which are likely to be used throughout all the scenario use cases or have already been identified in the Dx.3 deliverables. As some of the standards already provide security means, the security options of these standards have to be considered for the definition of functional security in terms of verification about effectiveness and applicability in the FINSENY scenario use cases.

- ISO/IEC 15118 – Road vehicles - Communication protocol between electric vehicle and grid. Its main focus is the electric vehicle to charging spot interface. Communication with the backend infrastructure is not directly targeted. Security is already part of the standard. Note that the standard is in development and is not fully adopted, yet;
- IEC 60870-5-104 – Tele-control standard for reliable data acquisition and control over TCP/IP networks between SCADA masters and substations;
- IEC 61850 – Power system control standards for communications and data acquisition;
- IEC 61851 – Electric vehicle conductive charging system. IEC 61851 defines a conductive charging system and was standardized in 2001. The standards applies to equipment for charging electric road vehicles at standard AC supply voltages (as per IEC 60038) up to 690 V and at DC voltages up to 1000 V, and for providing electrical power for any additional services on the vehicle if required when connected to the supply network. There is currently work being done on updating certain parts of the specification;
- IEC 61968 – Standards for Distribution Management System (DMS) interfaces for information exchange with other IT systems. These include the distribution management parts of the CIM and XML message standards for information exchange between varieties of business systems, such as asset management, work order management, Geographical Information Systems (GIS), etc.;
- IEC 61970 – Standards to facilitate integration of applications within a control centre, including the interactions with external operations in distribution as well as other external sources/sinks of in-formation needed for real-time operations. These include the generation and transmission parts of the Common Information Model (CIM), the Generic Interface Definition (GID) interface standards, and eXtensible Markup Language (XML) standards for power system model ex-change;
- IEC 62056 (DLMS/COSEM) for meter data and measurements.

# 3. Security Requirements

In the past the energy control systems were isolated due to heterogeneous proprietary networks and security concerns. Now the integration and increasing complexity of the emerging energy systems have caused that the usage of communication networks, open technologies and protocols in control and management of Smart Grids is increasing. The emerging integrated control networks require new IT capabilities and at the same time they are open to external threats typical for any information technology system and industrial control systems. In FINSENY, the security related threats have been identified based on the scenario use cases specified in the project, particularly on the identified information resources and their protection needs. They purely concentrate on the data exchange and assumptions about architectural components. The identified threats are the following:

- information disclosure of stored or transmitted data;
- information modification of stored or transmitted data;
- time manipulation;
- unavailability of the system resources (assets);
- modification of assets;
- repudiation of facts;
- impersonation;
- incomplete mediation;
- disclosure, modification and repudiation of Customer Contract Data and disclosure, modification and repudiation of Customer and Market Negotiation Data (Tariff Data) – Missing binding and missing acknowledgement of messages within transactions.

The above threats concern most of the IT systems except for the last one that relates to application level logic work flows and especially to the binding of offers and responses in a contractual relationship among the Smart Grid's actors. If an attacker should successfully disclose customer contract or negotiation data, he may use this information for ongoing or later negotiations causing the market or maybe even the grid not to function properly. Also modification or repudiation of such data may result in improper functioning of the market.

To prevent the above threats, a set of system requirements has been identified. Although the requirements of the control system are similar to the requirements of any IT system, their priorities differ. In IT systems data confidentiality and integrity is the main requirement. In control systems the focus is on the human safety followed by protection of the system processes to save from harm the environment and prevent financial losses, so system availability and integrity are the core priorities. Industrial control systems (ICSs) have also different performance and reliability requirements than IT systems. Its response to human and emergency interaction is critical. Furthermore, the goal of efficiency may sometimes conflict with security in the design and operation of ICSs.

The following requirements have been derived from the (WP-specific) analysis of the FINSENY scenarios and use cases:

**Requirement 1: Authentication and authorization.**

System components shall uniquely authenticate users and specific components before establishing a connection. The components shall enforce separation of duties through assigned access authorization. The user privileges should be restricted to only those that are required for each person's role, taking into account emergency cases. This reflects least privileged application.

Handling in emergency situations must be specifically considered, in such a case a user rights override option should be always implemented. This requires appropriate considerations in the general account policy definition as well as consideration of the specific situation (e.g., by using the situational information (emergency) as additional parameter for access control).

**Requirement 2: Data confidentiality.**

It shall be possible to ensure the confidentiality of data by cryptographic mechanisms, unless otherwise protected by alternative physical measures. The latency introduced from the cryptographic mechanism shall not degrade the functionality of the system.

Data confidentiality relates to both, data in transit and locally stored data which needs to be secured appropriately as well.

**Requirement 3: Data integrity.**

It shall be possible to ensure the integrity of data and to verify whether the data has not been tampered with. The latency introduced from the protection mechanism shall not degrade the functionality of the system.

Data integrity relates to both data in transit and locally stored data.

**Requirement 4: Non-repudiation.**

It shall be possible to prevent the sender of information from denying sending it.

**Requirement 5: Data backup and recovery.**

Backups of critical software, applications, and data for all components of the power system should be assured. Backup should be applied to all data and applications needed to replace failed components within a reasonable period of time as required to satisfy regulatory requirements and to restore the system to normal operation. Backups shall be physically separated from the operational components. Synchronization of the backup and operating data must be assured while the securely stored backup should be appropriately accessible for restoration.

**Requirement 6: System protection components.**

The devices deployed in the network shall employ system protection mechanisms.

The up to date protection mechanisms shall be deployed in such a manner as to limit the impact of the attack to a small geographical area prior to detection and eradication.

**Requirement 7: Secure software/firmware updates.**

The system shall ensure software/firmware updates only with integrity protected packages from an authorized source.

**Requirement 8: Secure system design.**

The system design should obey security design guidelines, for instance to restrict the ability of internal or external users to launch denial-of-service attacks against network components. Here, measures from the security requirement system protection components shall be applied.

**Requirement 9: Security management.**

Security management has to consider all involved cryptographic protection means, including key management infrastructure, certificate management, security policies, addressing both, technical and organizational means. The selection should match the protection needs of the information being protected and the protected system operating constraints.

**Requirement 10: Logging and audit.**

Logging processes shall be established on devices having appropriate resources to support monitoring, traceability, and auditing functionality. Logging itself also requires to be protected. Depending of the component providing the logging information this protection may vary from source authentication, integrity protection up to confidentiality, e.g., for privacy related data.

**Requirement 11: Time synchronization.**

Time synchronization keeps timer elements on different components synchronized.

**Requirement 12: Observation of policies & laws.**

All applicable policies of the utility and its major business partners must be observed, as well as the relevant legislation and regulation. Non-compliance may result in banning of the system, which would result in business loss.

**Requirement 13: Transaction security.**

It has to be guaranteed that whole transactions can be securely validated, i.e. that request and response message chains are acknowledged and securely bound together on application layer.

The following table maps the security requirements to the identified threats to show that each threat is adequately covered by security requirements.

| Basic Threat / Security Requirement | 1: Information Disclosure of Local Data | 2: Information Disclosure of Data in Transmission | 3: Information Modification of Local Data | 4: Information Modification of Data in Transmission | 5: Time Manipulation | 6: Unavailability of Assets | 7: Modification of Assets | 8: Repudiation of Facts | 9: Impersonation | 10: Incomplete Mediation | 11: WP6_19: Missing binding and missing acknowledgement of messages within transactions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1: Authentication and authorization | X | | X | | X | | X | | X | X | X |
| 2: Data confidentiality | X | X | | | | | | | | | |
| 3: Data integrity | | | X | X | X | | | X | X | | X |
| 4: Non-repudiation | | | | | | | | X | | | X |
| 5: Data backup and recovery | | | X | X | | X | X | | | | |
| 6: System protection components | X | X | X | X | | X | | | X | X | |
| 7: Secure SW/FW Updates | | | | | | | X | | | | |
| 8: Secure Network Design | X | X | X | X | X | X | X | X | X | X | X |
| 9: Security Management | X | X | X | X | X | X | X | X | X | X | X |
| 10: Logging and Audit | | | | | | | | X | | | |
| 11: Time Synchronization | X | | X | | X | | | X | | | X |

| Basic Threat / Security Requirement | 1: Information Disclosure of Local Data | 2: Information Disclosure of Data in Transmission | 3: Information Modification of Local Data | 4: Information Modification of Data in Transmission | 5: Time Manipulation | 6: Unavailability of Assets | 7: Modification of Assets | 8: Repudiation of Facts | 9: Impersonation | 10: Incomplete Mediation | 11: WP6_19: Missing binding and missing acknowledgement of messages within transactions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 12: Observation of Policies & Laws | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) |
| 13: Transaction Security | | | X | | | | | X | | | X |

**Table 1: Security requirements covering identified basic and WP-specific threats**

The table does not address session security as a specific item. Session security is achieved by combining the three security requirements 1, and 2 or/and 3. Session security may refer to a communication session between two hosts, e.g., by using TCP/IP as the transport medium. Transaction security instead refers to application level logic work flows.

The notion (X) refers to a rather indirect relation between the security requirement and the addressed threat. The security requirement is expected not to have a direct technical influence on the threat coverage. It rather implicitly requires the application of certain security measures to counter those threats.

Although all of the mentioned threats are basically covered by one or more requirements, it has to be pointed out that due to the complexity of Smart Grid and diversity of its assets, it may be difficult to fulfill some of the requirements using the existing standard security methods and so the following factors have to be considered:

- lack of suitable cryptographic key management methods;

  the cryptographic key of some of the assets have to be periodically updated, or at least revoked in contrary to the existing situation. Taking into account the scale of the Smart Grid system, maintenance of the keys may lead to a threat of key (e.g. of smart meters) corruption;

- lack of suitable encryption methods;

  due to limited memory and processing power of some of the control devices, fast cryptographic computation required for cryptographic methods may not be supported;

- lack of suitable malware protection methods;

  due to their technical limits the field devices may not have suitable malware detection software. If e.g. field workers access such devices through not maintenance dedicated terminals that are not malware-proof, the result may be malware being spread into the Smart Grid.

# 4. Existing Security Enablers and Constraints

This section provides an overview about existing security enablers which are either given by FI-WARE, existing standards or guidelines, and regulation and legislation frameworks. The figures and most of the text are adapted from the FI-WARE public wiki page on the security chapter [189] and the open specification pages for the different components [190].

## 4.1 Generic Enablers from FI-WARE

Figure 14 depicts the Security Reference Architecture from FI-WARE. This Reference Architecture comprises:

1. an advanced security monitoring system that covers the whole spectrum from acquisition of events up to display, going through analysis but also going beyond thanks to a digital forensic tool and assisted decision support in case of cyber-attacks;

2. a set of GEs for a number of shared security concerns (i.e. identity and access management as well as privacy and auditing) that are considered core and therefore present in any FI-WARE Instance;

3. a component able to dynamically invoke and compose security services in order to answer related security needs while dealing with constraints which may apply (e.g. regulatory);

4. a set of optional security GEs to address current and future requests from concrete usage areas.

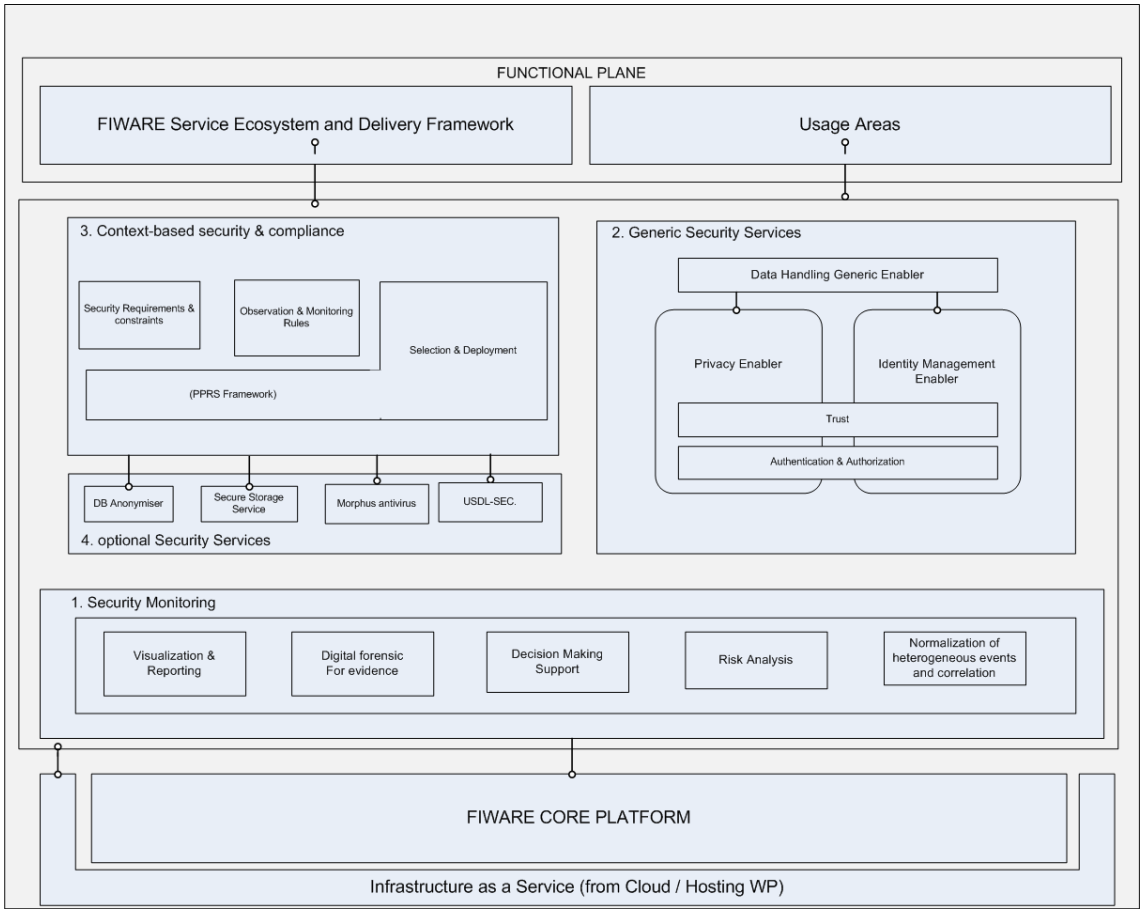


**Figure 14: FI-WARE high level security architecture**

In the following sections, we list the identified FI-WARE security-related Generic Enablers and provide a short description for each one.

### 4.1.1 Security Monitoring GE

The Security Monitoring GE is part of the overall Security Management System in FI-WARE and as such is part of each and every FI-WARE instance. The target users are: FI-WARE Instance Providers and FI-WARE Application/Service Providers.

The main concerns are:

- detect vulnerabilities and identify risks;
- score vulnerabilities impact and assess risks;
- analyze events to correlate and detect threats and attacks;
- treat risks and propose counter-measures;
- visualize result alarms and residual risks in order to allow efficient monitoring from the security perspective.

Security monitoring is the first step towards understanding the real security state of a future internet environment and, hence, towards realizing the execution of services with desired security behavior and detection of potential attacks or non-authorized usage.

Security monitoring is focused essentially on monitoring alarms from network equipment, systems and security sensors. By the collection, filtering and correlation of data from large-scale heterogeneous environments, including sensitive data from security tools and devices, SCADA events, raw sensor data, suspicions behaviors, etc., coupled with a dynamic risk analysis engine, decision making support and role-oriented visualization engine, the security stakeholders can take appropriate actions to prevent and mitigate the impact of abnormal behavior.

In addition, the availability of digital forensic evidence models and tools will provide a digital forensic for evidence solution to analyze abnormal behavior, carry out a criminal investigation and provide evidence with legal value.

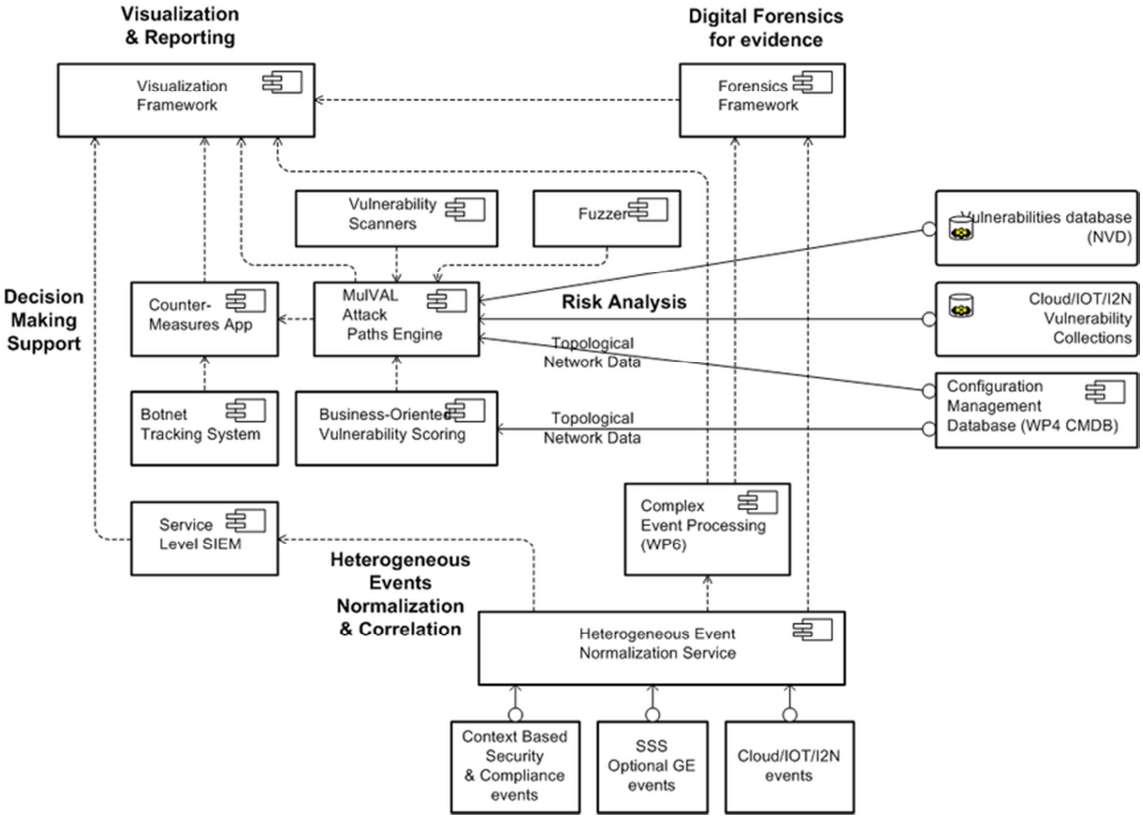


**Figure 15: Security Monitoring GE architecture**

### 4.1.2 Identity Management GE

This enabler provides authentication/access control and identity/attribute assertions as a service to relying parties. The relying parties are typically service providers that provide easy and secure access to their services to users/IoT/other services for instance by means of single sign-on (SSO), and that rely on personal user attributes (e.g. preferences, location, home address, etc.).

The users need easy access (SSO) to the growing number of services, and many of them also prefer their personal/identity attributes to be maintained by a trusted party which also protects the users' privacy. The Identity Management core Generic Enabler can be used by such a trusted party which we also call an identity provider (for SSO) and attribute broker.

The Identity Management GE is a core Security GE that provides services to its relying parties via open protocols such as OAuth [171] and OASIS SAML v2.0 [172] (Security Assertion Markup Language). Basic concepts are:

- **User Life-Cycle Management**
  The IdM offers tools for administrators to support the handling of user life-cycle functions. It reduces the effort for account creation and management, as it supports the enforcement of policies and procedures for user registration, user profile management and the modification of user accounts. Administrators can quickly configure customized pages for the inclusion of different authentication providers, registration of tenant applications with access to user profile data and the handling of error notifications. For end users, the IdM provides a convenient solution for registering with applications since it gives them a means to re-use attributes like address, email or others, thus allowing an easy and convenient management of profile information. Users and administrators can rely on standardized solutions to allow user self-service features like:
  - user registration and login resp. logout,
  - checks for password strength,
  - password reset or renewal procedures or Secured storage of user data.
- **Flexible Authentication Providers**
  In addition to providing a native login, the Identity Provider (IdP) supports the integration of multiple 3rd party authentication providers. Foremost, it supports in a first step the configuration of preferred identity providers to lower entry barriers for a native user registration to administrators and, on the user's side, to link a preferred 3rd party IdP as alternative authentication provider to a native account.
- **3rd Party Login**
  3rd party login supports customers of the IdM to enhance the reach of their websites by means of attracting users without forcing them to register new user accounts on their sites manually. 3rd party login allows users to register to the customers' sites with already existing digital identities from their favorite 3rd party identity providers, such as e.g. Google, Facebook or Yahoo. Thus, 3rd party login lowers the obstacles of registration processes and increases the number of successful business flows on the customers' sites.
- **Web Single Sign-On**
  As it is possible to configure several applications that shall be linked to his IdM, the main benefit for users is a single sign-on (SSO) to all these applications.
- **Hosted User Profile Management**
  The IdM offers hosted user profile storage with specific user profile attributes. Applications do not have to run and manage their own persistent user data storages, but instead can use the IdM user profile storage as a SaaS offering.
- **Multi-Tenancy**
  A multi-tenancy architecture refers to a principle in software architecture where a single software instance runs on a server, serving multiple client organizations/customers (tenants).

  Multi-tenancy is contrasted with a multi-instance architecture where separate software instances (or hardware systems) are set up for different client organizations. With a multi-tenant architecture, a software application is designed to virtually partition its data and configuration, and each client organization works with a customized virtual application instance. In a multi-tenancy environment, multiple customers share the same application, running on the same

operating system, on the same virtualized hardware, with the same data storage mechanism. The distinction between the customers is achieved during application design, thus customers do not share or see each other's data. The concept allows each tenant to apply their own branding to login or registration UIs or for user self-services to create a user experience that is aligned with the one offered in a tenant application.

### 4.1.3 Privacy GE

The Privacy Generic Enabler provides a set of functionalities similar in scope to the Identity Management Generic Enabler described in the previous section but enhanced using special privacy enhancing technologies. These privacy-enhancing technologies are primarily centered on special credentials that contain attributes about the user which can be disclosed for authentication purposes selectively on a need-to-know basis.

This component will utilize many of the basic functions provided by the Identity Management Generic Enabler (see Generic Identity Enabler). The Privacy Generic Enabler includes the IDM solution (IdM "front end" (IdMaaS) and the IdM "back end" (Authentication)). It communicates with the relying parties (services, things) as well as with the subjects of authentication and attributes assertions (users, things).

Special privacy enhancing technologies:

- Privacy Enhanced Credential Management: This privacy credential sub element is based on IBM's Idemix library and provides private credential systems and minimal disclosure tokens for enhanced privacy protection mechanisms. End-users are provided with the possibility of selectively disclosing their asserted private attributes or even just proving predicates over their attributes in an unlinkable manner. At the same time, the cryptographic technologies ensure strong and secure authentication to the service/resource providers. In a private credential system, users can have different identities with different identity providers and identity consumers. In fact, an identity should be seen as the collection of attributes that are known to a party about the users. Furthermore, identity providers can issue a credential asserting attributes to a user. A user can then selectively reveal the attributes contained in a credential to an identity consumer. That is, the consumer will only learn that the identity provider asserted the revealed attribute but is not able to learn any other asserted attributes. The user can repeat this disclosure process as many times as he/she wishes without that these transactions can be linked to each (unless the disclosed attributes are unique). Thus, together with privacy-enhanced attribute-based access control, private credentials offer the best possible privacy protection. Finally, we note that the Identity Mixer private credential system also offers all the standard feature of a public key infrastructure such as revocation of credentials or hardware-binding.
- Privacy Enhanced Access Control: In order to support the full functionality of privacy-enhanced credentials an enriched policy language and token format is needed. The PrimeLife Privacy Policy already extends the standard XACML language to express for the important concept of predicates on attributes. That is, instead of revealing an attribute only the fact that some condition on the attribute is fulfilled will be revealed. Further extensions in the Privacy Enhanced Access Policy will cover the use of unlinkable pseudonyms instead of (identifying) public keys, or the optional lifting of the anonymity. Please refer also to "Data Handling Generic Enabler".

Privacy aspects are related to more security controls than authentication. It should be therefore discussed with the FI-WARE to determine

- the linkage of other security enablers providing other important functionalities like encryption during transmission, secure storage or logging/audit functionalities to the Privacy GE;
- the applicability of the privacy architecture elements proposed within the draft of ISO standard 29101.

### 4.1.4 Data Handling GE

The component provides a mechanism for controlling the usage of attributes and personal data based on the concept of 'sticking' a data usage policy to the data to which it applies. When the data is accessed by an application, an access control technology is then used to verify that the intended use of the data matches the scope defined in the usage policy.

**Component Description**

- Privacy Policy Engine: After the credentials of the user have been verified a check is made which policies apply to the user's request. Policies are stored in the policy store and can be modified by both the users (own policies) and the administrators (all policies), depending on the scope of policy.
- Credentials and Crypto: This component is responsible for enciphering the data stored by the user in the Data Store. Enciphering is being done by the public key of the users. In the case the users intend to retrieve data, their private key would be required. On top of that, this component authenticates the users by checking the user's credentials, prior to forwarding the requests to the Privacy Policy Engine.

### 4.1.5 Context-based security and compliance

The role of this Generic Enabler is to support additional security requirements requested by a specific subset of applications as a result of the application of very specific regulatory constraints.

The GE will accept a security request from a client application and will select the best Optional Security Enabler to fulfill it.

The deployed security enabler will implement the compliance between the client security request and any applicable regulation from Private and or Public sources.

The framework has also monitoring capabilities to oversee the system performance.

As a result of this monitoring, if a non-conformance is detected, the framework is capable of performing run-time and context-based reconfiguration of deployed security enablers, so that, for example, a client application will be provided with a new configuration for the security enabler it is utilizing, or it can receive instructions to stop using that security enabler and start using a newly provided one.

The figure below provides a high-level initial architectural sketch of the components of this Generic Enabler.

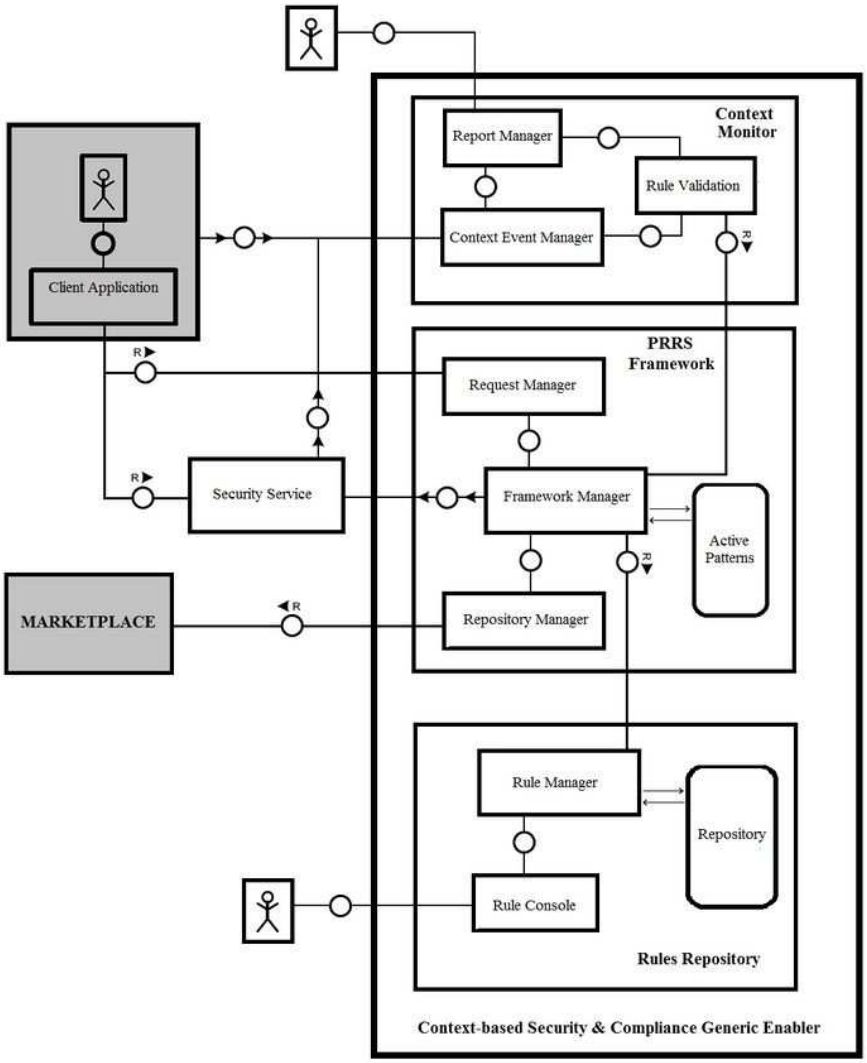


**Figure 16: Context-based security and compliance architecture**

### 4.1.6 Optional Security Service Enabler

The Optional Security service enabler is used to customize the security service description within USDL-SEC when the security functionality is not covered by the specification. This asset targets directly the application domain usage. The goal is to make easily extendible the security service description for customized usage. This functionality will encourage all the developers to define and describe their own services through the USDL standard by adding new functionalities and new capabilities.

Some example of possible optional security services could be:

- **a database risk evaluation and anonymization service** used to check a shared database is not vulnerable to the re-identification of the non shared part of the database. The service can be used to support these database administrators to evaluate the disclosure risk for all their types of data; by recommending the safest configurations using a smart bootstrapping system. The service will provide the user with a feedback on the re-identification risk when disclosing certain information and proposing safe combinations in order to help him/her during the information disclosure. Albeit privacy risk estimators have already been developed in some specific contexts (statistical databases), they have had limited impact since they are often too specific for a given context, and do not provide the user with the necessary feedback to mitigate the risk. In addition, they can be computationally expensive on large datasets;
- **secure storage service** that offers the possibility to safely backup data and delegates the access to parts of data to a third party. Data leaks are resulting from the lack of additional information

on data: sensitivity, access rights, lifetime, etc. The existence and the availability of these kinds of attributes are necessary to master the storage and the exchange of sensitive data. The concept consists in providing a secure storage service, manipulating self-protected metadata only. This (optional) service can be used or not by other services, depending on the privacy level of implied data. The main objective of the secure storage service is to provide a secure storage of sensitive / private data, privacy-oriented capacities, according to legislation;

- **malware detection service** (Morphus) that explores a data structure in order to check whether this dataset contains malware applications. Morphus is a generic malware detector based on graph signatures. Unlike the traditional notion of detection based on string pattern matching, graphs allow a behavioral analysis of programs, thus providing a much finer description of malwares.

## 4.2 Security requirement regulations and guidelines to be considered

Besides technical standards or guidelines in the context of Smart Grid provided by several standardization bodies like IEC, IEEE, IETF, etc. and guidelines provided by NIST or CIGRE, also regulatory requirements need to be obeyed. The following subsections provide a subset of potential applicable regulations and guidelines.

### 4.2.1 BDEW whitepaper

The German Association of Energy and Water Industries (Bundesverband der Energie- und Wasserwirtschaft – BDEW) was founded by the federation of four German energy-related associations: the Federal Association of the German Gas and Water Industries (Bundesverband der deutschen Gas- und Wasserwirtschaft - BGW), the Association of Multi-Utilities and Regional Energy Distributors in Germany (Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland - VRE), the Association of Network Operators (Verband der Netzbetreiber - VDN) and the Association of the Electricity Industry (Verband der Elektrizitätswirtschaft - VDEW). The BDEW introduced a white paper (cf. [2]) defining basic security measures and requirements for IT-based control, automation and telecommunication systems, taking into account general technical and operational conditions. It can be seen as a further national approach targeting similar goals as NERC-CIP. The white paper addresses requirements for vendors and manufacturers of power system management systems and is used as an amendment to tender specification. Meanwhile, there is also a country specific regulation enhancement available for Austria.

### 4.2.2 Results from the European Expert Group 2 (EG2)

Within the European Union, the Smart Grid Joint Working Group (SGJWG) has been founded in 2008 to advise the commission on policy and regulatory directions at European level and to coordinate the first steps towards the implementation of Smart Grids. The SGJWG splits its work into three expert groups (EG) working on specific topics like required functionalities of Smart Grids and smart meters (EG1), regulatory recommendations for safety data handling and data protection (EG2), and roles and responsibilities in the Smart Grid (EG3). The goal was to identify and produce of a set of regulatory recommendations to ensure EU-wide consistent, and fast implementation of Smart Grids, while achieving the expected Smart Grids' services and benefits for all users involved. The EG2 targets the identification of appropriate regulatory scenarios and recommendations for data handling, security, and consumer protection to establish a data privacy and data security framework that both protects and enables. The report is publicly available (cf. [36]).

The key recommendations of this report regarding data privacy are the following:

- “privacy and security by design” for all Smart Grid products and solutions;
- gap within EU standards relating to the handling and security of data within the area of Smart Grids;
- one European generic model for key management, and security and privacy, relevant for any device or body in the Smart Grid if communicating consumption data;
- distinction between personal (privacy issues) and non personal data (no privacy issues);
- clear division of roles and responsibilities regarding ownership, possession, and access to data.

All three expert groups collaborate with the joint working group on standards of CEN, CENELEC, and ETSI, which provides consulting for the commission addressing the mandate on Smart Grid M/490 (cf. [37]).

### 4.2.3 Results from the security team of the Smart Grid Coordination Group (SGIS)

The objective of mandate M/490 (cf. [37]) is the development or update of a set of consistent standards within a common European framework that will facilitate the implementation of the different high level Smart Grid services and functionalities. As a successor of the EU SGJWG, the Smart Grid Coordination Group (SGCG) has been founded in June 2011directly addressing mandate M/490. As security is one of the targets of this mandate, a dedicated subgroup – the SGIS – addresses this topic explicitly.

IT- security is closely connected to the architectural model provided by the reference architecture group as SGAM (Smart Grid Architectural Model). Security applies basically to every interface and component in the SGAM depending on the intended use cases. To provide guidance on which security means are to be applied, an analysis is necessary for a specific use case. This is typically being done by performing a threat and risk analysis for a dedicated use case targeting the identification of potential vulnerabilities in the use case and recommending appropriate counter measures as a bottom up approach. It is also possible to start with a top down approach, which has been done by the WG IS.

The SGIS mapped the security requirements stemming from regulation documents like NERC-CIP (see also section 4.2.4), but also from guidelines like the NIST IR 7628 framework (cf. section 4.2.5) to existing security standards, focusing at first on ISO 27001, ISO 27002, and IEC 62351. The goal was the identification of gaps and the description of necessary actions to be taken. Moreover, the target was also a toolbox that describes the available security measures based on a set of general use cases (see also draft report [84]). This toolbox should help system developer to choose the right security option. Security Task 1.6 had close interaction with the SGIS WG and provided to this toolbox. The toolbox itself has been applied in FINSENY in the context of defining security architecture elements.

Note that the 2-year working period of the SGIS WG and the complete SG-CG finished in December 2012. Nevertheless, there is a further two year working period during which Smart Grid specific issues, including security, can be addressed.

### 4.2.4 NERC (North American Electric Reliability Corporation)

The North American Electric Reliability Corporation's mission is to ensure the reliability of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards and monitors users, owners, and operators for preparedness. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. NERC has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–011 (cf. 9.1), which are defined to provide a foundation of sound security practices across the bulk power system. These standards are not designed to protect the system from specific and imminent threats. They apply to operators of Bulk Electric Systems. The profiles originate in 2006. NERC-CIP provides a consistent framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional as well as non-functional requirements. Table 2 provides an overview of the different parts of NERC-CIP.

| CIP | Title / Content |
|---|---|
| 002 | Critical Cyber Asset Identification<br>Identification and documentation of Critical Cyber Assets using risk-based assessment methodologies |
| 003 | Security Management Controls<br>Documentation and implementation of Cyber Security Policy reflecting commitment and ability to secure Critical Cyber Assets |
| 004 | Personnel and Training<br>Maintenance and documentation of security awareness programs to ensure personnel knowledge on proven security practices |
| 005 | Electronic Security Protection<br>Identification and protection of Electronic Security Perimeters and their access points surrounding Critical Cyber Assets |

| CIP | Title / Content |
|---|---|
| 006 | Physical Security Program<br>Creation and maintenance of physical security controls, including processes, tools, and procedures to monitor perimeter access |
| 007 | Systems Security Management<br>Definition and maintenance of methods, procedures, and processes to secure Cyber Assets within the Electronic Security Perimeter to do not adversely affect existing Cyber Security Controls. |
| 008 | Incident Reporting & Response Planning<br>Development and maintenance of a Cyber Security Incident response plan that addresses classification, response actions and reporting |
| 009 | Recovery Plans for Critical Cyber Assets<br>Creation and review of recovery plans for Critical Cyber Assets |
| 010 | Bulk Electrical System Cyber System Categorization (draft)<br>Categorization of BES systems that execute or enable functions essential to reliable operation of the BES into three different classes. |
| 011 | Bulk Electrical System Cyber System Protection (draft)<br>Mapping of security requirements to BES system categories defined in CIP-010 |

**Table 2: NERC-CIP overview**

CIP-011 did not lead to new cyber security requirements, but it provides a new organization of the existing requirements in the current CIP standards and eliminates the non-routable protocol exception. The classification of Bulk Electric Systems (BES) into the three categories low, medium, and high impact BES cyber systems, and the mapping of these to security controls are new.

### 4.2.5 NIST

The National Institute of Standards and Technology is a US federal technology institute that develops and promotes measurement, standards, and technology. In 2009, NIST formed the Smart Grid Interoperability Panel (SGIP) as a public-private cooperation with over 600 members that develops frameworks and roadmaps, not standards. SGIP's security related work is carried out in the Cyber Security Working Group (CSWG). The following subset of NIST documents directly applies to security in Smart Grid environments:

- NIST Special Publication 800-39: "Managing Information Security Risk: Organization, Mission, and Information System View" (cf. [8]) provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations);
- NIST Special Publication 800-53: "Recommended Security Controls for Federal Information Systems" (cf. [11]) provides guidelines for selecting and specifying technical and organizational security controls and connected processes for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200 ("Minimum Security Requirements for Federal Information and Information Systems"). It provides an extensive catalog of security controls and maps these in a dedicated appendix to industrial control systems;
- NIST Special Publication 800-82: "Guide to Industrial Control Systems (ICS) Security" (cf. [12]) provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). It uses NIST SP 800-53 (cf. [11]) as a basis and provides specific guidance on the application of the security controls in NIST SP 800-53. This publication is an update to the second public draft, which was released in 2007;
- NIST Special Publication 1108: "NIST Framework and Roadmap for Smart Grid Interoperability Standards" (cf. [4]), describes a high-level conceptual reference model for the Smart Grid. It lists 75 existing standards that are applicable or likely to be applicable to the ongoing development of the Smart Grid. The document also identifies 15 high-priority gaps and potential harmonization

issues for which new or revised standards and requirements are needed. Note that meanwhile a revision of this document is available;

- NISTIR 7628 (cf. [5], [6], and [7]) originates from the CSWG and targets the development of a comprehensive set of cyber security requirements building on NIST SP 1108 (cf. [4]), also stated above. The document consists of three subdocuments targeting strategy (cf. [5]), security architecture (cf. [6]), and requirements, and supportive analyses and references (cf. [7]).

### 4.2.6 Data privacy protection regulations

In most advanced industrial democracies, data privacy laws only emerged a few decades ago, aiming at protecting information on private individuals from intentional or unintentional disclosure or misuse. Through the increasing use of automated data processing and online communication the collection and correlation of data gets easier and easier. Privacy protection is necessary here, to protect person related data, like for example customer identification and location data, consumption profile, billing data, etc. from being revealed for purposes other than originally intended.

Privacy protection acts are typically applied as national laws and differ from country to country. Besides regulations, there exist also guidelines on defining privacy protection rules, which are provided for instance by the NIST. The following subsections give an overview about regulations at the European level and, exemplarily, in two European Member States, Germany and the United Kingdom.

#### 4.2.6.1 Data privacy regulations in Europe

Adopted in 1995, the European Directive 95/46/EC on Protection of Personal Data [52] was designed to unify national laws on data protection within the European Community and came into force in 1998. It regulates the handling of personal data relating to a natural person processed by automated means or in non automated filing systems. The following table summarizes the key requirements which Member States were required to transpose into compliant national laws:

| Requirement | Content |
|---|---|
| Transparency | – The data subject should have a clear understanding which data are collected and how they are processed and used.<br>– The data subject has to be notified about the processing of his personal data.<br>– Access to data has to be granted to the data subject.<br>– Data must be rectified, erased, or blocked if wished by the data subject.<br>– The instance responsible for the processing of personal data (=data controller) must provide its name and address, the purpose of processing, the recipients of the data and all other information required to ensure a fair processing. |
| Legitimate purpose | Personal data need to be collected and processed only for the specified, explicit and legitimate purposes. |
| Proportionality | – Data processing must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.<br>– Personal information shall not be disclosed to third parties unless authorized by law or by consent of the individual.<br>– Data has to be kept accurate and up to date.<br>– Adequate data processing must include protection against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. |

**Table 3: Data privacy protection requirements in the EU**

At the end of January 2012, the European Commission proposed a comprehensive reform of the EU data protection legal framework [53] with the objective to cope with divergences in implementation and enforcement in the EU Member States and reduce administrative costs. Among others, it includes as key changes:

- a single set of data protection rules across the EU,
- a single responsible national data protection authority for data controllers in the EU country where they have their main establishment,
- a data owner residence principle, wherever the data controller is located or data is stored,

- an explicit consent of the data owner required, rather than assumed.

#### 4.2.6.2 Data privacy regulations in Germany

The German data privacy legal framework is based on the one hand on the German Federal Data Protection Act [54] and on the other hand on different state data protection acts. Additionally, some further laws and regulations amending both German national and state laws will be considered too, as they are especially relevant for Smart Grid services.

##### *4.2.6.2.1 German Federal Data Protection Act*

The German Federal Data Protection Act (Bundesdatenschutzgesetz BDSG), first enacted in 1977 and revised in 2001, 2006, 2009 and most recently in 2010 [54], regulates the handling of personal data about individuals which is collected, processed and used in IT systems or collected by public and private bodies and commercial enterprises (e.g. energy suppliers, metering service providers and operators, …,) in a non-automated manner.

The office of the Federal Data Protection Commissioner was subsequently created in 1978.

In the BDSG, three requirements draw the general lines of the legal data protection framework:

- Data reduction and economy: as few as possible data shall be collected, processed and stored (BDSG §3a (1)); whenever possible with reasonable effort, pseudonyms shall be used instead of clear names, or – even better – data shall be made completely anonymous (BDSG §3a (2)).
- Necessity: only data which are necessarily required for a given purpose shall be collected (BDSG §§13, 14 (1)).
- Appropriation: data must not be used for other purposes than designated (BDSG §§ 14, 31, 39…).

The collection of private data is in general prohibited, except if it is explicitly allowed by a law, or by a qualified agreement of the subject (BDSG §4 (1), §4a (1)). Even after having given their consent, data subjects have the following inalienable rights (BDSG §6 (1)):

- Get information or be notified whether and which personal data are recorded about them (BDSG §§19, 19a)
- Get information or be notified about the source, recipients, and purpose of storing data (BDSG §§ 19, 19a)
- Let wrong data be rectified (BDSG §20 (1))
- Demand the erasure of illegitimately collected data and of data which are not required anymore (BDSG §20 (2))
- Block data, if:
  - erasure is prevented by legal, statutory, or contractual reasons (BDSG §20 (3))
  - erasure may affect interests of the subject which deserve to be protected (BDSG §20 (3))
  - erasure is not possible or requires a disproportional high effort because of the special way of recording (BDSG §20 (3))
  - correctness of data is contested and cannot be resolved (BDSG §20 (4))
- Limit transfer of blocked data to third parties (BDSG §20 (7))
- Object against generally legitimate data processing (BDSG §20 (5))
- Inspect procedure descriptions for automated data processing registered at the Federal Commissioner for Data Protection and Freedom of Information (BDSG §38 (2))
- Appeal to the Federal Commissioner for Data Protection and Freedom of Information (BDSG §21).

The privacy protection requirements resulting from the BDSG have to be fulfilled by organizational and technical measures (BDSG §9 (1)) as long as these require effort proportional to the desired protection level (BDSG §9 (2)). In case of automated processing or usage of personal data, the following measures are requested (Annex to BDSG §9 (1)):

- **Access control**, to prevent unauthorized access to and usage of systems processing or using personal data as well as to prevent access to personal data, except as defined in the access control model (i.e. including physical access control, user control, and data access control)
- **Disclosure control** to prevent unauthorized operations on personal data during transmission, transport or storage, and ensuring the control of correct distribution of data
- **Input control** to ensure that it can be detected afterwards, whether and by whom personal data were inserted, changed or removed
- **Job control** to ensure that personal data processed on behalf of others are processed only in the way they were ordered to
- **Availability control** to protect personal data against accidental loss or destruction
- **Separation of processing** to ensure that data which are collected for different purposes are processed separately.

Finally, state-of-the-art **encryption** is explicitly stated to be an appropriate measure for protecting access to personal data.

*4.2.6.2.2 Federal State Data Protection Acts*

In 1970 the German federal state of Hesse enacted the world's first general data protection law in response to concerns about the implications of automated data processing in the public administration like e.g. municipal energy suppliers (not privatized). By 1981, all other West German federal states had followed suit with laws regulating data protection both in federal state and local government agencies and in public bodies [55].

In each federal state, observance of the law is controlled by a state data protection commissioner.

The state data protection acts [56] regulate the handling of personal data about individuals in the related state administration and public agencies. In all of them, the processing of personal data is generally prohibited except if it is explicitly allowed by law or by consent or in case of emergency. Moreover, data subjects have the following unalienable rights:

- get information or be notified whether and which personal data are recorded about them;
- let wrong data be rectified;
- blocking if correctness of data is contested and cannot be resolved, or if data are not required anymore;
- demand the erasure of illegitimately collected data and of data which are not required anymore;
- object to generally legitimate data processing;
- claim to omission and compensation in case of violation;
- inspect procedure descriptions for automated data processing registered at the relevant state commissioner for data protection;
- appeal to the relevant state commissioner for data protection.

The federal states of Berlin, Brandenburg, Hamburg, Mecklenburg-West Pomerania, North-Rhine Westphalia, Saxony, Saxony-Anhalt and Thuringia require that security measures are used to protect the following properties:

- **confidentiality** of personal data;
- **integrity** of personal data during processing so as to keep them intact, complete and up to date;
- **reliable and in-time provision** of data for proper processing (availability);
- **authenticity** of data for correct classification of their source;
- **auditability** to provide traceable processing;
- **transparency** of processing, thank to complete and up to date documentation.

Similarly, the federal state of Schleswig-Holstein defines confidentiality, integrity, availability, transparency, and auditability as protection objectives. Moreover, it relies on two further key principles:

- **unlinkability** of personal data to any other set of personal data collected, processed or used for another purpose;
- **intervenability** in any kind of personal data processing, where necessary.

Other federal states like Baden-Wuerttemberg, Bavaria, Bremen, Hesse, Lower Saxony, Rhineland-Palatinate, and Saarland define some technical and organizational measures to be deployed:

| Security measures | Baden-Wuerttemberg | Bavaria | Bremen | Hesse | Lower Saxony | Rhineland-Palatinate | Saarland |
|---|---|---|---|---|---|---|---|
| Access control (incl. physical access control, system access control / user control, and data access control) | X | X | X | X | X | X | X |
| Data media control (against unauthorized reading, copying, modification or removal of data media) | X | X | | | X | | |
| Storage control (against unauthorized input of data and unauthorized inspection, modification or deletion of stored personal data) | X | X | | | X | | |
| Communication control (to verify and establish to which bodies personal data may be or have been transmitted) | X | X | | X | X | | |
| Transport control (against unauthorized reading, copying, modification or deletion of personal data during transfer of personal data or during the transportation of data media) | X | X | | | X | | |
| Input control (to verify and establish which personal data have been input into automated data processing systems and when and by whom they were input) | X | X | X | | X | X | X |
| Processing control (to verify and establish which personal data have been processed into automated data processing systems and when and by whom they were processed) | | | | X | | X | |
| Job control (to ensure that personal data processed on behalf of others are processed only in the way they were ordered to) | X | X | X | X | X | X | X |
| Availability control (against accidental loss or destruction) | X | | X | | X | X | X |
| Organization control (design the internal organization so that it meets the data protection requirements) | X | X | | X | X | | |
| Disclosure control (against unauthorized operations on personal data during transmission, transport or storage, and to ensure the control of correct distribution of data) | | | X | | | X | X |
| Separation of processing (to ensure that data which are collected for different purposes are processed separately) | | | X | | | X | X |

| Security measures | Baden-Wuerttemberg | Bavaria | Bremen | Hesse | Lower Saxony | Rhineland-Palatinate | Saarland |
|---|---|---|---|---|---|---|---|
| Documentation control<br>(to document the processing of data to ensure traceability) | | | | X | | X | |

**Table 4: Security measures required by German federal state data protection acts**

*4.2.6.2.3 Further Smart Grid specific regulations in Germany*

Additionally, further regulative requirements in regard to the processing of Smart Grid related information are provided in the next table:

| Regulations | Requirements |
|---|---|
| Energy Industry Act (Energiewirtschaftsgesetz<br>- EnWG incl. EnWG Novelle 2011) [57] | – Adequate protection of communication and data processing systems used for power system control<br>– Metering point operator change: exchange of necessary data between the former and new operators and immediate erasure of all personal data by the former operator<br>– Information and access right of end user to personal data processed by the metering point operator<br>– Collecting, processing and use of personal data from metering systems only by authorized parties (metering point operator, network operator, supplier, …) and only if necessary according to EnWG (e.g. consumption measurement, energy supply incl. billing, variable tariffs…)<br>– Qualified information and consent form of end user necessary for remote control and metering<br>– Compliance of metering, storage, and processing systems with data privacy requirements<br>– Installation only of certified metering systems fulfilling the protection profile requirements for data acquisition, processing, storage, checking, transfer<br>– State-of-the-art security and data privacy protection measures for metering data transfer (data confidentiality + integrity, authentication of the transferring party, state-of-the-art encryption over public networks…)<br>– Anonymization or at least aliasing of personal data whenever possible<br>– Fulfill principles of data reduction and economy, necessity of data processing, and appropriation<br>– … |
| Metering Access Ordinance (Messzugangsverordnung - MessZV) [58] | Contractual obligation to mutual data transmission between network operator and metering operator / service provider and to archiving of transmitted data by the network operator for the time necessary to network access |
| Ordinance on Electricity Grid Access (Verordnung über den Zugang zu Elektrizitätsversorgungs-netzen - StromNZV) [59] | – Energy supplier change: handles customer data transfer by the new supplier to the grid operator.<br>– Household customers: manual reading metering devices at regular time intervals (app. every 12 months),<br>– Electronic data exchange for initiation and settlement of the network use between the grid operator and users |

| Regulations | Requirements |
|---|---|
| Ordinance on General Terms Regulating Universal Service for Household Customers and Replacement Supply via the Low Voltage Network (Verordnung über Allgemeine Bedingungen für die Grundversorgung von Haushaltskunden und die Ersatzversorgung mit Elektrizität aus dem Niederspannungsnetz - StromGVV) [60] | Representatives of the network operator, metering point operator, or basic supplier must be granted access by the customer (upon prior notification) for determining the basis for price assessment or meter reading |
| Low Voltage Connection Ordinance (Niederspannungsanschlussverordnung - NAV) [61] | – Representatives of the network operator, metering point operator or service provider must be granted access by the energy subscriber / user (upon prior notification) for inspection, replacement, reading, or disconnection of the technical equipment and metering devices. |

**Table 5: Further German regulations for data privacy protection**

At the moment, there are ongoing discussions about adapting the German regulation to new requirements related to Smart Grids. Data protection officers and consumer protection organizations demand high protection of end customer data.

#### 4.2.6.3 Data privacy regulations in the United Kingdom

Unlike Germany, the UK legal data privacy protection framework is based on persuasion rather than punishment. Its more flexible approach makes it easier for technologies with global data flows like cloud computing. However, tougher regulatory measures are expected in the future, as the EU data privacy regulation is being reformed as explained in chapter 4.2.6.1.

In the UK, data privacy is protected by various laws, regulations, and so-called “soft laws” [63]:

- the Human Rights Act 1998 (HRA) [64];
- the Data Protection Act 1998 (DPA) [65];
- the Freedom of Information Act 2000 (FoIA) [66];
- the Regulation of Investigatory Powers Act 2000 (RIPA) [67], regulating the way some public bodies may conduct surveillance and access electronic communications;
- common law protection through the tort of breach of confidence, when personal information of private or confidential nature has been given to a third party without the data subject’s consent;
- informal regulation, codes of practice, and other forms of “soft law”.

In the following sections, laws and regulations which could be relevant in Smart Grid scenarios will be briefly described.

##### *4.2.6.3.1 The Human Rights Act 1998*

The Human Rights Act (HRA) 1998 [64] came into force on October 2, 2000, introducing the European Convention on Human Rights (ECHR) [68] into English law, which provides in its article 8.1 an explicit right to respect for a private life. The HRA applies to all public bodies in the UK, like central government, local authorities, and any bodies exercising public functions.

According to the HRA, public bodies handling personal data must be able to demonstrate that data processing is:

- authorized by law;
- proportionate to the designated purpose;
- necessary for the functioning of a democratic society;
- compliant to one of the legitimate aims stated in Article 8(2) of the ECHR:

> "(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." [68]

*4.2.6.3.2 The Data Protection Act 1998*

The Data Protection Act 1998 (DPA) [65] regulates the handling of personal data related to a living individual by public authorities and private organizations and implements the EU Directive 95/46/EC by defining the following eight key principles for the processing of personal data (see DPA, Schedule 1, Part I):

- personal data shall be processed fairly and lawfully, i.e. processing must fulfill at least one of the following conditions (see DPA, Schedule 2):
  - The data subject has given his consent to the processing.
  - The processing is necessary for a contract or for the preparation of a contract.
  - The processing is necessary for a legal obligation (other than a contract).
  - The processing is necessary to protect the vital interests of the data subject.
  - The processing is necessary for the administration of justice or other public functions.
  - The processing is necessary to pursue the legitimate interests of the data controller or of third parties to whom the data are disclosed (unless it causes prejudices to the data subject).
- personal data shall be collected and processed only for the specified, explicit and legitimate purposes (DPA, Schedule 1, Part I, §2);
- data processing must be adequate, relevant, and not excessive in relation to the specified purposes (DPA, Schedule 1, Part I, §3);
- personal data shall be accurate and, where necessary, kept up to date (DPA, Schedule 1, Part I, §4);
- personal data shall not be not kept for longer than necessary (DPA, Schedule 1, Part I, §5);
- personal data shall be processed in accordance with the rights of data subjects (DPA, Schedule 1, Part I, §6);
- adequate data processing must include protection against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (DPA, Schedule 1, Part I, §7);
- personal data shall not be transferred to other countries outside the EU without adequate protection (DPA, Schedule 1, Part I, §8).

Besides, data subjects have the following rights:

- get information whether and which personal data are recorded about them, possibly against a small fee (DPA, Part II, section 7);
- get information about the recipients and purpose of storing data, possibly against a small fee (DPA, Part II, section 7);
- prevent processing likely to cause damage or distress (DPA, Part II, section 10);
- prevent processing for direct marketing purposes (DPA, Part II, section 11);
- prevent automated decision-taking significantly affecting the data subject (DPA, Part II, section 12);
- get compensation for breaches of the DPA (DPA, Part II, section 13);
- let wrong data be rectified, blocked, erased or destroyed (DPA, Part II, section 14);
- inspect the register of notifications held by the Information Commissioner (DPA, Part III, section 19).

The right to access personal data is restricted to electronic data and structured manual files.

*4.2.6.3.3 The Freedom of Information Act 2000*

The Freedom of Information Act 2000 (FoIA) [66] regulates the access to information held by public authorities in England and in Wales. Scotland has a similar Freedom of Information Scotland Act 2002 (FoISA).

The FoIA and the DPA overlap where personal information is considered for disclosure. In comparison to the DPA and in case of data processing by public authorities; the FoIA extends the notion of "data" to personal information in manual records, even unstructured ones (FoIA, Part VII, section 68).

Though, a 2003 Court of Appeal judgment (Durant vs. the Financial Services Authority) [69] restricted the notion of "personal data" to documents with the data the subject as its focus and not impacting his privacy and the right of access to structured manual files organized for the retrieval of personal data.

*4.2.6.3.4 Further Smart Grid specific regulations in the UK*

The Electricity Act 1989 [73] and the Gas Act 1986 [74] are the main acts regulating the energy sector, both respectively prohibiting the supply of electricity and gas without license. Additionally, the Energy Act 2011 [75] aims at improving the provision of energy efficiency measures to homes and businesses, especially favoring low carbon energy supplies.

In 2010, a coalition agreement between Conservatives and Liberal Democrats included an agreement to establish a Smart Grid and a rollout of smart meters across the country [76]. Regulations will need to be changed to achieve these goals. For this purpose, the Government has established the "Smart Metering Implementation Programme" (SMIP) and published a prospectus containing proposals for the design of a delivery model, the technical specification of smart meters, and other aspects like consumer protection and data privacy issues. In March 2011, the Government's Response to the Smart Meter prospectus was published. One proposal is, for instance, the establishment of a central Data and Communications Company (DCC) to coordinate communications between smart metering home equipment and authorized smart metering data users. Concerning data privacy, "privacy by design" is the favored approach. Moreover, the following activities are planned [77]:

- a "Privacy Impact Assessment" dedicated to the SMIP;
- a privacy policy framework dedicated to the SMIP, giving consumers the "choice as to how their smart metering data is used and by whom, except where it is required to fulfill regulated duties" [77];
- a privacy charter to be developed by suppliers to provide transparency about the new arrangements;
- the implementation of the framework through changes to the license model.

## 4.3 Security standards to be considered

This subsection lists several technical standards or current drafts of standards, which may need to be especially considered in the description of security countermeasures. These standards offer general and also domain specific security measures.

### 4.3.1 ISO/IEC

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are cooperating standardization bodies. ISO provides international standards, which target technical and organization means in several application domains. IEC develops international standards for all electrical, electronic and related technologies.

The following list contains potential standards targeting technical and administrative security requirements and solutions. Note that for selected standards that are likely to be applicable in FINSENY use cases separate subsections will provide more information:

- IEC 15118, which is currently being specified, defines the standard for vehicle to grid communication allowing for application layer interaction based on TCP/IP communication. Communication with the backend infrastructure is not directly targeted. Security is an integral part of the standard and is based on transport layer security using TLS (Transport layer Security) as well as XML digital signatures and XML encryption at the application layer. As security also targets the billing and payment relevant information, which may be exchanged with the backend

in case of contract based payments (plug & charge), the security measures in the standard go beyond the hop between the vehicle and the charging spot;

- ISO/IEC 27001 (cf. [39]), “Information technology – Security techniques – Information security management systems – Requirements” specifies a set of information security management requirements designed to be used for certification purposes;
- ISO/IEC 27002 (cf. ) “Information technology – Security techniques – Information security management systems – Code of practice for information security management” establishes guidelines und general principles for initiating, implementing, maintaining, and improving information security management in an organization. The power systems domain has some specifics, which are not directly considered in this specification;
- ISO/IEC TR 27019 (cf. [39]), “Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002” provides a mapping of the ISMS guidelines in ISO/IEC 27002 to the specifics of the power system domain;
- ISO/IEC 62351-1 to 10 (cf. [42]) is being standardized by the ISO/IEC TC 57 WG15 and defines data and communications security for power systems management and associated information exchange. It comprises security definitions for communication protocols, network and system management as well as role-based access control. The standard is extensible, thus allowing further parts to be added if necessary. The newest part will target the management of security credentials. Table 6 provides an overview of the different parts and their standardization status:

| IEC 62351 | Definition of Security Services for | Standardization Status |
|---|---|---|
| Part 1 | Introduction and overview | Technical Specification (TS) |
| Part 2 | Glossary of terms | TS |
| Part 3 | Profiles Including TCP/IP | TS, edition 2 is currently work in progress targeting an IS |
| Part 4 | Profiles Including MMS | TS |
| Part 5 | Security for IEC 60870-5 and Derivatives | TS, work on edition 2 targeting an IS is almost finished |
| Part 6 | Security for IEC 61850 | TS, will be updated in edition 2 to align with IEC 61850-90-5 TR |
| Part 7 | Network and system management (NSM) data object models | TS |
| Part 8 | Role-Based Access Control for Power systems management | TS |
| Part 9 | Credential Management | Work in Progress |
| Part 10 | Security Architecture Guidelines | TR |
| Part 11 | XML File Security | Work in Progress |

**Table 6: IEC 62351 parts**

- an overview of the different parts of IEC62351 is provided either in IEC 62351 Part 1 (cf. [42]) or in a TC 57 WG 15 White Paper (cf. [43]). These documents also provide an overview of security services necessary to protect against certain threats from a more general point of view and their mapping to the power domain by using IEC 62351 defined security technology;
- IEC 61850-90-5 describes the use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. It addresses security for synchrophasor communication in terms of integrity (based on HMAC) and optional confidentiality (using AES) using GDOI (RFC 6407) for key management. Note that this document is a technical report;

- IEC 61851 defines a conductive charging system and applies to equipment for charging EVs at standard AC supply voltages up to 690 V and at DC voltages up to 1,000 V. The current revision of IEC 61851 does not provide IT security measures, but defines a safe and reliable infrastructure for conductive charging, taking particularly into account the safety requirements for a publicly accessible infrastructure;
- ISO 29101 (draft) defines a privacy reference architecture. This may be considered within the FINSENY architecture providing "privacy by design".

#### 4.3.1.1 Vehicle-to-Grid communication using IEC 61851

IEC 61851 defines a conductive charging system and was standardized in 2001. The standard applies to equipment for charging electric road vehicles at standard AC supply voltages (as per IEC 60038) up to 690 V and at DC voltages up to 1,000 V, and for providing electrical power for any additional services on the vehicle if required when connected to the supply network. IEC 61851 requires a hard-wired physical control pilot conductor, which is connected through a separate cable.

IEC 61851 targets four different charging modes:

- Mode 1 (AC): slow charging from a standard household-type socket-outlet;
- Mode 2 (AC): slow charging from a standard household-type socket-outlet with an in-cable protection device;
- Mode 3 (AC): slow or fast charging using a specific EV socket-outlet and plug with control and protection function permanently installed;
- Mode 4 (DC): fast charging using an external charger.

The current revision of IEC 61851 defines a safe and reliable infrastructure for conductive charging, taking particularly into account the safety requirements for a publicly accessible infrastructure. The concept of the "control pilot", defined in the existing IEC 61851-1 as a hard-wired conductor, will be extended to other technological solutions providing the same degree of safety. The control pilot conductor is replaced with a control pilot function, which may use the carrier line signal between charging post and vehicle. Hence, an extra conductor is not necessary.

Safety measures to protect against overvoltage and over current targeting the EVSE are described in IEC 61851-1 (cf. [21]) and IEC 61851-22 (cf. [23]) for the AV charging and safety measures described in IEC61851-1 (cf. [21]) and IEC 61851-23 (cf. [24]) to protect against overvoltage and over current when using the DC charging.

| IEC 61851 ed.2 | Content | Status |
|---|---|---|
| 1 | Electric vehicle conductive charging system – General requirements | TS |
| 21 | Electric vehicle conductive charging system - Electric vehicle requirements for conductive connection to an A.C./D.C. supply | CD |
| 22 | Electric vehicle conductive charging system - A.C. electric vehicle charging station | CD |
| 23 | Electric vehicle conductive charging system - D.C electric vehicle charging station | CD |
| 24 | Electric vehicle conductive charging system - Control communication protocol between off-board D.C. charger and electric vehicle | CD |

**Table 7: IEC 61851 parts and status**

The communication between the EV and the EVSE depends on the mode applied. In Mode 1 or Mode 2 there is no communication, while in Mode 3 there is the control pilot communication, and in Mode 4 additional communication functions to allow battery management are supported. Common to all modes is that IT-security is not provided here. Nevertheless, for the vehicle integration into a smart-grid-connected charging infrastructure, (secure) communication is necessary to provide for tariff exchange, billing, and optimization of charge cost and grid load, value added services, etc. IT –security is being defined within the context of developing the standard ISO/IEC 15118 for communication between the EV and the EVSE. This standard is being discussed as part of the following section.

#### 4.3.1.2 Security in Vehicle-to-Grid communication using IEC 15118

ISO/IEC 15118 is currently being standardized in an ISO/IEC joint working group. Its main focus is the electric vehicle to charging spot interface. Communication with the backend infrastructure is not directly targeted. The specification is split into different parts, which are all still work in progress:

- ISO 15118-1: General information and use-case definition (cf. [16]);
- ISO 15118-2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements (cf. [16] and [17]);
- ISO 15118-3: Physical layer and Data Link layer requirements (cf. [18]).

IEC 15118 currently targets different profiles as there are EIM – External Identification Means and PnC – Plug and Charge, both for AC (Alternating Current) and DC (Direct Current). In the EIM profile, TLS can be used optionally, while in the Plug and Charge profile, it is mandatory. The reason is that in the EIM profile there is only a minimum set of data exchanged allowing to control the charging, where this set is investigated through safety applications to ensure that there is no deviation from an allowed set of parameters. Note that these safety measures are always in place, but also show the interworking between security and safety means.

Security is an integral part of the standard and has been considered right from the design phase. ISO/IEC 15118-1 contains a security analysis, which investigates in specific threats. This security analysis is the base for the security requirements definition targeting the specified use cases.

The security measures defined in ISO/IEC 15118-2 build upon existing standards as far as possible. The access media for AC and DC charging will be power line communication. Support of inductive charging will most likely use wireless communication. As both feature different OSI layer 1+2, security measures have not been placed here to allow a unique solution. ISO/IEC 15118-2 applies TCP/IP for the communication between the vehicle and the charging spot. Consequently, security is applied on transport layer using TLS (cf. [14]) ensuring a protected channel between both. Since ISO/IEC 15118 targets the communication between the vehicle and the charging spot, this might be sufficient at the first glimpse. But security measures on application layer have also been defined applying XML security (digital signatures and encryption). Application layer security became necessary, as the communication also targets billing and payment relevant information, which may be exchanged with the backend in case of contract base payments in case of the Plug and Charge profile. To enable contract based payments the vehicles need means for authentication, which need to be provided to the car in a secure manner, too. To enable these scenarios the electric vehicle possesses an own certificate and a corresponding private key. These security measures go beyond the communication hop between the electric vehicle and the charging spot.

Using the security approach currently proposed in ISO 15118-2 the charging process would precede as shown in Figure 17. Note that the general process has been simplified and mainly security related exchanges are shown. Note also that the application of TLS is optional in scenarios only providing basic charging functionality without any value added services.

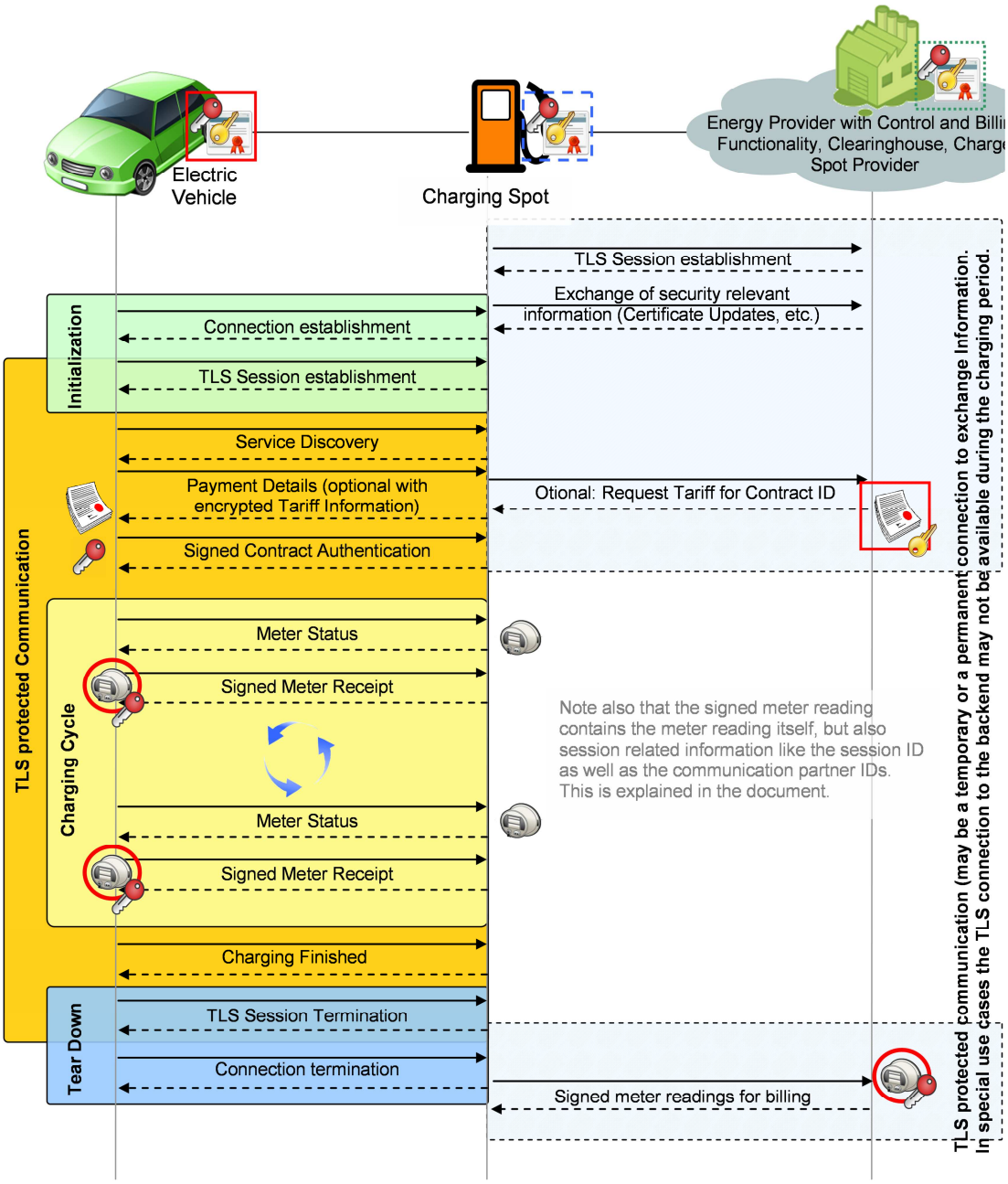


**Figure 17: Secured communication exchange using IEC 15118 for plug & charge**

The proposed security solution also addresses the online state of a charging spot to support charging spots that have very limited or even no online connectivity. In general, the charging spot is assumed to be online at least once a day. This online period may coincide with the charging period of an electric vehicle. Therefore, explicit precautions have to be given to the exchanged data, especially, if the backend depends on these.

To enable this secure transmission of data from the backend to the vehicle (e.g., credential updates or tariff information) a secret needs to be established between the vehicle and the backend allowing an end-to-end encrypted transfer. Therefore, the certificates of the electric vehicle feature static Diffie-Hellman parameters to enable an easy setup of a session based encryption key. Only the backend needs to generate fresh per-session Diffie-Hellman parameters that are used to calculate a fresh Diffie Hellman secret, which can then be used as session secret. This has the advantage that the backend can pre-calculate session keys for vehicle communication, once the vehicle's certificate is known at the backend. This approach is known from many of today's web server applications, which use the same technique.

For normal operation the vehicle certificate will be a contract based credential, thus the backend already possesses the certificate information, once the customer enrolled for a contract. For setup operation, the

vehicle may possess an OEM credential installed during manufacturing of the car and used for bootstrapping the contact based credential.

Notably, the used security mechanisms target elliptic curve cryptography (ECC) for authentication (during key management phases) and for digital signatures. The digital signature standard ECDSA based on ECC provide comparable security to RSA, but uses significantly shorter cryptographic key sizes. As the certificates support ECDSA, the Diffie-Hellman key agreement is performed in its elliptic curve variant ECDH. Moreover, elliptic curves can be implemented efficiently in hardware. As ISO/IEC 15118 targets especially electronic control units (ECU) in vehicles and charging sports, memory and calculation constraints are evident.

As described above, digital certificates for the charging spot, and, depending on the use cases, also a vehicle certificate are the base for the charging security. This requires a dedicated credential management infrastructure (Public Key Infrastructure – PKI) handling the initial provisioning, but also the revocation and update of certificates and cryptographic keys. The call flow as depicted in Figure 17 is based on the application of unilateral authenticated TLS, where the electric vehicle implements the client part. Hence, the client is required to check the certificate validity including the issuer. ISO/IEC 15118 requires vehicles to store only a limited number of root certificates to enable issuer verification. Moreover, it also allows for a limited number of intermediate certification authorities, which will not be stored in the vehicle. Besides the validity and issuer, the client also needs to check the certificate revocation state. One option to avoid the handling of certificate revocation lists is the usage of short term certificates from the server side. Another option would be the provisioning of the revocation state by the server itself, e.g., by attaching a fresh Online Certificate Status Protocol (OCSP) response to the certificate during the authentication phase. To keep a balance regarding the implementation and operational effort, the current ISO/IEC 15118 proposal features both, short term certificates for the server side certificates and OCSP responses for intermediate CAs.

#### 4.3.1.3 Securing energy automation using IEC 62351

In the context of energy automation, IEC 62351 defines explicit security measures for TCP-based and serial protocols. It applies directly to substation automation deploying IEC 61850 and IEC 60870-x protocols as well as in adjacent communication protocols supporting energy automation, like ICCP (TASE.2) used for inter-control center communication. A clear goal of the standardization of IEC62351 is the assurance of end-to-end security. The standard comprises multiple parts that are in different state of completion.

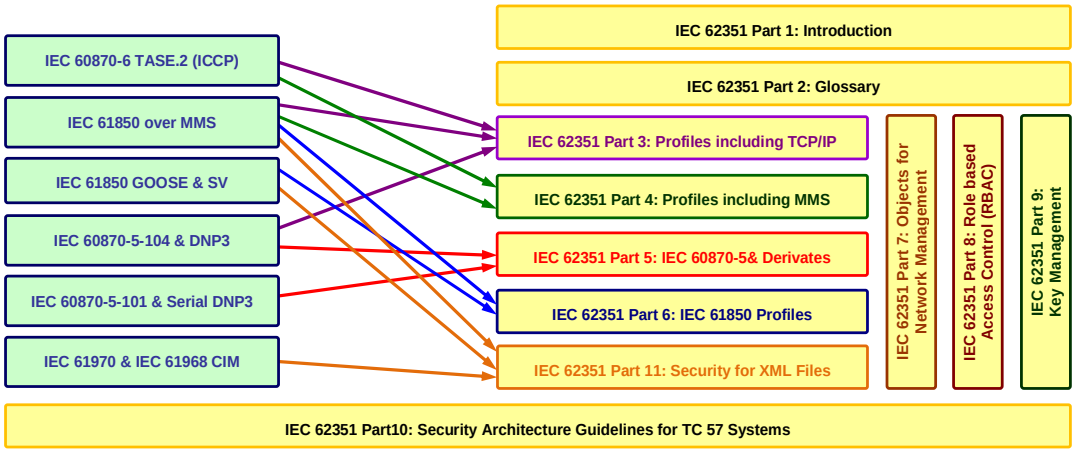


**Figure 18: IEC 62351 parts and their coverage of existing protocols (from IEC 62351-10, [32])**

While part 1 and 2 are more general and comprise the explanation of threat scenarios and the definition of terms, part 3 to 8 are directly related to dedicated protocols like IEC 61850 (IEC 62351 Part 6) and IEC 60870-5-x (IEC 62351 Part 5) and their mappings to lower layer protocols like TCP/IP (IEC 62351 Part 3) and MMS (IEC 62351 Part 4) as well as the mapping of security to the network management (part 7) and role-based access control (part 8). These parts utilize symmetric as well as asymmetric cryptographic functions to secure the payload and the communication link. The remaining part of this section provides an overview about the different parts of IEC 62351 and their current status in standardization.

IEC 62351 applies existing security protocols like TLS (cf. [14]), which has been successfully used in other technical areas and industrial applications, in different parts of the standard. The application of TLS provides for security services like mutual authentication of communication peers and also integrity and confidentiality protection of the communicated data. Thanks to the mutual authentication required by IEC 62351 attacks like Man-in-the-Middle can be successfully countered.

Part 3 of IEC 62351 defines how security services can be provided for TCP/IP based communication. As TLS is based on TCP/IP part 3 specifies cipher suites (the allowed combination of authentication, integrity protection and encryption algorithms) and also states requirements to the certificates to be used in conjunction with TLS. These requirements comprise for instance dedicated certificate context, application of signatures, and the definition of certificate revocation procedures. Part 3 is currently under review to provide an edition 2.

Part 4 of IEC 612351 specifies procedures, protocol enhancements, and algorithms targeting the increase of security messages transmitted over MMS. MMS is an international standard (ISO 9506) dealing with a messaging system for transferring real time process data and supervisory control information either between networked devices or in communication with computer applications. Part 4 defines procedures on transport layer, basing on TLS, as well as on application layer to protect the communicated information. One goal of this paper is to analyze if the defined security is appropriate especially in the context of Smart Grid applications.

Besides TCP/IP, IEC 62351 Part 5 relates to the specialties of serial communication. Here, additional security measures are defined to especially protect the integrity of the serial connections applying keyed hashes. This part also specifies a separate key management necessary for the security measures. Currently this part has been reworked. An edition 2 is expected soon.

Part 6 of IEC 62351 describes security for IEC 61850 Peer-to-Peer Profiles. It covers the profiles in IEC 61850 that are not based on TCP/IP for the communication of Generic Object Oriented Substation Events (GOOSE), and Sample Measured Values (SMV) using, e.g., plain Ethernet. Specific for this type of communication is the usage of multicast transfer, where each field device decides - based on the message type and sender - if it processes the message or not. Security employs digital signatures on message level to protect the integrity of the messages sent, to also cope with multicast connections.

IEC 62351 Part 7 describes security related data objects for end-to-end network and system management (NSM) and also security problem detection. These data objects support the secure control of dedicated parts of the energy automation network. Part 7 can help to implement or extend intrusion detection systems for power system specific objects and devices.

Part 8 of the standard is currently in definition and addresses the integration of role-based access control mechanisms into the whole domain of power systems. This is necessary as in protection systems and in control centers authorization as well as stringent traceability is required. One usage example is the verification of who has authorized and performed a dedicated switching command. Part 8 supports role-based access control in terms of three profiles. Each of the profiles uses an own type of credential as there are identity certificates with role enhancements, attribute certificates, and software tokens.

Part 9 is work in progress targeting the definition of Key Management supporting power system architectures in general and IEC62351 specifically.

Part 10 is a technical report and provides an overview where to consider security for power system architectures. It motivates the incorporation of security right from the beginning and also suggests certain security controls. The document is intended to foster the adaptation of security and thus does not provide a complete architecture, but architecture elements. Moreover, it references several other documents providing comprehensive insight like the NIST documents referenced above.

Part 11 is a New Work Item Proposal targeting Security for XML Files. The first goal here is the definition of a security tag stating the sensitivity of transmitted information. This enables the receiver to act accordingly on the data, especially, if the data is stored and processed and forwarded to others at a later point in time, when the communication channel to the source of information has already been torn down.

### 4.3.2 IEEE (Institute of Electrical and Electronics Engineers)

IEEE is an international organization providing standards and other publications. Beyond other domains the standards address areas like power and energy, biomedical and healthcare, telecommunications. The

following list of standards is considered applicable in the context proving of security enablers for FINSENY.

- IEEE 1686-2007 (cf. [44]), Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. The standard defines functions and features that must be provided in substation intelligent electronic devices to accommodate critical infrastructure protection programs. It addresses security in terms of access, operation, configuration, firmware revision, and data retrieval from IEDs. Encryption for the secure transmission of data, both within and external to the substation is not part of this standard;
- IEEE 802.1X (cf. [45]): Port Based Network Access Control specifies port based access control, allowing the restrictive access decisions to networks based on dedicated credentials. It defines the encapsulation of EAP over IEEE 802, also known as EAP over LAN or EAPOL. The specification also includes the key management, formally specified in IEEE 802.1AF;
- IEEE 802.1AE (cf. [46]): MAC security specifies security functionality in terms of connectionless data confidentiality and integrity for media access independent protocols. It specifies a security frame format similar to Ethernet;
- IEEE 802.1AR (cf. [47]): Secure Device Identity specifies unique per-device identifiers and the management and cryptographic binding of a device to its identifiers.

### 4.3.3 IETF (Internet Engineering Task Force)

The IETF develops international standards targeting protocol suites operating on different layers of the OSI stack. Prominent examples of standards relate to TCP/IP and Internet protocol suite. The IETF cooperates also with other standardization bodies like the ISO/IEC or W3C. The Internet Engineering task Force published:

- RFC 6272, “Internet Protocols for the Smart Grid,” which contains an overview of security considerations and a fairly thorough list of potentially applicable security technologies defined by the IETF;
- RFC 3711: Secure Real-time Transport Protocol (SRTP) may be used for securing VoIP communication including video conferencing or video surveillance;
- RFC 4101, RFC 4102, RFC 4103 are the base standards for IP Security (IPsec) providing Layer 3 Security, typically used for VPNs or for remote access. The listed RFCs describe general architecture as well as the two modes AH (Authentication Header) and ESP (Encapsulated Security Payload);
- RFC 4962: Authentication, Authorization, and Accounting provides guidance for Authentication, Authorization, and Accounting (AAA) Key Management and an architecture allowing centralized control of AAA functionality;
- RFC 5246: Transport Layer Security (TLS) provides Layer 4 security for TCP/IP based communication, currently used in IEC 62351. Note that there are several extensions to TLS for additional cipher suites, transmission of additional information like authorizations or OCSP responses and so on. These extensions are not listed here explicitly;
- RFC 5247: Extensible Authentication Protocol (EAP) provides a Key Management Framework for EAP. Single EAP methods are defined in separate RFCs. EAP is typically used for controlling device (or human) access to networks;
- RFC 5746: Datagram Transport Layer Security (DTLS) provides Layer 4 security for UDP/IP based communication. May be applied in scenarios, were TLS is not applicable;
- RFC 6407: Group Domain of Interpretation (GDOI) defines group based key management, currently used in IEC 61850-90-5.

### 4.3.4 W3C (World Wide Web Consortium)

The W3C develops and maintains standards to be used in web environments and provides a foundation for web services defined by OASIS (SOAP and XML). Some of the W3C standards likely to be used in Smart Grid environments also incorporate security:

- XML Signature (cf. [48]) defines a mechanism by which messages and message parts can be digitally signed to provide integrity, to ensure that the data is not tampered with, and authentication, to verify the identity of the message producer. The document is currently being updated (cf. [49]), e.g., to enhance the supported algorithms with elliptic curve based cryptography;
- XML encryption (cf. [50]) allows the transport of information in a confidentiality protected way. The document is currently being updated (cf. [51]), e.g., to enhance the supported algorithms with elliptic curve based cryptography.

## 4.4 Security elements (general view)

### 4.4.1 Encryption

Encryption is used to achieve the confidentiality of data. The process consists in the encryption (transforming plaintext information to make it unreadable except to those possessing special knowledge), and decryption (the reverse process, where encrypted data is transformed back to plaintext).

There are a lot of algorithms that have been provided in order to achieve encryption. They can be distinguished between two main areas: symmetric-key cryptography and public-key cryptography. Symmetric-key cryptography refers to methods where the person that encodes and the person that decodes the data share the same key (or related in an easy way). DES or AES are typical widely used algorithms relying on symmetric-key cryptography.

In public-key cryptography, the public key may be freely distributed and is paired with a private one which must remain secret. The public key is used for encryption, and the private one for decryption. RSA or ECIES are typical algorithms implementing asymmetric cryptography.

### 4.4.2 Entity authentication

Within the Smart Grid (and elsewhere) it is often very important to assure one entity of another entity's claimed identity. It is for instance not acceptable that everyone is able to log into a console and sent arbitrary control messages. Thus the entity that wants to use the console has to verify her or his identity beforehand. This and the like is called entity authentication. Besides authentication of humans, authentication of devices is often needed as well, especially in device-to-device communication scenarios.

Apart from entity authentication another important type of authentication is message or data origin authentication that is used when messages are exchanged between parties A and B and delays may take place. This is handled in section 4.4.3.

Entity authentication in general is a two-step process. The first step is to claim a certain identity. The second step is to verify the claimed identity using evidence created with active involvement of the claimant. Thus one could say that

Entity Authentication = Identity Claim + Active Verification

After party A authenticated party B, party A knows with some certainty (specified by the authentication process itself) that it really communicates with party B and not an impostor. If next, party B authenticates party A as well, this is called mutual entity authentication. Subsequent communication in (almost) real-time is afterwards based upon the previous (almost) real-time authentication. To assure timeliness of authentication, it may be necessary to repeat the process. To avoid such repetition the authentication process can be extended by negotiation of session keys used to secure the subsequent communication session.

As the first step of entity authentication is to claim an identity, some kind of identity management is needed as a prerequisite. The identity management may not only provide rules for assigning identities, but may as well attach attributes to identities that are later on used for authorization and it may even comprise access management. Further details on identity management can e.g. be found in section 4.1.2.

Entity authentication as a building block can be used to e.g. control physical or logical access to all kinds of resources. As different environments and types of access provide different possibilities to execute the

process of authentication a great number of different authentication options are present today providing different levels of certainty concerning the result of the authentication process. This subsection describes such authentication options.

In general there are three main categories of authentication that are differentiated by the means that are used as basis to prove the identity claim. These categories are

a) "Something the claimant knows"

   This category comprises e.g. passwords, the most commonly used means of verifying an identity within IT systems, but also includes personal identification numbers (PIN), transaction numbers (TAN), whole passphrases or question & answer processes as well as cryptographic secrets or keys e.g. used within challenge and response protocols. At the heart of the process lies some secret knowledge that is bound to the entity's identity.

b) "Something the claimant has"

   This category is mainly about a hardware token only the claimant is able to present and that can in turn be used in another automatic process to decide whether the token assures an identity or not. Examples are identification cards, passports, ATM cards, credit cards, or generally tokens. They may incorporate electronic means or not and range from a piece of paper to intelligent devices like smartphones. Concerning device authentication this category is only artificially applicable.

c) "Something the claimant is"

   Regarding authentication of humans this category makes use of unique ways of physical or behavioral characterizations of humans like fingerprints, retina images, handwritten signatures, or voice patterns. These in turn fall into the category of biometrics. Physical unclonable functions (PUFs) can be seen as an equivalent for devices.

One prominent authentication process for humans today, a smartcard together with a PIN, combines category a) with category b). The claimant not only presents a smartcard to be used for authentication within the system, but a PIN as well to make sure that the smartcard can only be deployed, if the entity presenting it, knows a secret that can be verified by the token internally. Such processes using two different authentication processes are called two-factor authentication.

Whenever cryptographic keys are used for entity authentication, key or credential management becomes an important aspect as well. Some options need for instance a whole PKI based upon on X.509 certificates in place. Others may be less demanding, but may not provide all the pros provided by a PKI.

The following subsections will elaborate further on the already given and some other authentication options.

#### 4.4.2.1 Options for human to human authentication

When humans authenticate each other they mostly use biometrics and they use it subconsciously. As a prerequisite they have to be introduced beforehand or they have to meet each other in a given context. A lot of authentication is done this way. Humans that do not know each other beforehand and need some authentication process may use (the non-electronic part of) identification cards.

##### *4.4.2.1.1 (Non-electronic part of) identification card*

An identification card is issued by an authority that is trusted within a given user group. Before issuance an agreed upon enrollment process is used that in turn includes some kind of authentication (the root of all of this e.g. being a birth certificate). When the identification card is later on used for authentication, the authority is known from the optically readable content of the card. The card itself has to have some so-called document security properties (testable by humans like a hologram) if easy copying of cards shall be prevented. An identity of the holder of the card can be obtained by reading the card as well. If the holder of the card shall be bound to the card, a facial image is printed on or connected to the card. The active part of the cardholder consists of presenting the card, knowing its content and being actually there.

#### 4.4.2.2 Options for human to device authentication

Like within human to human authentication, human to device authentication always needs an application, enrollment and issuance process as a first stage of a whole lifecycle management of the authentication process as well. Representing the three above mentioned categories of authentication the following

subsections shortly discuss “user ID and password”, “token” and “biometrics” in the context of human to device authentication.

#### *4.4.2.2.1 User ID and password*

If a human wants to authenticate to a device, a widely used process is based on “user ID and password”. The user has to acquire some user identity (user ID) that can be given as input to the device together with an initial password that should be changed to a new user chosen password after the first authentication took place. This user ID may later e.g. be used for authorization. The system restricts the number of possible failed login attempts, for instance over some time period, to make password guessing improbable. The device needs access to a database or file that maps user IDs to passwords in a way that the passwords cannot easily be stolen and used, but can easily be checked. Hashing of passwords and shadowing of password files is the usual way to implement this. If a password file gets stolen, it is almost always possible to execute brute force attacks against it, i.e. attacks that essentially try every password possible. Passwords that appear in dictionaries will easily be found by such an attack. If passwords are well chosen (e.g. randomly), have sufficient length and are only known to the user, user ID and password achieves a good level of security. To enforce more randomly looking passwords, the functionality for password changing is often linked to some password policy that describes rules like “choose at least one special character”. Unfortunately users are not good in remembering random or random-like passwords and, if they are allowed, often choose easily guessable ones or even write them down and do not hide such notes appropriately. If a password has been forgotten, e.g. because it is not used very often, this means that there must be a process to reset it to a new initial value.

#### *4.4.2.2.2 Token*

Another means for entity authentication is to use a token. Such tokens are either realized as hardware tokens or in software. They contain secret or private keys usually together with verification authentication data for access control. The keys are used in specialized authentication protocols on behalf of the user.

Software tokens are specially designed data structures that incorporate their own mechanism to control access to the secret that is stored by the token. Such tokens are usually encrypted and a password is needed to decrypt and use the secret contained in the data structure. A PKCS#12 file (extension .p12) is an example of such a token. They are often called Personal Security Environments (PSE or soft PSE) as well. Kerberos access tokens do not fall into this category as they are only the result of an authentication process that may in turn be built upon software tokens. Kerberos authentication itself is based on passwords or public keys (see PKINIT [63]).

Hardware tokens are small hardware devices that can be easily carried around and have storage and/or computing ability on their own. This ability is used to control access to a system based upon a secret only known within the token’s environment. To avoid that loss of the token leads to easy misuse of the system, access to the token may in turn be controlled by the token itself e.g. via a so-called PIN (Personal Identification Number) or a password. Examples of tokens are a smartcard or a USB token that integrates a security access module. Tokens range from easily readable to specially secured and controlled.

A very special kind of token in this context are physical keys without any electronic parts that may be bound to humans by organizational measures, but do not carry any identification information by themselves. In combination with an electrical keylock, access to devices may be regulated using such tokens as well. But as no real verification process is possible when using physical keys, they somehow fall out of this chapter and are anyway primarily used for physical access control.

Tokens that have computing ability can be used as the so-called prover in sophisticated authentication protocols. The system acts as a verifier and challenges the prover in a way that the token can only give correct answers if it is able to access a specific cryptographic secret. Essentially, knowledge of this secret gets verified.

Token solutions always need proper processes in place for applying for a token, issuing a token, revoking a token etc. This means a proper life-cycle management has to be set up that controls the issuance and operation of token.

If tokens with computing ability are used, all or parts of the authentication protocols are provided by the token. There are numerous authentication protocols in use today. Some of them are proprietary, others are standardized. They use different cryptographic algorithms that may e.g. be based upon modular exponentiation of integers or upon elliptic curve point addition. The interface that is required and the computing ability that is available at the host always have to be considered when choosing a token.

Furthermore such protocols use special data or keys for the verification process that are to be kept secret. If symmetric cryptography is used, the host needs to securely store his copy of the secret as well. If asymmetric cryptography is used, the host only needs the public part of a corresponding key pair used by the token. This public part is to be stored with integrity protection in place.

Another important aspect concerning hardware tokens is their communication interface. Current realizations implement contact-based, contactless and dual-interface communication solutions. The following two subsections will shortly discuss contact-based and contactless tokens. Dual-interface tokens combine both types of interfaces into one chip.

##### 4.4.2.2.2.1 Contact-based

Contact-based solutions are mainly smartcards or wired USB tokens, whereby some USB tokens are just realized as USB smartcard terminals that use ID-000 sized smartcards (SIM card dimension). Others provide their own security controller environment for internal use. The communication interface of smartcards is standardized within ISO 7816 [108]. Contact-based protocols like T=1 or T=0 are used to transfer so-called APDUs (Application Protocol Data Unit) that are interpreted as commands by the smartcard resulting in a response APDU. USB tokens use packet based communication as defined by the USB industry standard (www.usb.org).

On host side the corresponding interface has to be available as well as middleware and/or applications able to communicate with the token and to support the authentication protocol as well as the PIN or password verification methods used by the token.

##### 4.4.2.2.2.2 Contactless token

Contactless solutions are for example RFID, NFC or wireless USB tokens. Going exemplary into some detail, an instantiation for RFID tokens may be smartcards offering an ISO 14443 A or B interface (cf. [96] to [100]) for communication together with the T=CL protocol for transfer of APDUs. But this is just one example out of a wide spectrum.

Concerning the host side, almost the same as for contact-based tokens holds. As an addition it has to be guaranteed that the air interface does not interfere with other functionality within the environment it is used.

#### *4.4.2.2.3 Biometrics*

If biometrics shall be used for entity authentication, options that might be taken into account are for example voice recognition, fingerprint recognition, facial recognition, retinal scan, vein recognition, keyboard typing, or sensing handwritten signatures. All possibilities have different pros and cons that have to be considered when choosing a solution. Important aspects in the context of biometrics are false acceptance and rejection rates. Also important are the aspects of special enrollment requirements and that not everyone can always be enrolled. Privacy considerations are to be considered here as well.

The host side always needs a special device capable of creating a set of digital data that characterizes the biometric used. Special processing of this data may be needed as well.

### 4.4.2.3 Options for device to human authentication

Device to human authentication is e.g. useful when a technician shall replace an original sub-module of a complex electronic system by another original to preserve liability. One option is equivalent to non-electronic identification cards. Another option is electronic product authentication supported by special hardware usable by the human who wants to authenticate the device.

#### *4.4.2.3.1 Appearance*

To base device to human authentication on appearance is equivalent to identification cards. The only prerequisite is a trusted source of information providing characteristics of a device that can be validated by humans. Features like holograms that cannot be detached without damage and free of residues may be used as a tool to support the authentication process.

#### *4.4.2.3.2 Electronic product authentication*

If appearance is not enough, processes using electronic devices, e.g. so-called tags or PUFs, may be used to verify the origin of a product and maybe its unique serial number representing another identification of the device. Such solutions need some electronic counterpart that may easily be applied by humans to validate the tag, e.g. a mobile tag reader. PUFs are shortly discussed in section 4.4.2.4.2.

#### 4.4.2.4 Options for device to device authentication

Device to device authentication is needed as an anchor for secure communication between devices. It is a fully electronic process relying on secrets stored or characteristics provided by the device. Both options are used to execute authentication protocols. As always, storage of secrets has to be realized as secure as possible.

Within environments that call for device to device authentication, usually topics like auto-configuration or secure credential bootstrapping become important as well. They are to be implemented by the devices and/or handled within the devices' lifecycle management.

##### *4.4.2.4.1 Cryptographic keys and SAMs*

Usually cryptographic keys are used as secrets for authentication protocols. These secrets may be derived from passwords or by fully random processes. To preserve secrecy they may be stored in so-called Security Application (or Access) Modules (SAMs) that provide specially designed countermeasures against extraction. Security controllers that are used within smartcards can e.g. as well be used within SAMs.

Commonly used cryptography often requires a lot of time and space from its computing environment. As environments like the (smart) grid do in turn have many resource constraints caused by the use of special purpose embedded systems, research on new cryptographic algorithms started to reflect these circumstances several years ago. The resulting class of cryptographic algorithms and protocols that can be chosen from is called Lightweight Cryptography. If no such resource constraints exist, an implementer may choose from a huge set of long-time available protocols, but is better advised to realize standardized protocols than proprietary solutions.

##### *4.4.2.4.2 PUFs*

A PUF can be seen as biometrics for devices. PUF is sometimes written out as Physical Unclonable Function and sometimes as Physically Unclonable Function. A more precise way would be to call it "(Physical) Function that is Physically Unclonable" or shorter "Unclonable Physical Function". A PUF may be defined as a sum of the following attributes: "is a physical object" plus "behaves like a function" plus "offers uniqueness" plus "makes it hard to create a physical clone". The function can then be used within an authentication protocol. The easiest instance of such a protocol needs access to the device's PUF during initial enrollment to execute the function on random inputs and store the results in a central database. Later on if the device shall be authenticated one of the inputs is chosen from the database and the PUF is executed using the device again. If the response can be validated as correct using the stored counterpart from the database, authentication succeeds.

### 4.4.3 Message authentication

If messages are exchanged within the Smart Grid (and elsewhere) it is often a requirement to have some assurance about the sender of the message, i.e. party A wants to be assured that message M really comes from party B when only examining the message and without any challenge and response mechanism that needs party B to become active at the time of processing the message. This is called message or data origin authentication.

Another important type of authentication is entity authentication that deals with the problem of assuring the identity of an entity that participates actively in the process. This is handled in section 4.4.1.

Message authentication within ICT networks is based upon symmetric or asymmetric cryptography:

- symmetric cryptography is used to send a so-called message authentication code (MAC) alongside the message. The message authentication code is bound to the message and can only be created and verified by the communicating parties. The sender of the message is either known within the given context or the claimed identity of the sender is part of the message as well. The MAC is based upon some secret key only known to the parties that shall take part in the communication;
- asymmetric cryptography is used to send a so-called digital signature alongside or within the message. Again the sender is either known by context or includes its identity claim. The signature is created by using the private part of the sender's key pair and gets verified by using the corresponding public part.

The following subsections discuss the above mentioned options (MAC and Digital Signature) in more detail.

#### 4.4.3.1 Message Authentication Codes (MAC)

A MAC function can also be called keyed cryptographic hash function. It is based on symmetric cryptography and essentially uses a secret key and an initialization vector to build a unique cryptographic fingerprint of the message. This cryptographic fingerprint can only be verified if the corresponding secret key and initialization vector (IV) are known by the verifier. After sender and receiver agreed upon the secret key and IV, the sender computes the MAC and sends it alongside the message. The verifier takes the actually received message and computes the corresponding MAC himself. If it matches the received MAC, data origin, which also implies integrity, of the message is proven. Assumed that the secret key does not leak, only the sender and the receiver are able to produce the MACs in question.

Key management for message authentication codes can e.g. be realized by incorporating a key derivation mechanism into the entity authentication phase of a protocol. The derived key is later on used to create the MACs.

#### 4.4.3.2 Digital signatures

Digital signatures that may as well be used for message authentication are based upon asymmetric cryptography, i.e. cryptographic functions that rely on so-called public/private key pairs. The private part of the key has to be kept secret by its unique key holder who acts as the sender of a message. The public part is given to all possible receiving parties. Each receiving party has to assure itself about the genuineness of the public key, i.e. whether it really belongs to the party it is mapped to. The private key is used by its key holder to compute a digital signature of a message. This process is again based upon some cryptographic hash function that uses the message as input. The (unkeyed) hash then gets processed by a function that uses the private key as another input. After receiving the message and its corresponding digital signature, the receiver computes the hash of the message using his own resources. After that he processes the digital signature using the public key of the sender to re-produce the sender's hash. If both hash values match, data origin and thus integrity of the message are proven.

Digital signatures may e.g. be used within the following well-known protocols respectively message formats:

- S/MIME (PKCS#7);
- OpenPGP;
- XML-DSig.

Such protocols or message formats often rely on so-called X.509 certificates that can be used to publish and validate public keys. Public-Key Infrastructure is the keyword for this.

### 4.4.4 Authorization

Authorization in combination with access control basically means definition and enforcement of access policies. The access control process is based upon entity authentication, which is used to first detect who wants access to a resource. Then it uses the previously defined access policies to decide whether access may be granted or not, i.e. whether the subject is authorized to take an action or not. The simplified architecture as depicted in Figure 19 shows the most important aspects of authorization and access control.

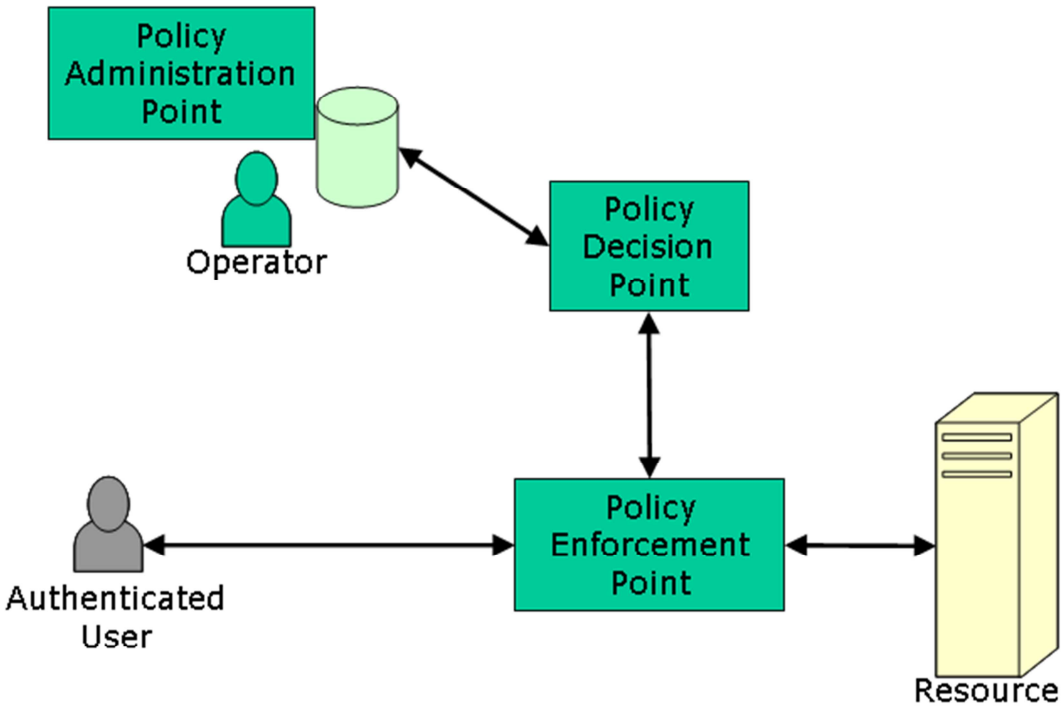


**Figure 19: Authorization and access control - Simplified architecture**

An operator starts with defining access policies by using a Policy Administration Point. The access policies contain user identities and corresponding access rights. If a user tries to access a resource, a policy enforcement point transparently communicates with a policy decision point to get a decision whether the user is allowed to access the resource. The policy decision point in turn searches the access policies for authorization information. If needed, a prior authentication has to be done as well.

Operating systems often use mandatory access control (MAC) or discretionary access control (DAC), whereby only discretionary access control allows passing of permissions from one subject to another. Access control lists are used by DAC to e.g. assign read/write/execute permissions to files. As often the same access profile shall be mapped to many different users and as it gets quite ineffective to manage full user/resource matrices, access policies use concepts like groups or roles to effectively realize authorization in multi-user/multi-resource environments. One such concept is called role-based access control (RBAC). Within RBAC, roles specified by a certain set of permissions can be assigned to subjects that are thereby authorized to exercise these permissions. RBAC can e.g. be implemented as MAC or DAC. RBAC can as well be used to define permissions on specific operations that have some application context whereby traditional DAC is restricted to low-level data objects.

To be able to re-use authorization decisions within complex IT infrastructures, access management systems assign special authorization token to users that later on are used transparently to reduce communication complexity within the access control infrastructure. Well-known examples for such systems are SAML or OpenID. A system that uses similar tokens, called tickets, is Kerberos, which is nowadays e.g. widely used within Microsoft Windows domains.

Whatever technical solution is chosen for authorization and access control, it is always important to adhere to the principle of least privilege. Operators that define access policies should always keep in mind that subjects should be restricted to the rights necessary for their legitimate purpose.

### 4.4.5 Data integrity

Integrity of data in digital security is an assertion that no one has tampered with data over its entire life cycle. It means that the data is complete, whole, not modified deliberately or not, compliant with the intension of the creator of the data; an intruder should not be able to substitute a false data for a legitimate one. It relates to data in transit and locally stored data.

In case of transmitted data it assures the sender and the receiver that every bit produced by the sender is received by the recipient in precisely unaltered form. Concerning stored data it means preventing accidental or deliberate but unauthorized insertion, modification or destruction of the data.

Integrity of a transferred data involves:

- compression of the data (message) to be transferred
- encryption of the compresses string
- sending the resulting string together with the plain data to the receiver.

The receiver repeats the compressing and subsequent encryption of the plain data and compares the result with the one created by the sender (originator).

For data compression secure hash function is used. A secure hash function is a one-way function, so no invert function can be computationally derived in a specific time frame. Additionally, it must be computationally impossible to construct another input message which hashes to the same result as the original sent message, or in general, the function must be collision-free, i.e. it must be computationally infeasible to construct two distinct input messages which hash to the same result. The most widely used hash functions belong to SHA-1, or MD5 (MD4, SHA2, SHA3 can be used as a less strong alternative).

The encryption of the compressed plain data can be provided by either a symmetric or an asymmetric scheme. With the symmetric scheme, compression and encryption of data may be processed simultaneously. For that purpose MAC functions can be used, which implies that the sender and receiver of a message must agree on the same key before initiating the communication. However, if the key used for encryption is the sender's private key, the mechanism provides digital signature and not only data integrity, but also the sender's authenticity is proved. Of course, in that case the message's receiver first decrypts the message and then compresses it.

As together with the encrypted part the plain text is sent too, the mechanism provides message integrity, but not confidentiality.

The same mechanisms can be used for integrity of stored data, but to allow integrity check of the data by any authorized entity, the data should be encrypted by a secret key of the data originator.

### 4.4.6 Non-repudiation

As message non-repudiation means that the sender of a message cannot later deny having sent it, there needs to be provided a proof of the transferred data integrity and origin. The integrity of the data can be provided in the way described above. However, integrity is not sufficient as the message could be tampered through a man-in-the-middle attack. Therefore it is necessary to guarantee that the message is the one that was originally sent by the communicating party what can be done by the sender signing the message with his digital signature.

Not to be able to repudiate a signature presents a challenge to the trustworthiness of the signature itself. The standard approach to mitigating this risk is to involve a trusted third party which verifies the authenticity of the signature by issuing a digital certificate to which the digital signature belongs. This way the recipient of the message has the ability to verify the origin of it even if no direct exchange of the public information with the sender has ever been made.

The digital origin of sent messages means only that the certified/signed data can be, with reasonable certainty, trusted to be from somebody who possesses the private key corresponding to the signing certificate. If the key is not properly protected by the original owner, digital forgery can become a major problem. To mitigate the threat it is important to revoke a certificate any time when there is a suspicion that the private key has been stolen. A good practice is:

- periodical update of devices cryptographic keys, especially keys of unmanned field devices.
- in case of human personnel, usage of personal cards which never allow the key to leave the card, and the personal identification number (PIN) code necessary to unlock the card for permission to use it for digital signatures.

### 4.4.7 Transaction security

Within FINSENY transaction security has been identified as a requirement for the electronic market place for energy (eMarket4E). The term transaction itself can have many different meanings. Within business administration it describes a transacted business agreement or exchange. Within computer science it is a sequence of operations that are to be executed as a whole. The eMarket4E results in business agreements between e.g. an energy supplier and a consumer. To achieve this, it uses a sequence of requests and responses on an electronic market place. The service operator that offers the market platform for

negotiations needs to guarantee an environment where no party can deny the result of the transaction after it took place. This should be handled by organizational and technical measures able to achieve a high level of transaction security.

Financial markets today and online payment is to some point comparable to the eMarket4E when opened up to prosumers. Transaction security naturally plays a vital part of financial transactions over electronic networks as well. Thus existing solutions for the financial sector can be used to study possible solutions for the eMarket4E. Two such solutions that are shortly discussed in the following are SET and 3-D Secure:

- SET (Secure Electronic Transaction).

  SET has been proposed during the nineties as a protocol for secure credit card transactions. Its development was led by Visa and MasterCard but companies like IBM or RSA participated as well. SET was planned to become a de facto standard, but failed mainly because of its complexity and costs. SET provides confidentiality and integrity as well as cardholder account and merchant authentication.

  Its security is based upon X.509 certificates with special “electronic wallet” extensions and so called “dual signatures”. Dual signatures link together two messages intended for two different recipients and thus separately encrypted by using their respective public keys. The link is established through incorporating the hash of the one encrypted message into the digital signature of the other message as well. Each recipient verifies the signature by taking the hash of the other message into account without knowing the message itself. Thus from an application perspective privacy can be preserved by separation of order and payment information. The merchant only gets to know the order while the credit card company only gets to know the payment information that includes the credit card number. Nevertheless both messages are cryptographically bound together and cannot be denied by the customer as he created the digital signature. If the payment is accepted by the credit card company the merchant may ship the order.
  The security protocols used for SET are essentially SSL and S-HTTP.

- 3-D Secure.

  3-D Secure has been developed by Visa and has been deployed by e.g. Verified by Visa or MasterCard SecureCode.

  It is an XML-based solution that uses messages sent over SSL/TLS channels. After an order has been placed, 3-D Secure adds a special authentication step for the purpose of online payment by integrating a redirection (using pop-up windows or inline frames) to an issuing bank for authorization of payment. The issuing bank may then use a customer authentication method of its choice, which is typically password-based, to authorize the transaction. From the issuing bank perspective it is seen like entering a PIN at an ATM. The merchant never sees the authentication process. In essence each transaction consists of two request/response pairs, the original request/response and the authorization request/response. The actual transaction only takes place if the payment authorization ended successfully. Because of its redirection technique 3-D Secure is not without critics. To reduce the risk of phishing, display messages (a special message chosen by the customer during registration) are for instance used by Verified by Visa.

Other, more generic, solutions that may be deployed in the context of the eMarket4E are Electronic Data Interchange (EDI/EDIFACT)[1] or Electronic Business using eXtensible Markup Language (ebXML [70]). The latter can eventually be integrated with WS-Reliability [71] or WS-ReliableMessaging [72]. Both claim to achieve Web Services Reliable Messaging.

- EDI/EDIFACT is used for electronic exchange of business data between enterprises based upon domain specific agreements (de facto standards or standards). Such agreements may be stipulated between business partners or rely on national or international standards. They may be very specific to the application domain. The predominant European EDI system is called UN/EDIFACT, the “United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport” (cf. http://www.unece.org/trade/untdid/welcome.html), which is also

[1] Although „electronic data interchange” (abbreviated as EDI) can be used to classify all mentioned solutions, the term EDI is restricted within this document to solutions like EDIFACT.

standardized as ISO 9735 (cf. http://www.gefeg.com/jswg/). The following parts of ISO 9735 are especially concerned with EDI security:

- ISO 9735 part 5: “Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)”;
- ISO 9735 part 6: “Secure authentication and acknowledgement message (message type - AUTACK)”;
- ISO 9735 part 7: “Security rules for batch EDI (confidentiality)”;
- ISO 9735 part 9: “Security key and certificate management message (message type - KEYMAN)”.

- ebXML, that was designed as a counterpart to EDIFACT, is a framework developed to support electronic business processes based upon the eXtensible Markup Language (XML).
- WS-Reliability “is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering” ([71], abstract).
- WS-ReliableMessaging “describes a protocol that allows messages to be transferred reliably between nodes […] in the presence of software component, system, or network failures” ([72], abstract).

From all the reported examples it can be realized that transaction security may be supported by protocols such as HTTPS (SSL/TLS) or S-HTTP. It can take advantage from digital signature schemes and needs some acknowledgement scheme, e.g. cryptographic binding of request and response, as well. Full integration of all security requirements at the application layer like in EDIFACT is also possible.

From the eMarket4E point of view the special requirements for transaction security should be formulated in full detail before a solution is specified or chosen. As a starting point RFC 2084 (Considerations for Web Transaction Security) could be used as a source of information concerning special requirements for transaction security (in this case in the context of HTTP).

### 4.4.8 System protection components

Various systems components can be used to protect a system. User / component management and authentication are explained in 4.4.2.2. Anti-malware, antivirus and anti-spyware tools are now common in personal computers, but it gets more complicated when dealing for example with SCADA systems.

Firewalls are used to deny network transmissions based on specific rules, typically used to protect networks from unauthorized access, or non-legitimate use, while authorizing legitimate communications to pass. They can be used in accordance with Intrusion Detection and Prevention systems, that can be used both at the host and at the network level, which monitor network and / or system activities in order to detect malicious activities (based on pattern recognition or anomaly detection); further activities include logging and reporting intrusion events or malicious activities, as well as blocking the originator of the suspicious events so that s/he cannot harm the system or, at least, limit the damages to a small geographical area or a small set of devices.

### 4.4.9 Logging and audit

Logging and auditing functionalities are crucial for a secure Smart Grid infrastructure. A system must be put in place to consolidate all of the log data recorded by devices having appropriate resources for logging in order to achieve a detailed understanding, traceability, and reaction to unexpected and possibly harmful events.

When developing an effective logging and auditing strategy, it is important to first define the logging and audit policy. Lifetime and maximum storage size of log files is to be specified, including ways to handle overflows. The types of security events to be recorded in the security event logs of devices have to be specified within the logging and audit policy. Systems can be monitored for security breaches on network, server and application, and process-specific levels. Event categories may be for example logon events, object access, process tracking, policy changes, account management, system events…

Logging and audit policies also typically include statements about the location of logging data, the logging format, and the managements of access rights.

As an example of logging and auditing best practices, the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) [78] require audit records to contain:

- the date and time of the event's occurrence;
- the unique ID of the user creating the event;
- the type of event;
- the success / failure of the event;
- the origin of the event (user, system,…);
- the name of the accessed object (file, process,…);
- a description of any security database modifications.

Security event auditing does not only involve the collection and logging of system events, but also the analysis of their impact in relation with the logging and audit policy. Such security audits should be carried out regularly in order to identify vulnerabilities, suspicious activities, unauthorized access attempts, and security breaches and take appropriate measures against them.

The Smart Grid logging and auditing infrastructure should fulfill the following requirements:

- it should be able to operate across the Smart Grid distributed networks and collect secure logging events. A critical aspect of any logging and auditing system is hereby the support of accurate time stamps. Thus, network time synchronization is an essential feature;
- it requires enough computational resources to handle and produce the expected large amounts of log data without affecting the operation of devices and networks;
- logging data shall be kept for the retention period stated in the audit policy and in compliance with relevant laws and regulations (e.g. data privacy protection laws);
- logging itself also requires to be protected. Depending on the component providing the logging information, this protection may vary from source authentication, integrity protection up to confidentiality. For instance, access must be limited to authorized administrators and privacy related logging data must be protected in a way that they are not editable and not erasable even if the data subject (end user) withdraws his permission for the processing of his personal data.

The steps necessary to implement a logging and auditing infrastructure include:

- identifying critical components and defining the logging and audit policy;
- evaluating the amount of log data to plan enough network bandwidth and storage resources;
- providing administration staff with security and forensic analysis experience for logging and auditing operation, including the information to be reported, archiving processes, and reaction procedures to possibly harmful events.

However, it is very unlikely that the analysis of log data in such complex systems and networks as in Smart Grid scenarios can be done entirely manually. It will surely require monitoring tools to perform cross-platform query and reporting. Such tools are usually also able to react automatically locally or remotely (user logoff, system shutdown…) or to send administrators notifications or alerts (mail, SMS, alert on screen, sound…).

Logging and auditing are commonly required by data privacy protection laws.

### 4.4.10 Data backup and recovery

Data backup and recovery is the process of making copies of data which may be used to restore the original state. Its primary use is after data loss (because of data deletion or data corruption), but backups can also be used to recover data from an earlier time.

Typically, data can be stored on several kind of medium, depending on its use and importance. Magnetic tapes have long been the most used for data backups, optical storage (DVDs for example), hard disks or remote backup services are also used. The main criteria to take into account when backing up data are:

- performance impact (and especially the time when the backups are done, also called backup window)

- software and hardware costs
- network bandwidth (for remote backups)
- security of backuped data (access control, integrity, localization…)

The data recovery is the process performed when restoring a previous state from backup data. Specific action plans are needed to efficiently and correctly achieve it. The recovery point objective (RPO – describes the age of the data that can be restored) and recovery time objective (RTO – defines the time it takes to recover from the time the disaster has been declared to when the system is back available) are the key metrics.

### 4.4.11 Observation of policies and laws

For each Smart Grid utility, all applicable policies and the policies of its major business partners must be observed, as well as the relevant legislation and regulations.

Compliance must be enforced by organizational and/or technical measures, like e.g. policies and awareness training, regular security or data protection audits including vulnerability scans. Non compliance may result in the banning of the utility from the Smart Grid network, which would result in business loss.

Examples for such issues are the compliance with data privacy protection laws and regulations, as described in chapter 4.2.6 or with encryption laws.

Indeed, the export of cryptographic software, especially encryption software, is strictly regulated individually by each country. A manufacturer of hardware/software including cryptographic functions must comply with these regulations.

Let us take as an example a tool for digital signature and their verification from Germany to another country, implemented on the basis of Microsoft .NET framework. In such a case, both German and US export regulations would have to be complied with; given that the usage of the .NET framework implies that an amount of more than 25% of the software has US origin. According to the US guidelines, cryptographic software is subject to the Export Administration Regulations Database [79] by category 5D (software).

Some countries (e.g. Austria, Finland, France, Germany, Spain, United Kingdom, United States…) committed to the Wassenaar arrangement [80] containing uniform regulations for all members summarized in a commerce control list. This list specifies amongst other things the export rules for security products – called the “Dual-Use List Category 5 - Part 2” [81] and explains which kind of cryptography is restricted for export. Any cryptographic function other than authentication or digital signature is controlled if it is a:

- symmetric algorithm with key length greater than 56 bit;
- asymmetric algorithm based on:
  - factorization of integers and modulus is greater than 512 bit;
  - computation of discrete logarithms in a group Z/pZ, where the modulus is greater than 512 bit;
  - computation of discrete logarithms in a group not Z/pZ (e.g. elliptic curve group), where the modulus is greater than 112 bit.

Decryption algorithms are under export control in the same way as encryption algorithms.

Moreover, exporting cryptography from Germany to other countries, for example, is subject to different restrictions depending on the destination country. Most products which are subject to export regulations have so-called “reasons”, why they are regulated. Cryptographic software is controlled due to reasons NS (National Security), AT (Anti-Terrorism) and EI (Encryption Item):

- rxport back to the United States: Exporting cryptography containing US parts back to the United States underlies no restrictions;

- rxport to Canada: Canada is explicitly excluded from all control reasons. No export restrictions exist, no export licenses are required;
- rxport to terrorist-supporting countries: These countries are Iran, Cuba, North Korea, Syria and Sudan. Export of cryptography is forbidden;
- rxport to all other countries: Licenses have to be acquired for reasons NS column 1 and EI (in the country chart). For all countries license exceptions are possible. In §740, supplement 3 [82], countries are listed, for which the review process of encryption software is less stringent than for those which are not listed there. License exceptions can be acquired more easily, too;
- currently in §740, Supplement 3, the following "good" countries are named: Australia, Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom.

In Germany, any open source software is completely excluded from export regulation. This might not be the case in other countries (e.g. USA).

This security element strongly depends on the final functional architectures of the work packages and therefore needs to be described in further details once these are available. Besides, it also requires that accountability shall be assured. In other words, the identification of the person/entity responsible for a given action is necessary in order to assume responsibility on it. FINSENY security functional architecture covers this requirement in the form of several specifications, such as those concerning audit and logging described in section 4.4.9.

### 4.4.12 Security management

Security management involves management related to asset management, physical security and technical and organizational means. It consists in identifying the organization's information assets, developing, documenting and implementing security policies and procedures, and thus includes (or involves) many other security elements (subfunctions).

### 4.4.13 Secure system design

Secure system design methods comprise the complete system development process, from the idea to the actual target system. One of the basic paradigms to be followed is layered defense or defense in depth for the design of a security architecture.

Defense in depth can be described as the application of security controls in layers and at different levels. "Layers" imply multiple security barriers between the attacker and the target, while "levels" relate to the different levels in the communications infrastructure underlying any cyber system (transport, application, etc.). This concept ensures that if one security barrier is broken (for instance the lock on a door), the next layer may prevent the attack (the attacker does not have the correct password) or it may just deter the attack until it is detected (such as video surveillance or an alarm notifies personnel that an excess of passwords have been attempted).

Another principle to be followed is privacy by design, which is outlined in section 4.2.6.3 and will be described in further details in section 6.6.1. Here it is to be ensured that person related data are used and exposed following the general security requirements, but especially the legislative rules, which may be country specific. ISO 29101 provides a privacy reference architecture which can be used to support privacy by design for FINSENY.

Technological security controls are typically a combination of different security mechanisms. An example may be a secured transport channel, which authenticates the communicating peers and uses integrity mechanisms and encryption to protect the contents of a message on transport level. This may be sufficient for several use cases, but application level security may be required by others. One example is role-based access control on application level, e.g., to ensure that certain actions can only be executed by authorized personnel.

To determine the actual need for certain security controls and their placement within the system architecture a security assessment is the typical starting point. This assessment may target both, the systems general design based on a conceptual assessment of the scenario use case specific data model and the data exchange and its derived security requirements as well as practical tests on dedicated

components. Note that this analysis should be performed regularly; at least whenever the general functionality of the target system is enhanced or when new components are added.

The security assessment itself is only one part of a security oriented design, development, and operation process as shown in Figure 20. The process of determining the actual security needs are further explained in NIST SP 800-30. This process bases on a specific system architecture and includes the determination of assets and connected risks to the assets. (cf. [8]).

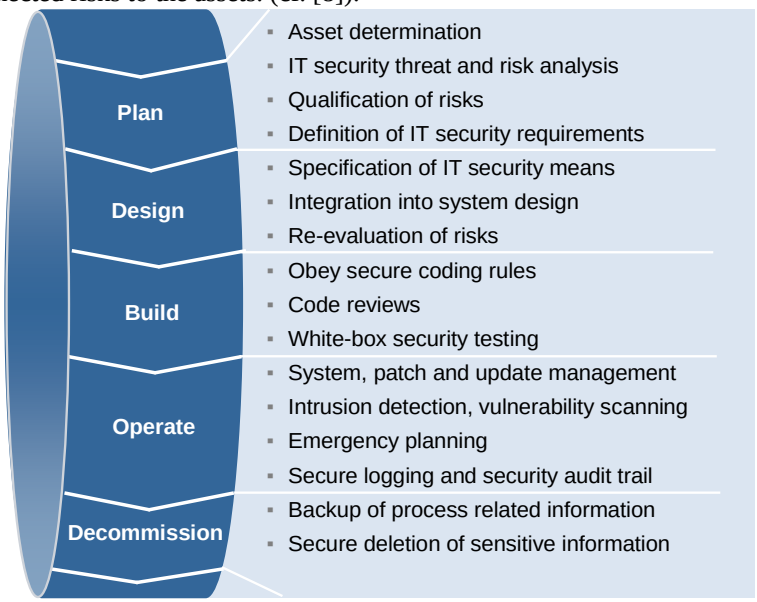


**Figure 20: Secure design, development, and operation process**

## 4.5 European Security projects

FINSENY has made an extensive analysis of FI-WARE Generic Enablers which can be used for FINSENY purposes. Additionally, we include in this section, mention to other European projects, security specific, which results can be applied as well, to go further on energy management in Europe.

### 4.5.1 STORK - Secure idenTity acrOss boRders linked

Websites: http://www.eid-stork.eu http://www.eid-stork2.eu

The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders

The STORK interoperable solution for electronic identity (eID) is based on a distributed architecture for full integration of EU e-services while taking into account specifications and infrastructures currently existing in EU Member States.

STORK gives the common specifications for eID interoperability in Europe. This opens possibilities for transnational and even international energy projects and has direct impact on FINSENY credential management possibilities.

STORK is part of FI-WARE where ATOS participates directly. Software and specifications can be found online:

https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312

New process flows have being designed for STORK2.0. The first one, *authentication on behalf of*, will allow citizens to electronically act on behalf of legal persons, especially SMEs. The second one, *Powers (for digital signature)* has been designed to be implemented in situations where a Service provider has received a digital signature whose signatory has signed in representation of a legal person.

In addition, in order to better adapt the project's technology to the arising needs of the upcoming pilots in terms of citizen authentication, the team has redesigned pre-existing key business attributes implemented in previous STORK project.

STORK 2.0 will apply the common electronic identity interoperability infrastructure developed in the project and will evaluate its corresponding services in the context of four cross-sector and cross-border pilots in key strategic areas for European economic growth and competitiveness, namely eLearning and Academic Qualifications, eBanking, Public Services for Business and eHealth.

**We think this could be applied as well for energy and FINSENY use cases such as electric mobility or the electronic marketplace for energy. In fact, many technical and business requirements are the same.**

These pilots explore possible ways to fulfill real needs of citizens and businesses in real-life settings and further explore the potentialities and benefits generation for a rich community of stakeholders offered by STORK 2.0 federated and trustworthy framework for cross-border eID services at European level. The four pilot applications will facilitate borderless digital living and mobility in the EU, enhancing the Digital Single Market for public and commercial services in alignment with the Services Directive and the upcoming Regulation on Electronic Identification and Trust Services for Electronic Transactions in the internal market. During this period, the pilots are focused in a detailed requirements and functional specification, working closely with other project tasks focused on the analysis of existing infrastructures and resources, legal and trust analysis and common specifications and building blocks.

### 4.5.2 SEMIRAMIS – Secure Management of Information across multiple Stakeholder

Website: http://www.semiramis-cip.eu

SEMIRAMIS made special effort on exchange of information across borders.- Individual country´s laws are examined and so attributes related to the person. Technical procedures are provided for both exchange of attributes and documents. We consider application for exchange in energy market.

Results from SEMIRAMIS can be of benefit for FINSENY use cases. Concretely, SEMIRAMIS makes the following:

- Deploy common rules and specifications for secure information management within organizations and across trans-EU e-service chains, including service compositions with public and private e-services;
- Test, in real life environments, solutions for various types of cross-domain and cross-stakeholders e-services constellations
- Provide application level, end-to-end security, paying special attention to privacy concerns when dealing with sensitive information
- Support the specific approach of the ID provider in terms of personal or organizational policies
- Implement a User-centric Identity Interoperability, a federated schema that can be managed by public/private organizations

As we see, concepts and requirements from FINSENY security functional architecture are considered in this project.

### 4.5.3 Massif – MAnagement of Security Information and events in Service InFrastructures

Website: http://www.massif-project.eu

The main objective of MASSIF is to achieve a significant advance in the area of SIEM (Security Information and Event management) of relevance for critical infrastructures, and concretely, on distribution systems (WP2).

In this project, advanced concepts of SIEM in an IT system supporting a critical infrastructure are used.

The deliverables list can be found here: http://www.massif-project.eu/list_deliverables

# 5. Security Countermeasures

WP1 security task has analyzed the assets and threats to these assets for the different use case work packages WP2 to WP6. In this chapter we recommend security controls and other options that are able to reduce the risks by ensuring the protection needs of the assets.

## 5.1 Security countermeasures and controls

Commonly used security controls for IT infrastructures are for instance:

- TLS tunnels for hop-to-hop authenticity, integrity protection and confidentiality;
- digital signatures and envelopes for end-to-end authenticity, integrity protection and confidentiality, Digital Signatures also to ensure non-repudiability;
- encrypted file systems, databases, or hard disks for storage security;
- PKI for credential management;
- tamper resistance and intrusion detection for exposed components;
- access control policies for controlled access to and use of information assets;
- logging for improved accountability;
- alarming and event handling to react to and manage critical situations.

Such a multitude of security mechanisms raises the issues of where to deploy them, and on what assets they have to be applied, which need to be addressed by the use case specific security architecture. This deliverable (D1.11) now lists security controls able to support the fulfillment of the FINSENY IT security requirements as a catalogue. A mapping between the security controls and the security requirements is shown in the following chapter 5.2.

Note that the list of examples does not claim to be complete. The examples are described in order to provide an idea of how a security control may look like.

**Control 1: User authentication methods**

User authentication is to be performed for different purposes, which may be connected to authorization, service subscription and/or payment options. Typical methods for user authentication comprise, but are not restricted to, the following technical means:

- combination of username password (cf. also section 4.4.2.2.1);
- token based authentication (cf. section 4.4.2.2.2) using e.g., RFID tags or Smartcard based authentication;
- biometric authentication (cf. section 4.4.2.2.3).

**Control 2: Device authentication methods**

Device authentication is needed to assure the identity of a device, especially in communication scenarios. Methods or solutions for device authentication include, but are not restricted to:

- cryptographic keys stored in software or special hardware (cf. section 4.4.2.4.1);
- unclonable physical functions (cf. section 4.4.2.4.2);
- electronic product authentication (cf. section 4.4.2.3.2);
- appearance (cf. section 4.4.2.3.1).

**Control 3: Authorization and access control methods**

Authorization and access control means definition and enforcement of access policies (cf. section 4.4.4). Methods or solutions for authorization and access control include, but are not restricted to:

- Mandatory Access Control;
- Discretionary Access Control;
- Role-based Access Control;
- Claim-based authorization;
- SAML;
- OpenID;
- Kerberos.

**Control 4: Message authentication methods**

Message authentication (cf. section 4.4.3) is needed to have assurance about the sender of a message. Methods or solutions for message authentication include, but are not restricted to:

- Message Authentication Code (cf. sections 4.4.3.1), e.g. HMAC-based;
- Digital signatures (cf. sections 4.4.3.2)

**Control 5: Digital signature methods**

Digital signatures (cf. sections 4.4.3.2 and 4.4.6 ), if supported by laws and regulations, are an electronic equivalent to handwritten signatures. Methods or solutions for digital signatures include, but are not restricted to:

- RSA;
- ElGamal;
- DSA
- ECDSA, ECGDSA;
- S/MIME (PKCS#7);
- OpenPGP;
- XML-Dsig.

**Control 6: Encryption methods**

Encryption is used to achieve confidentiality of data. Methods or solutions for encryption include, but are not restricted to:

- RSA;
- ElGamal;
- ECIES (Elliptic Curve Integrated Encryption Scheme);
- 3-DES;
- AES (in different modes, can also be combined with authentication);
- Blowfish;
- Twofish;
- Fully Homomorphic Encryption (FHE).

**Control 7: Secure system design methods**

Section 4.4.12 describes secure system design methods. One of the methods described in this section is a threat and risk analysis. In the context of FINSENY, this part of the secure system design has been accomplished by the WP1 security task. Note that a threat and risk analysis should always be (re-)performed whenever the underlying system or the target use case (and thus th assumptions) change. Moreover, as part of the Generic Enablers, security architecture design has been discussed in the context of Generic Enablers (see section 4.1). The Generic Enablers in this context provided by FI-WARE are:

- security monitoring (see section 4.1.1);
- identity management (see section 4.1.2);
- privacy (see section 4.1.3);
- data handling (see section 4.1.4);
- context based security and compliance (see section 4.1.5);
- additional security services (database security, etc - see section 4.1.6).

Methods or solutions which interplay with secure system design targeting e.g. availability and robustness include, but are not restricted to:

- hot and cold stand-by;
- mirroring;
- load balancing;
- redundancies.

**Control 8: Basic IT protection methods**

Methods or solutions for basic IT protection include, but are not restricted to:

- user/component management and user /component authentication (IAM);
- patching and security maintenance;
- hardening/secure configuration;
- anti-malware, antivirus and anti-spyware tools;
- firewalling (network and host);
- intrusion detection/prevention (network and host);
- backup procedures (secure archiving and restore).

**Control 9: Trusted and well-trained personnel**

Methods or solutions for trusted and well-trained personnel include, but are not restricted to:

- tolerable and legally allowed checks before hiring;
- general IT training;
- special IT security training;
- data privacy training.

**Control 10: Basic protection of physical systems**

Methods or solutions for basic protection of physical systems include, but are not restricted to:

- protection against natural disaster;
- physical access control;
- security guards.

**Control 11: Basic safety protection**

Basic safety protection within FINSENY mainly targets the enforcement of adherence to physical limits as well as the limitation of consequences of failure, damage, or errors of the target system. Methods or solutions include, but are not restricted to:

- protection against excess of physical limits (sensors, actuators, fuses, …);
- in the electro mobility environment, there are several standards targeting safety means (cf. also section 4.3.1.1), such as:
  - ISO 17409 (under work) to protect against overvoltage and over current when using the AC or DC charging on the EV side;
  - IEC 61851-22 (CD phase) and IEC 61851-1 to protect against overvoltage and over current when using AC charging on the EVSE side;
  - IEC 61851-23 (CD phase) to protect against overvoltage and over current when using the DC charging on the EVSE side.

**Control 12: Acknowledgement methods (cryptographic binding methods)**

Acknowledgement methods are a building block for transaction security (cf. section 4.4.7). Methods or solutions for acknowledgement and transaction security in general include, but are not restricted to:

- EDIFACT/ISO 9735;
- ebXML;
- WS-Reliability;
- WS-ReliableMessaging;
- SET.

**Control 13: Secure coding methods**

Methods or solutions for secure coding include, but are not restricted to:

- code review;
- usage of secure coding tools.

**Control 14: Secure time synchronization methods**

Methods or protocols to securely synchronize the time include, but are not restricted to:

- usage of multiple time server and consistency check between the provided time information;
- if NTP (Network Time Protocol) is used for time synchronization application of security options provided through authkey (specified in RFC 5906) → target would be integrity protection and source authentication of time information;
- if IEEE 1588 is applied for time synchronization application of the security options in IEEE 1588 → target would be integrity protection and source authentication of time information;
- usage of DCF77 receivers as additional source of information;
- usage of GPS internal time information as additional source of time information.

**Control 15: Integrity protection methods for stored data**

Data integrity provides protection against unauthorized data modification. It proves that the data has not been changed since it was created by its author. Data integrity relates to both, transmitted and stored data in contrast to message authentication stated above, which is applicable for the transmission only.

Methods or solutions for integrity protection of stored data include, but are not restricted to:

- cryptographic check sums using involving a key such as:
  - hash functions: HMAC-SHA1, HMAC-SHA256, etc.;

- symmetric encryption mechanisms in MAC modes: AES-CBC-MAC, AES-CMAC, etc.;
- digital signatures like RSA, ECDSA, etc.

**Control 16: Privacy protection methods**

The protection of data privacy is a common legal requirement in many countries. It cannot be achieved by a single measure only, but with a catalog of organizational and technical measures.

Organizational measures include:

- comprehensive information of data subjects about the use of their personal data;
- qualified agreement of the data subjects to the processing;
- procedures to respond to personal data copy requests;
- rectification, erasure and blocking procedures;
- obligation to data secrecy for any person in contact with personal data (e.g. staff);
- privacy awareness training for staff;
- blinded installation.

Technical measures include standard IT security measures already considered in other security controls listed previously, like for example:

- restriction of the physical access to rooms where personal data are processed or stored (server and archive rooms, workplaces...) and its protection by appropriate measures like self-closing doors, locks, and alerting systems;
- protection of the access to data processing systems by access control at login, preferably based on two factor authentication like a personal chip card with PIN;
- an elaborate role and rights concept which allows a fine-granular regulated access to personal data by the service personnel, while supporting detailed logging and tracing back any change by human intervention too;
- protection of logging data to prevent unauthorized analysis e.g. for supervision of the personnel’s working time, and in such a way that logging data are not editable and not erasable even if the customer withdraws his permission for data processing;
- logging of security relevant events like failed connection attempts;
- hardening of all devices (servers, databases, workstations, mobile devices, sensors, etc.) according to IT security recommendations;
- installation of software patches in time;
- installation of security software against viruses and other malware;
- device sealing to detect tampering;
- firewalls to protect internal networks in combination with demilitarized zones (DMZ) where all servers accessible from outside are placed;
- encryption to protect communications between devices via wireless or public networks, on the basis of state of the art cryptographic methods, algorithms and key lengths;
- encryption of data in persistent memory of devices in physically not secure environments;
- encryption of personal data in databases and only grating of access to authenticated and authorized users, processes and devices to connect to the databases;
- appropriate organization of logical database structures to support separate processing and storing of personal data;
- mutual authentication may prevent undesired data disclosure by sending data to wrong receivers;
- mapping of data by digitally signing data as close to the source as possible;

- storage of private cryptographic keys and other confidential security credentials in an HSM (hardware security module) and only use of security tokens like certified chip cards and RFID tokens which are resistant against side channel attacks for authentication;
- redundant installation of critical system components;
- regular backups.

Nevertheless, standard IT security measures are not sufficient. Specific privacy protection methods are needed, like for instance:

- anonymization and aliasing;
- transparency measures (e.g. visualization of personal data processed);
- reliable erasure of data;
- functionality to stop the data processing if desired by the user.

## 5.2 Control analysis

This section finally maps the security controls defined in the section 5.1 to the security requirements to validate the effectiveness of the proposed security controls.

| Security Requirement / Security Control | 1: Authentication and authorization | 2: Data confidentiality | 3: Data integrity | 4: Non-repudiation | 5: Data backup and recovery | 6: System protection components | 7: Secure SW/FW Updates | 8: Secure Network Design | 9: Security Management | 10: Logging and Audit | 11: Time Synchronization | 12: Observation of Policies & Laws | 13: Transaction Security |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1: User Authentic. Methods | X | | | X | X | X | X | X | X | X | X | X | X |
| 2: Device Authentic. Methods | X | | | | | X | X | X | X | X | X | X | X |
| 3: Authoriz. & Access Control Methods | X | X | X | | X | X | X | X | X | X | X | X | X |
| 4: Message Authentic. Methods | X | | X | | | | X | (X) | X | | X | X | X |
| 5: Digital Signature Methods | X | | X | X | X | | X | | X | X | X | X | X |
| 6: Encryption Methods | | X | | | X | | (X) | X | (X) | X | | X | X |
| 7: Secure System Design Methods | (X) | (X) | (X) | (X) | X | X | (X) | X | X | (X) | (X) | X | (X) |
| 8: Basic IT-Protection Methods | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) |

| Security Requirement / Security Control | 1: Authentication and authorization | 2: Data confidentiality | 3: Data integrity | 4: Non-repudiation | 5: Data backup and recovery | 6: System protection components | 7: Secure SW/FW Updates | 8: Secure Network Design | 9: Security Management | 10: Logging and Audit | 11: Time Synchronization | 12: Observation of Policies & Laws | 13: Transaction Security |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9: Trusted and Well Trained Personnel | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) |
| 10: Basic Protection of Physical Systems | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) |
| 11: Basic Safety Protection | | | | | | (X) | | | | | | X | |
| 12: Acknowledgement Methods (Cryptographic Binding Methods) | | | | (X) | | | | | | | | | X |
| 13: Secure Coding Methods | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) | (X) |
| 14: Secure Time Synchronization Methods | X | | (X) | X | (X) | | (X) | | X | X | X | | X |
| 15: Integrity Methods for stored data | | | X | (X) | X | | X | | X | X | | X | X |
| 16: Privacy protection methods | X | X | X | | X | | | | | X | | X | |

**Table 8: Security requirements being supported or met by security controls**

Some notes and explanations to the entries in the table above:

- Some of the marks have been stated in parenthesis. The reasoning is that certain security controls may be seen as supportive actions to tackle a dedicated requirement but do not necessarily provide the basic means.
- User authentication has been added also for component management. The reasoning for this is that the management of components may influence the service provided. An example is the administration of the time servers providing the synchronization base.
- Authorization and access control has been explicitly added also for stored data to ensure that only authorized people or components have access to stored information.
- Encryption methods for SW/FW updates have been stated with a mark in parenthesis. The reasoning is that encryption may not always be necessary for these updates. As soon as there are sensitive information (like IPR relevant information) is included, encryption becomes necessary.

- Encryption methods have also been added to security management to ensure that the exchange of sensitive information, e.g., during remote maintenance, is protected appropriately.

# 6. Security Architecture Elements

This section addresses the further discussion of security architecture elements considered by the WP1 security task team as essential for the further specification of the functional architectures of the different FINSENY work packages:

- Security credential and identity management
- Authentication elements and services for FINSENY
- Security aspects of an IPv4/IPv6 interworking
- Secure discovery and connectivity to Smart Grid devices
- Migration aspects when introducing security
- Security technologies to protect customer privacy in Smart Grids.

These security architecture elements either support or complement the security controls defined in section 5 and constitute a more energy scenario-related view of the general security elements described in section 4.4 with the objective to achieve a further mapping of suitable security elements to the FINSENY functional architectures. For this, the suitability of the available FI-WARE general enablers is examined and domain-specific measures are proposed.

Note that the described security architecture elements are intended to be used to build an appropriate security architecture addressing the security needs of the target functional architectures. Therefore, the security measures described throughout this section (and also section 4) are to be seen as catalog of security controls for Smart Grid use cases. The final application strongly depends on the target architecture. An example for such an application is given by the final chapter 7.

## 6.1 Security credential and identity management

This section focuses on the management of credentials necessary for different security services used to protect the different use cases. In general, as outlined in section 4.4 security credentials may be related to machines or humans and are applicable for the communication between both. This section discusses several options for security credentials, their lifecycle and their integration into the product lifecycle.

Security parameters are used in different phases of the product lifetime and are applied as:

- short term or session parameters (e.g., for integrity or confidentiality protection of an administrative action). Short term parameters may comprise:
  - Session keys;
  - Session parameters (dedicated cryptographic algorithms).
- long term or permanent parameters (e.g., for authentication). Long term parameters may be for instance:
  - Certificates and corresponding private keys;
  - Symmetric keys (e.g., for static VPN tunnel);
  - Allowed cipher suites for a cryptographic protocol;
  - Configuration parameters (security policy) of cryptographic protocols (e.g., renegotiation, resumption, re-keying, etc.);
  - Association of access rights to defined roles;
  - Definition of roles and the association of users to dedicated roles;
  - Seeds (initial start parameter, e.g., for a random number generator).

### 6.1.1 Security credential lifecycle

The following description of the security credential lifecycle applies to basically all security credentials but is focused on device credentials here. The typical life cycle of security credentials is depicted in Figure 21. The general key life cycle management is elaborately discussed within IEC 11770 (cf. [85]) and in NIST SP 800-130 (cf. [86]). The life cycle of security credentials is depicted here on an abstract level to have a reference point for recommended solutions in other clauses of this document.

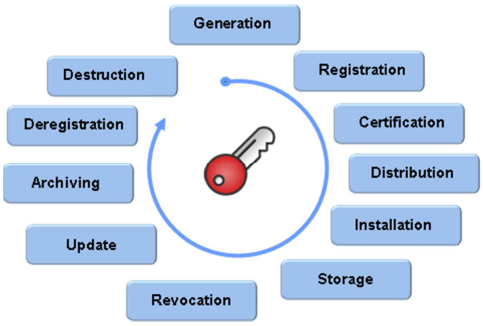


**Figure 21: Security Parameter Life Cycle**

The following list briefly describes the single stages in the life cycle of a cryptographic key as part of the security parameter set:

- **Generation**: Device keys can be created on the device itself. For example, in case of asymmetric key pairs, the device may generate the key material and a Certificate Signing Request (CSR), which is sent to a Certification Authority. Alternatively, keys may be created externally (e.g., a trust center, an engineering station, or an administrator laptop) and installed on the target device (off-device key generation). Also new pre-shared keys can be distributed as part of the configuration data.
- **Registration:** Typically, a registration authority registers a key by associating a key with an entity based on a key register.
- **Certification**: Typically done for asymmetric keys through a certification authority. Depending on the key generation, this can be part of the key generation in a trust center or may be done using information sent in a CSR. The certification process ensures the association between an entity and a public key.
- **Distribution**: Key distribution comprises the process steps to transport keys as well as key management information to authorized entities in a secure manner. In the case of off-device key generation, the device key has to be installed on the target device. This can be performed offline, e.g. the key is installed to the target entity during the manufacturing and/or engineering processes, or online requiring communication with a security server (out-of band using a separate communication channel or in-band as part of a service communication). Key distribution may refer to asymmetric keys, such as certificates and associated private key, and also to symmetric keys.
- **Installation**: A key must be installed in a secure environment in order to provide services (e.g.: encryption) through well defined, secure interfaces.
- **Storage**: The private/secret device key should be stored in secured memory (e.g., E2PROM) or in a separate hardware module (e.g., smartcard or a trusted platform module).
- **Update**: Cryptographic keys must be regularly updated. Cryptographic keys have a dedicated lifetime, e.g., user certificates typically have a lifetime of 2 years, while server certificates are typically limited to 1 year, pre-shared keys to a few weeks or months and session keys to a few hours or packets. Session key update does not belong to the process of security rollout as it is typically performed by the security protocol used, based on a given security policy.
- **Archiving**: Typically long term encryption keys are archived to enable access to stored encrypted data. A use case is given by an employee leaving a company. While encryption keys are archived, signature and authentication keys may not be archived, but it is recommended [86].
- **De-Registration**: This procedure is typically provided by the registration authority to remove the association of an entity with a dedicated key. It is typically used in the key destruction phase.

- **Key Revocation**: Key revocation may occur when a key is no longer authorized to be used. This may be the case if a user or device leaves the organization or if a private key is compromised.
- **Destruction**: Keys should be deleted. Typically, old keys should be destroyed after those keys have been updated.

### 6.1.2 Security and identity credentials

The following list shows examples types of device identifiers which are often associated with credentials. These device identifiers are typically used in today's deployment, e.g., to associate an IP address with a given MAC address, apply port based network security, or also device authentication.

- MAC Address, which is being used on layer 2, e.g., during network attachment
  - IEEE 802 defines a 48 bit (EUI-48) address (or a 64 bit address – EUI-64 as used in IPv6 )
- Serial number
  - Often an alphanumeric string or an integer. When serial numbers are used in the context of the Domain Name Service (DNS) they need to comply to RFC 1982. This RFC defines the serial number arithmetic to be used for calculations.
  - ISSN (International Standard Serial Number) defines the syntax and structure of serial numbers
- Symbolic names
  - Mapping to device identifier, there may be multiple symbolic names for the same device ID
- X.509 Certificate
  - Typically an identity certificate, which may be issued for the device during production by either the device vendor or the security component vendor (e.g., in case of a TPM)
- Cryptographically Generated Address (CGA)
  - generated by hashing the already existing public key (e.g., used in the Host Identity Protocol (HIP))
- IEEE 802.1ar Secure Device Identity, which may be used in the context of IEEE 802.1x security
  - Defines globally unique per-device identifiers and their management and cryptographic binding of a device to its identifiers

Based on the discussion of applicable security standards in section 4.3 and security elements in section 4.4 it is very likely that from the list of identifiers at least MAC addresses, serial number symbolic names, and X.509 certificates are used in the different Smart Grid scenarios. Therefore the further discussion concentrates on protocols, services, and functionalities supporting this type of identifiers.

For dedicated functionalities, enhancements to identifiers or identifier related credentials are necessary. An example is given by remote management of a substation applying role based access control. Here, remote administration may apply IEC 61850 as protocol for communicating from a control center to a substation. This connection can be secured by using IEC 62351-3 and IEC 62351-4 basically securing the TCP connection between the participants using TLS. According to IEC 62351-3 TLS is mutually authenticated.

### 6.1.3 Identifier mapping / resolution / conversion

It is expected that a given device already gets certain identifier information during the production process. In many cases this is the serial number. Nevertheless, besides vendor specific identifiers, a device most often gets operational identifiers which better suit the operational environment. An example is given by the MAC address which is imprinted in a NIC (Network Interface Card) during production. In an operational environment this NIC typically gets an IP address assigned, which is specific for the deployment environment.

Device specific identifiers are not always directly applicable in target use cases. This is given by the fact that different services or applications rely on different identifiers. Hence, a conversion function is used to translate from one identifier to another. Going back to the MAC example, this task is being fulfilled by

the ARP protocol, which provides a resolution between a device's MAC address and the associated IP address in a given subnet to enable routing.

- There are numerous ways to map identifiers to other (identifier) information
  - ARP defines the mapping of MAC addresses to IP addresses (within a LAN segment)
  - DNS defines the mapping of IP addresses to symbolic names (within an Intranet or the Internet)
  - ENUM defines the mapping of telephone number to IP addresses
- There are further ways to map identifier information to certain policies:
  - IEEE 802.1x providing access control to networks, based on provided (identity) information,; employs further protocols like RADIUS, Diameter, EAP, …
  - LDAP based systems like Microsoft's Active Directory
  - Device Inventory Management Solutions based on Network Access Control Solutions (provided, e.g., by Cisco, Juniper, Enterasys as part of their Network (Management) appliances)

### 6.1.4 Identity and credential management protocols

Identity management is enabled by different protocols, services, and applications. The following subsections provide examples for the single categories. At first identity management protocols are investigated. The following subsection depicts identity management systems, partly relying on the protocols stated below.

Protocols for identity management discussed here focus mainly on identifiers in the form of cryptographic credentials. Identifier resolution protocols are described in section 6.1.3.

- PKCS #10 (Certificate Signing Request – CSR)
  - Describes the syntax for certificate requests, which are sent to a certification authority, transforming the requests into X.509 public-key certificates
  - May be mapped to different protocols if necessary like HTTP (see also SCEP below)
- CMP – Certificate Management Protocol
  - Provides on-line interactions between PKI components, including an exchange between a Certification Authority (CA) and a client system.
  - Supports proof-of-possession for key management keys (like Diffie-Hellman, RFC 2875)
  - Standardized in RFC 4210 (http://tools.ietf.org/html/rfc4210)
- CMC – Certificate Management over CMS (Cryptographic Message Syntax, PKCS#7)
  - Support certificate enrollment within one roundtrip
  - Performs as a two party protocol, directly between the client (requestor) and the server (CA)
  - Less functionality than CMP, but supports CMS, which in turn is supported in many toolkits
  - Supports proof-of-possession for key management keys (like Diffie-Hellman, RFC 2875)
  - Uses the Certificate Request Message Format (CRMF) defined in RFC 4211
- Standardized in RFC 5272 (http://tools.ietf.org/html/rfc5272) SCEP – Simple Certificate Enrollment Protocol (Cisco, VeriSign)
  - Supports certificate management (enrollment, renewal, and distribution) and CRL queries
  - Leverages existing technology by using PKCS#7 and PKCS#10 (CSR) over HTTP

- RSA is only public key algorithm supported
- IETF Draft (https://datatracker.ietf.org/doc/draft-nourse-scep/ ) → Is on historic track, CMP or CMC should be used instead, but SCEP is supported by several manufacturers of network equipment and software

- Trust Anchor Management Protocol (TAMP) may be used to manage the trust anchors and community identifiers in any device, defined in RFC 5934
  - Requirements are defined in RFC 6024 (http://tools.ietf.org/rfc/rfc6024.txt)
  - Several specifications address trust anchor management and trust anchor usage
    - Trust Anchor Format (TAF), RFC 5914 (http://tools.ietf.org/rfc/rfc5914.txt)
    - Trust Anchor Management Protocol (TAMP) may be used to manage the trust anchors and community identifiers in any device, defined in RFC 5934 (http://tools.ietf.org/rfc/rfc5934.txt)
      - Based on CMS (Cryptographic Message Syntax, RFC 5651)
      - Provides integrity protection by using digital signatures, but no confidentiality
      - Trust Anchor = PublicKey + Key ID
      - Types: apex (single trust anchor store with one superior trust anchor), management (for crypto modules), and identity trust anchors (PKI related)
    - Using Trust Anchor Constraints During Certification Path Processing (UTAC), RFC 5937 (http://tools.ietf.org/rfc/rfc5937.txt)

### 6.1.5 Identity and credential management systems

Identity and credential management systems build the base for deploying and maintaining secure solutions. As outlined in section 6.1.1 credentials have a lifecycle, which is being maintained by the management systems. This is especially true in operational phases like initial deployment, credential renewal, or component exchange (spare parts). Depending of the environment, identity and credential management may also been used to support for instance secure inventory management.

FI-WARE already discusses the Identity Management as one of the Generic Enablers, interfacing the IMS (IP Multimedia Subsystem). The figure is taken from http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.I2ND.S3C:

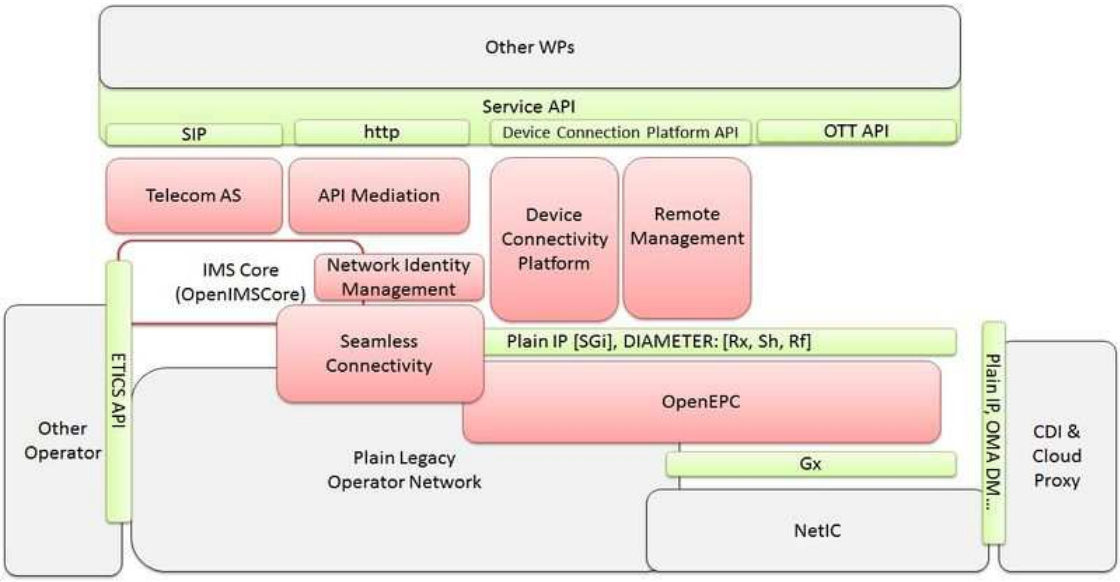


**Figure 22: FI-WARE high level architecture**

The figure above shows on the one hand the IMS core interfacing the Network Identity Management and on the other hand OpenEPC. OpenEPC is a toolkit from FHG Fokus, for prototyping IP connectivity related features like QoS and charging, mobility management, access and security for 3GPP and non-3GPP wireless technologies including 3GPP Long Term Evolution (LTE).

The following Identity Management Systems are discussed within FI-WARE. The information is taken from the Generic Enabler description for Identity Management (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Materializing_Security_in_FI-WARE#Identity_Management_Generic_Enabler). Images and information are taken from FI-WARE site.

#### 6.1.5.1 STORK

STORK implements an EU wide interoperable system for recognition of eID and authentication that enables businesses, citizens and government employees to use their national electronic identities in any Member State. It helps to simplify administrative formalities by providing secure online access to public services across EU borders. (See http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Stork for a short description or https://www.eid-stork.eu for the project itself. The latter site also hosts the documentation of the project deliverables.)

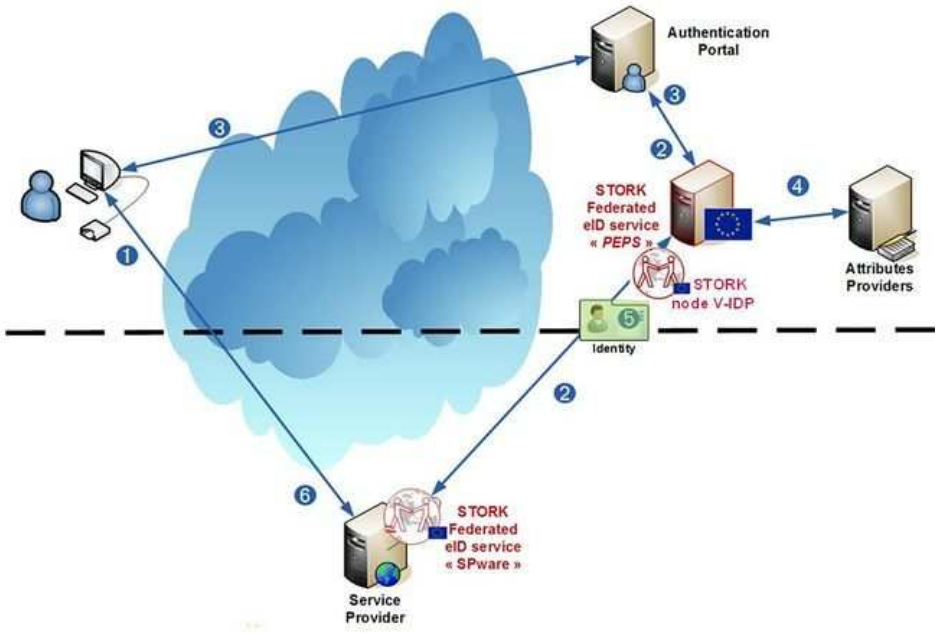


**Figure 23: STORK service architecture**

The core of the STORK platform is built with Java, and the interchanged messages are standard OASIS SAML 2.0 messages as it seeks to be technologically neutral and based on open standards.

As stated above, this system concentrate on human related identifier and connected credentials. Within FINSENY, both human and component related identity handling is necessary. One example can be given by electric mobility scenarios where a user of a service typically uses a related identifier for authentication, e.g. bound to a contract. On the other hand, a component related credential is used to achieve mutual authentication. To analyze the applicability of STORK services a comparison of the Identifier and corresponding credentials with the FINSENY use cases is necessary. Luckily, both use X.509 certificates, thus, base interoperability can be ensured.

**Questions to be clarified before final application (and some answer points):**

- FINSENY requires the support of RBAC ideally in the context of X.509 credentials. IEC 62351-8 describes X.509 public key and attribute certificate extensions to support RBAC. Does STORK allow for the support of additional extensions?
    - RBAC is always external to Stork. In Stork, authorisation is functionality inside each electronic services portal (service provider). Since Stork is not an identity provider, the accounts maintenance is also outside the system.

Stork just provides cross-border authentication. Therefore, applications that could be designed for energy projects (e.g. EVs, eMarketplace), could rely its authentication on Stork mechanisms while keeping their specific RBAC authorization model and systems, which could also differ according to the application functionality.

- How does the credential issue process look like?
  - We face here the issue of identifiers source and management.

    The functional needs of the specific application would give us the answer regarding which architecture is the adequate to use:

    1) Need of interoperability across borders

    In the case we want to use national eIDs and interoperability across borders, we can use Stork. Access management should be done through authorisation mechanisms.

    Therefore, we could suggest that the most "powerful" or effective solution to authenticate people would be one which uses Stork and has a good RBAC system. That is because maintenance of the IDs has to be done by other party (Identity Providers government…) and also because integration across European systems can be guaranteed.

    2) Business integrated applications B2C

    Businesses have their own users´ databases, which can be employees or customers. We can imagine the management of a fleet of EVS. Technicians would be employees (HHRR databases) and the drivers, the customers (customer DDBB).

    In this case, and depending on the functionality of the application, the option would be to consider the internal DB of Ids to manage credentials.

    In this scenario, and if the business needs interoperability across borders, they can work mapping their Ids with the national ones and then use Stork

    3) The application needs to manage their own credentials

    In the case the application needs to generate, revoke or delete, their own credentials, the best option should be FI-WARE GE module for authentication.

- For revocation of credentials, is there an interface for CRLs and also for OCSP?

#### 6.1.5.2 NSN provided Identity Management

The NSN Identity Management provides federated identity for Web-SSO and attributes for an authenticated user. This system links the network access authentication with the application level access authentication.

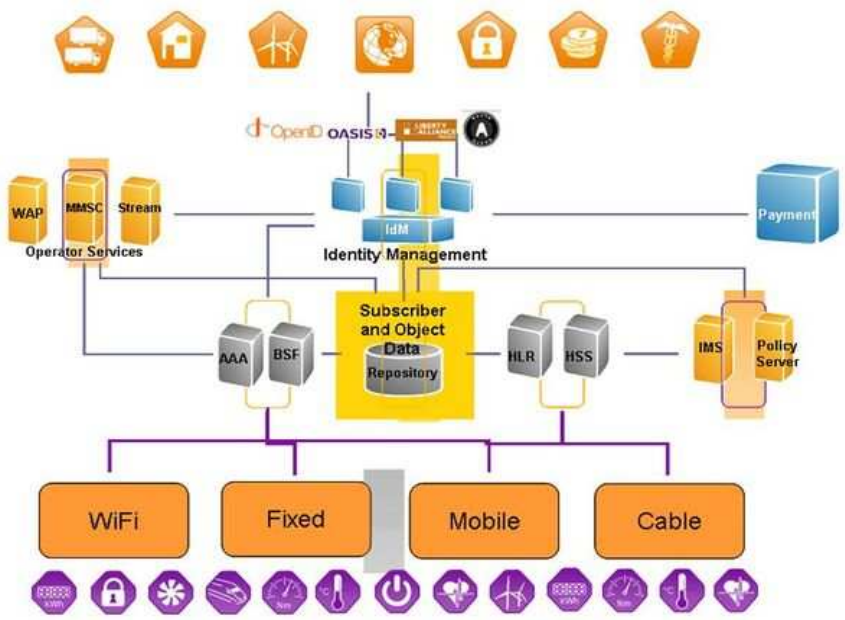


**Figure 24: NSN Identity Management**

The basic functionality of identity management enabler is protected by IPRs.

**Questions to be clarified before final application:**

- FINSENY requires the support of RBAC ideally in the context of X.509 credentials. IEC 62351-8 describes X.509 public key and attribute certificate extensions to support RBAC. Does the NSN identity management system allow for the support of additional extensions?
- Can it only be used in a Web-SSO environment or is it applicable in other environments too?
- From the description it did not became clear if this system also comprises CA functionalities for issuing credentials to users and to maintain revocation state of the credentials.

#### 6.1.5.3 Cloud user management “Global Customer Platform”

The Cloud User Management "Global Customer Platform" (GCP) stems from Deutsche Telekom. It enables storing user data and relevant profile information safely and reliably in the cloud. To use this, it just requires integration into Web applications. The solution can be used free of charge and provides typical basic functions of user management:

- Registration of user accounts
- Login for registered users by means of user name and password
- Single sign-on between several Web services of one provider
- Self-administration for users (e.g., password reset and changes to user data)
- Ending of sessions
- Deletion of account

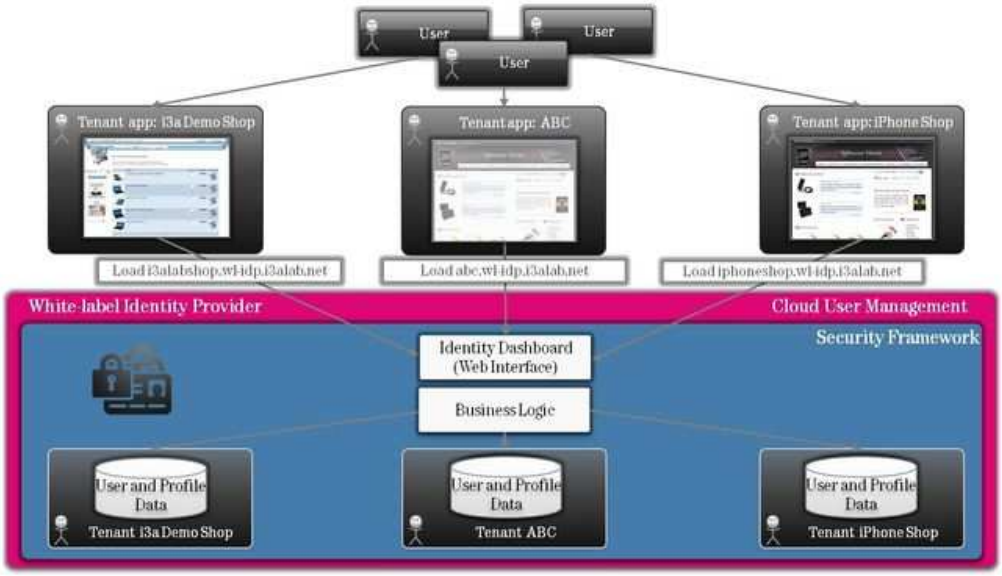


**Figure 25: Deutsche Telekom approach for cloud-based profile management**

The technologies used are Java EE and HTTP/HTTPS. The API description is available under http://www.developergarden.com/apis/apis-sdks/cloud-user-management

**Questions to be clarified before final application:**

- Applicability seems to be rather use case specific, as an online connection to the cloud management is always necessary?
- From the description it did not became clear if this system also comprises CA functionalities for issuing credentials to users and to maintain revocation state of the credentials. → Looks rather like a profile storage.

#### 6.1.5.4 SENSEI – access control

SENSEI (Integrating the Physical with the Digital World of the Network of the Future) is the result of an EU FP7 project. It provides an access control architecture for REST-based web services.

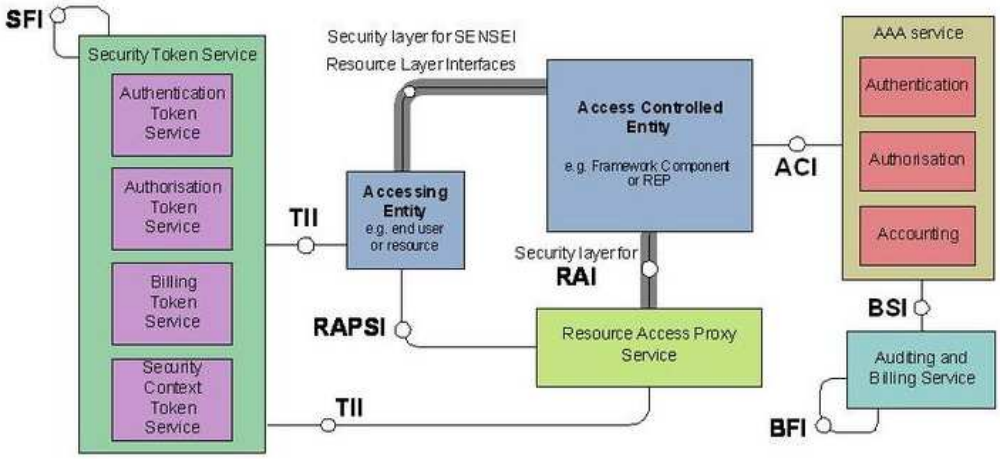


**Figure 26: Sensei overview**

SENSEI security components:

- AAA – Provides access control for the entire SENSEI system using both, a security token service for providing identities, and an AAA service against which Resource End Point (REP) and other components check access control rights for requesting resources. The Security Token Service (STS) provides security assertions to access restricted resources.

- Privacy and Billing - The Privacy and Billing component provides a complementary approach to the access control provided by the AAA component, with an accounting service that allows access to be denied due to insufficient funds. A security token installed in the resource user (a Firefox plug-in is also provided) is used to authenticate a resource user.
- Security Token Service: https://ncit-cluster.grid.pub.ro/trac/Sensei-WP5-Public/wiki/Aaa#Identityprovider:STS

**Questions to be clarified before final application:**

- Description of the security token services would be helpful to determine applicability in FINSENY use cases.

#### 6.1.5.5 Network Identity Management using the S3C.IdentityManagementModule API

S3C stands for Service, Capability, Connectivity, and Control. The network identity management bases on IMS (IP Multimedia Subsystem of mobile phone networks) and SIP (Session Initiation Protocol) to handle identities. The figure below is taken from the FI-WARE wiki and shows the general interaction.

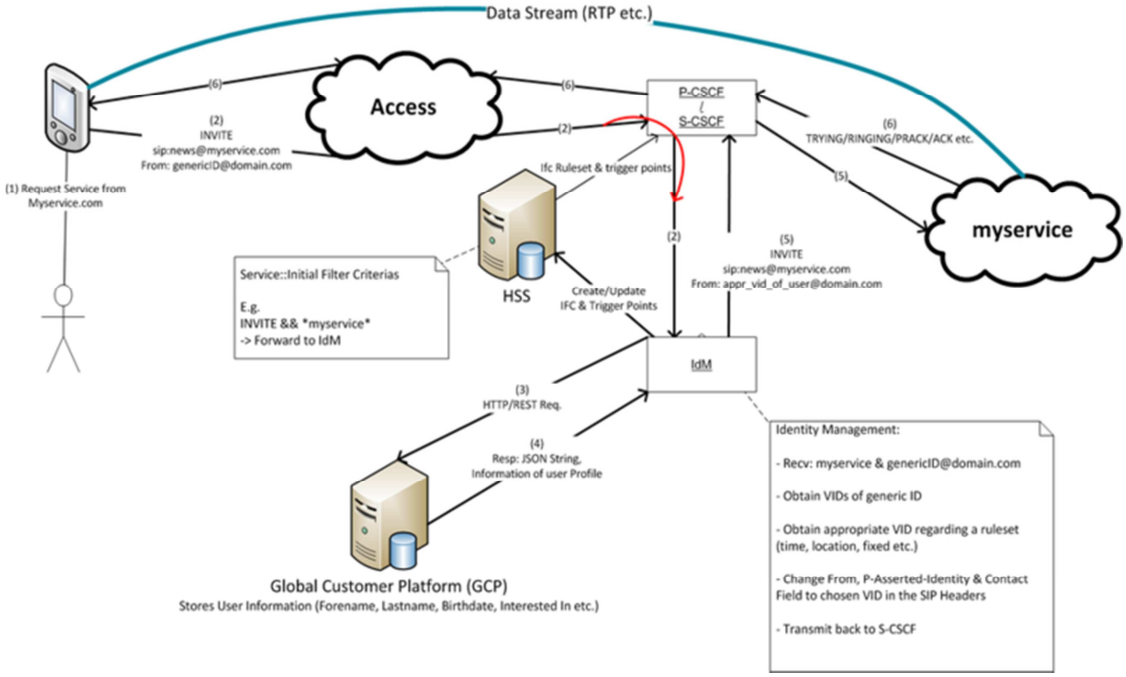


**Figure 27: S3C Identity Management**

Info: http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Network_Identity_Management

**Questions to be clarified before final application:**

- While the service provides identity management functionality, the issuing and format of the credentials connected to an identity seem to be a prerequisite. The applicability of the depicted approach strongly depends on the use case and especially on the protocol framework used within the use cases.

#### 6.1.5.6 FI-WARE Identity Management API

FI-WARE Generic Enabler for Identity Management: http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Identity_Management_Generic_Enabler

The FI-WARE GE for Identity Management (IdM) targets scenarios in which a user wants to access a certain resource, but is identified by a third party. This leads to a triangle communication scenario, in which the IdM has a trust relationship to the user and also to the service which depends on the IdM for identification and authorization of the user. Such approaches have been used already; most commonly known is probably Kerberos (RFC 4210). FI-WARE provides a similar functionality with the Generic Enabler by offering interfaces to different IdM solutions available, as shown in the figure below.

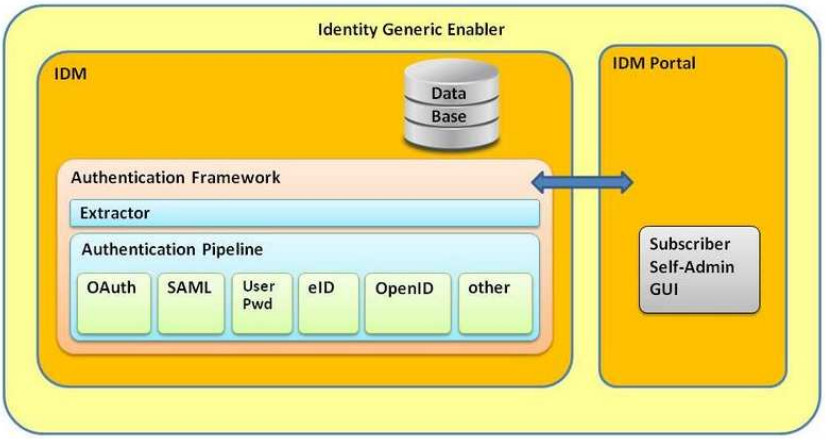


**Figure 28: FI-WARE GE Identity Management**

As shown in the figure, the following identity management solutions are in scope for the FI-WARE GE:

1. SAML (in a later version), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20
2. OAuth, http://oauth.net
3. OpenID, http://openid.net/connect/
4. Username / Password
5. eID – cards, http://www.eid-stork.eu

**Questions to be clarified before final application:**

- Detailed requirements to the IdM solution can be provided as soon as the WP specific functional architectures have evolved, to better match the target architecture.

### 6.1.6 Security rollout options

Security rollout describes the process of initial setup of security credentials (e.g., keys, certificates) and configuration information (rights, policies, etc.). The result is a trust anchor for further application to secure information, services, and communication. The process to distribute the security parameters into the component or parts of the component is called bootstrapping, while the adaptation of the security parameters to the deployment and operational environment is called secure operation. The distribution of these parameters at different times during the product lifetime is shown in the following figure.

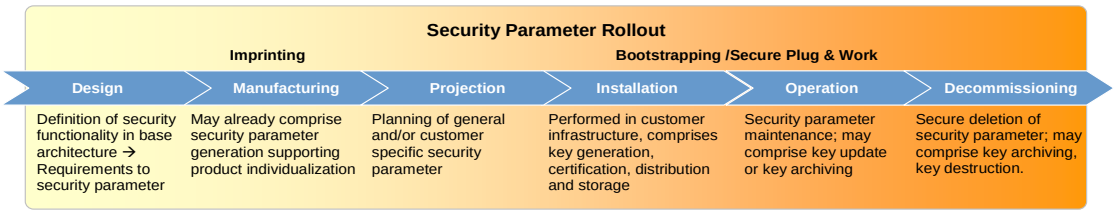


**Figure 29: Security parameter handling as part of the product lifecycle**

It is useful to distinguish different phases of the security rollout as there are:

- **Imprinting** concerns device-specific credentials that may be installed as part of manufacturing or during the initial phase of device installation. These may be not bound to a specific usage environment of the product. During the imprinting phase a manufacturer or installer creates and installs credentials for one or more devices in a uniform way. The challenge is to define processes that allow handling of huge numbers of security credentials cost-efficiently, in a uniform way. This comprises the in-factory handling as also the distribution of the device connected parameters to the end customer.
- **Bootstrapping / Secure Plug & Work** describes the process of installing a device in its intended usage environment. The installed credentials are specific to the intended usage of the

device. During Plug&Work the installation personal has to get suitable support so that they can install and commission very easily devices according to the project planning documentation. As a huge number of devices have to be installed in a typical industrial plant, it is important to limit the effort to install a single device while configuring it according to its role in the project plans.

Many devices in industry and energy automation have been enabled for secure communication and secure process performance. These devices often contain individual security credentials like secret (private) keys, and digital certificates, which have to be protected against readout and unauthorized replacement, respectively.

Ideally, the credentials are written into or generated by the devices during the individualization phase at the end of the production chain, e.g. when the firmware is uploaded. They may also be generated upon first initialization at a customer side. In practice, the process of creating and uploading the security credentials may be performed in several variations (not a complete list):

- External generation (maybe even by an external company) of keys and corresponding certificates, and provision of key / certificate lists to the firmware upload station
- Generation of keys and certificates by a software certification authority on a local PC which is connected to the firmware upload station
- Generation of keys directly inside the devices, export of public keys to a PC (e.g. by a CSR = certificate signing request), signing of the keys by a software certification authority on the PC by a HSM (e.g. a chip card) connected the PC, upload of the certificate into the device

An efficient and secure solution requires well-defined organizational processes, standardized (and preferably certified) software and hardware components, a protected environment, etc. Furthermore, a secure backup of related security credentials in central components, e.g., CA's private key, has to be considered to ensure continuous (secure) service access.

## 6.2 Authentication elements and services for FINSENY

This section gives the results of an analysis concerning the possible realization of authentication elements and services within the smart energy domain as seen by FINSENY. Another main contribution of this section is related to the possible use of FI-WARE Generic Enablers in the context of FINSENY authentication elements and services.

Section 4.4 already contains two subsections that give general overviews concerning authentication elements and services. Subsection 4.4.2 covers entity authentication and subsection 4.4.3 covers message authentication. In principle, it can be said that whenever there are enough system resources to deploy standard state-of-the-art solutions for authentication elements and services, such solutions should be thoroughly analyzed regarding possible usage within the smart energy domain as well. But as the smart energy domain has to cope with a great number of restricted environments, standard solutions from office IT may not always fit. Especially on the level of field elements like Intelligent Electric Devices (IED) the IT resources are sometimes restricted to such an extent that they cannot easily be enhanced by standard security solutions without affecting their non-security functionality and requirements. If security is nevertheless needed end-to-end or hop-to-hop, with at least one part being such a device, special solutions have to be developed to assure that e.g. timing requirements for real-time environments can still be met after integration.

Much insight into the analysis and considerations concerning the integration of authentication elements and services into the Smart Grid can be found in past and current scientific publications. This section thus starts with short summaries of a selection of such publications to provide a snapshot for further analysis within the FINSENY realm:

- Himanshu Khurana, Rakeshbabu Bobba, Timothy M. Yardley, Pooja Agarwal, Erich Heine: "Design Principles for power grid Cyber-Infrastructure Authentication Protocols" [87]

  Short summary: The authors discuss design principles for authentication protocols that shall be used within the Smart Grid under the constraints of power grid IT equipment. The constraints of the power grid are given as the need for highly efficient and highly available systems. The goal of the paper is to help ensure correctness and effectiveness of new cyber security standards for the Smart Grid area. Concerning the differences between the power grid and Internet systems the authors state in section 2 that "These differences arise largely from the critical and real-time

nature of electric grid systems, their impact on the safety of equipment and personnel and their long component life." With regard to the development of new standardized authentication protocols the authors argue that they should be developed having the fundamental differences in mind and not limitations that may soon be overcome by modernization in general. Apart from a few overarching principles like "know your threat environment" and "make all communication explicit", the following design principles for authentication protocols are discussed in the paper:

- Explicit Names: Always explicitly mention names respectively IDs, if they are essential to the meaning of a message.
- Unique Encoding: Make it possible to deduce whether a message belongs to a certain protocol and even to which particular instantiation of the protocol.
- Explicit Trust Assumptions: Have sound and clearly stated reasons for all trust relations a protocol is built upon.
- Use of Timestamps: If timestamps are used to guarantee freshness, be aware of secure and practical time synchronization.
- Protocol Boundaries: Be aware of the whole environment and thoroughly analyze any boundaries of the protocol.
- Release of Secrets: Be careful about all possible secrets, even that of the past. The protocol shall be resilient against the release of any secrets.
- Explicit Security Parameters: State every possible limitation of the protocol and take it into account. Make all your security parameters explicit.

Then the authors analyze other key issues for the design of authentication protocols within the Smart Grid, namely efficiency, availability and evolvability. Concerning efficiency, the overhead induced by the authentication protocol regarding communication and computation needs to be such that timely execution within the grid is still possible. Examples for possible overhead reductions and induced trade-offs are given in the paper. Availability calls for efficient use of resources, efficient error management as well as support for detection of attacks and response to attacks. Evolvability is ranked as being of special importance because of the long component life in the power grid. It requires e.g. modularity and possibility for updates of whole protocols or inner parts of them.

- Shailendra Fuloria, Ross Anderson, Fernando Alvarez, Kevin McGrath: "Key Management for Substations: Symmetric Keys, Public Keys or No Keys?" [94]

  Summary: The authors analyze key management for electrical substations motivated by NISTIR 7628 and IEC 62351. The devices that are to be managed are the network control center, the substation controller and IEDs. It is assumed that the network control center and the substation controller secure their communication in line with IEC 62351 and thus use TLS. For substation internal communication and, if needed, direct communication to IEDs from remote, approaches using asymmetric as well as symmetric cryptography are analyzed. The main use case for the analysis is adding a new IED to a substation. It is stated that setting up a whole substation simply uses repetition of this process.

  As an example of symmetric approaches the protocol as used in Homeplug AV is described together with its "simple connect" variant, which needs a trusted environment during initialization. Concerning asymmetric approaches, the commonly assumed TLS using client (and server) authentication is described. In both cases the final result is the distribution of the current network key that is to be used by the device to secure its communication with all other devices. In case of the symmetric key management approach an ignition key loaded by the manufacturer bootstraps the device. In case of the asymmetric approach several options of bootstrapping are described even including omission of client certificates. In this case the ignition key is either represented by the hash of an IED certificate or by a password that gets verified by the substation controller.
  Regarding key backup and remote access, it is said that the usual difference between the two approaches applies (requires confidentiality for symmetric keys vs. integrity protection for

public keys).
Regarding recovery from attacks, the authors differentiate between malicious intruder, malicious repair staff, supply chain attacks, network attacks, non-malicious failure of a substation key database, compromise of the network control center key database, and intrusion in unprotected areas. Their analysis in this part shows that the difference between symmetric and asymmetric key management approaches falls behind the general question whether cryptographic protection of communication as such is helpful or not. The result is that only communication between the network control center and the substation controller gains from such protection. As the use of TLS is already reflected in standards like IEC 62351, TLS should be used to secure this communication. Concerning substation internal communication, the authors conclude that there is no real gain from cryptographic protection. Only unprotected areas like pole tops may benefit. In general, they conclude that the key management approach to be chosen should be the one offering lowest overall costs. They state that this is reflected by the symmetric key approach in its simplest mode.

- Sean W. Smith: "Cryptographic scalability challenges in the Smart Grid (extended abstract)" [92]

  Summary: The author surveys scalability challenges when using PKI based schemes within the Smart Grid. As exemplary security element the author chose the authentication of devices and their messages. One proposition is that the Smart Grid will probably have more devices interconnected than the Internet currently has. Thus purely symmetric key approaches cannot be used because of their key management complexity and public-key cryptography is the better choice. The latter theoretically allows having only one private key and one trusted public key securely stored by the device instead of a quadratic order of magnitude in the symmetric case. Nevertheless, the author warns of other costs induced by a PKI that he sees not nearly as scalable.
  According to the paper a large scale PKI deployment within the Smart Grid has the following problem areas:

  - The single root assumption has failed in many other deployment areas. Alternatives are cross-certification, a bridge CA or "a loosely-organized oligarchy".
  - A valid certification path has to be found to validate a device's certificate. It may be necessary to acquire intermediate certificates of the path from outside resources, which in turn requires corresponding repositories.
  - As secrets may get compromised, a revocation scheme is needed. This is of special importance for devices that are not user-centric. The author doubts that the current solutions based upon CRLs and OCSP scale enough for the Smart Grid.
  - The identity information needed for Smart Grid devices is seen as context-sensitive by the author, which implies more changes than e.g. in web server PKIs. Such additional information may be supplied by a PKI able to handle dynamic identities or by using attribute certificates or by means outside of the PKI. Another issue regarding dynamic information is to assure that changes are only possible for authorized parties.
  - A PKI needs additive resources regarding communication and processing time. This will be a problem especially in those areas of the Smart Grid that are time-critical.
  - The data aggregation services that are discussed for the Smart Grid may have side-effects on the cryptographic services as well, eventually resulting in further PKI requirements.
  - Lastly, the author mentions privacy issues that may be induced by the PKI itself, e.g. when the certification path allows for deducing information about contractual relationships.

  The author's conclusion is that deploying a PKI within the Smart Grid "is the beginning, not the end, of the solution".

- Depeng Li, Zeyar Aung, John R. Williams, Abel Sanchez: "Efficient authentication scheme for data aggregation in Smart Grid with fault tolerance and fault diagnosis" [93]

Summary: The authors state that authentication schemes that rely on per-packet signature and per-signature verification are not suitable for the Smart Grid with its constrained resources and its high-availability requirements. Thus they argue that signature aggregation, batch verification and signature amortizing schemes may overcome these problems and propose a corresponding authentication scheme. This authentication scheme additionally offers a fault tolerant architecture by supporting so-called backup collectors and tools for fault diagnosis, e.g. regarding loss of authenticated messages.

The paper especially focuses on data aggregation, e.g. in the context of smart meters, which requires protection against attacks on intermediate hops together with highest efficiency regarding time and space complexity. For such scenarios the authors propose to combine minimum spanning tree (MST) based signature amortization and batch verification at collectors together with MST based signature aggregation at intermediate nodes. This is flanked by algorithms for failure locations of batch verification and signature aggregation.
The performance of this combination of algorithms is then analyzed theoretically and experimentally. The stated results show significant gains compared to straightforward schemes. Additionally, the authors state that the security of the scheme relies on the security of the underlying digital signature scheme. The latter statement is based upon references. Aspects like denial of service or replay attacks are shortly mentioned as well.

- Carl H. Hauser, Thanigainathan Manivannan, David E. Bakken: “Evaluating Multicast Message Authentication Protocols for Use in Wide Area power grid Data Delivery Services” [88]

Summary: The authors deduce that multicast message authentication is needed by the Smart Grid from the arguments that “multiple [system control and monitoring] applications will use data from each location” and that “the use of the data for important power grid control functions requires each message’s source to be authenticated”. The paper thus analyzes several multicast authentication protocols with regard to application in data delivery services for the power grid, especially considering quality of service.
The analysis focuses on periodic delivery of remote sensor data sent from a substation to the outside. Such data delivery underlies the following varying requirements: (low) latency, (high) rates, (high) availability. These requirements are to be met for millions of data streams. From the point of view of the authors, their variance means that a variety of authentication solutions is needed for fulfillment as well. From the security point of view, integrity and timely delivery of legitimate messages are seen as the most important requirements by the authors.
The following types of multicast authentication protocols are then analyzed by the authors:

  - MACs using shared keys
    Although well researched and used in unicast scenarios, the authors point out that the MAC approach using symmetric keys suffers from its lack of non-repudiation. This especially holds in multicast environments as every subscriber may create and sent valid MACs.
  - Public-key based techniques
    These techniques provide an adequate level of non-repudiation, but come with increased computational requirements and added latency compared to symmetric solutions. To overcome this by using special-purpose hardware is not seen as a feasible solution by the authors, because of its overall high costs and difficult management within long-lived components.
  - Timed Efficient Stream Loss-tolerant Authentication (TESLA)
    The basic idea behind TESLA is described as delivering the subscriber key only after the message should already have reached every subscriber. TESLA depends heavily on time synchronization as the timestamps from the message and the key delivery are taken as additional evidence during verification. To reassure the subscriber that the key came from the right publisher, one-way hash chains are deployed that can, according to the authors, be generated at low computational cost. As the minimum latency depends

on the maximum distance of all subscribers to the publisher, significant latency is added regarding the possible point in time of authentication verification. Delaying messages may even result in denial-of-service. On the other side, the authors do not see time-synchronization as a real issue in the power grid because of the many other consequences of bad time-synchronization within the power grid.

- Time-Valid One Time Signatures (TV-OTS)
  According to the authors TV-OTS resembles TESLA in many ways, but as it uses public-key techniques it needs much effort for generation of new keys as soon as the end of a hash chain is reached. It has the advantage that no latency occurs by having to wait for keys to be revealed.

This analysis of available types of protocols is followed by their short assessment in terms of computational costs of sender and receiver, message size overhead, buffering, key size and total latency. The results can be taken into account when choosing the right solution for the special data delivery task in question. The authors let their paper end with the statement that "providing "one size fits all" authentication would be inappropriate for today's and tomorrow's power grids."

- Xiang Lu, Wenye Wang and Jianfeng Ma: "Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems" [91]

Summary: The authors had built up an experimentation lab for substation automation systems to test data origin authentication. Their main result is that the current security solutions (RSA, MACs and One-Time Signatures) do not suffice out-of-the-box on current power grid equipment. Their analysis offers hints for the design of new security elements for the Smart Grid.

A substation automation system is according to the authors not only the most critical system of the power grid but has as well strict needs for timely and accurate transmission of information. The interconnection of substation automation systems additionally means that failures caused by an attacker at one substation may spread to other substations as well. Thus integrity and authenticity of messages between interconnected power equipment is a must requirement. Another important point that is to be considered for substation automation is that message delivery is mostly done using multicast.

To test data origin authentication based upon RSA (1024 bit), MACs (SHA-1 based, two variants: incomplete-key-set scheme and TESLA) and One-Time Signatures (160 byte, (TV-)HORS: (time valid) hash to obtain random subsets), the authors chose an application scenario with GOOSE/SMV based relay protection and data sampling according to IEC 61850. For this the authors summarize timing requirements that range from 3ms to 10s depending on the type of message. The security challenge is stated as "to deliver a message with integrity protections within a pre-determined time period to multiple receivers". The experimentation lab used emulations on laptops that ran Ubuntu together with openssl as library for the authentication functionalities. Measurements were executed by counting the number of successfully verified messages that were delivered and verified in time. The following results are then stated by the authors.

Regarding RSA signatures the CPU frequency is a critical factor. RSA signatures are not suitable on current IED hardware for the 3 ms threshold, but may be used for thresholds larger than 10ms. From the authors' point of view, RSA is thus suitable for protection of information transmitted across substations, but not inside of them, at least for delay-sensitive teleprotection and data sampling.

If used in Ethernet-based architectures, solutions based upon MACs and HORS schemes in principal show satisfactory results regarding additional delay of messages even for the 3 ms threshold,. Concerning WiFi architectures, MACs and HORS schemes can only be

recommended as long as a throughput of at least 6 Mbps is available. HORS schemes are second in this scenario, because HORS signatures are longer compared to MACs. Next, the authors mention special constraints for TESLA, the Incomplete-Key-Set scheme and TV-HORS. All in all it is said that “OTS-based schemes, like HORS, are far from practical deployments, since the allowable reuse times of a key are still relatively low”.

The overall result of the paper is that there is a need for novel data origin authentication schemes that are able to fulfill not only security requirements but strict timing requirements as well.

- Qinghua Li, Guohong Cao: “Multicast Authentication in the Smart Grid With One-Time Signature” [89]

  Summary: As one exemplary use case for multicast communication within the Smart Grid the authors mention demand-side management when a control center multicasts a request to many home appliances. Other examples are in-substation and wired-area protection. Unicast is said to have its applications as well, but the focus of the paper is multicast communication. As multicast data often are control commands or measurement data, authentication is needed to avoid unauthorized commands and forgery. The authors then state requirements regarding multicast communication and multicast authentication in the Smart Grid. They argue that authentication needs to fulfill strict timing requirements of field devices with limited capacity, which rules out public key-based digital signatures like RSA or schemes like TESLA. They state that one-time signatures are promising for authentication, but current schemes are not specifically designed for the Smart Grid and lack e.g. strict timing requirements. HORS for instance does not suffice according to the authors because of its storage requirement concerning the public key and by its signature size of 130 bytes. Thus the authors propose a new HORS-based OTS scheme called “Tunable Signing and Verification” (TSV) that is argued to reduce the “storage cost by a factor of 8” and the signature size by 40% compared with existing [OTS] schemes”. TSV is then used as a basis for the definition of a multicast authentication protocol and its key management scheme. For distribution of initial public keys a secure distribution is assumed. Additionally a “loose time synchronization is required between the sender and receivers”.

  The storage and size benefit of the scheme comes from increased costs concerning signature generation and/or verification. The latter may nevertheless be flexibly allocated depending on the application. The authors consider applications like demand-response and wide-area protection most suitable for this.

- Jianqing Zhang, Carl A. Gunter, C.A.: “Application-aware secure multicast for power grid communications” [90]

  Summary: The authors argue that security and especially integrity of multicast messages will be a great challenge for the future power grid as standards like 61850 already incorporate multicast protocols (GOOSE, SMV) and as power grid communication migrates from closed to public infrastructures. They especially see a need for automatic and error-resistant configuration of devices because the heterogeneous and complex environment of the power grid is prone to misconfiguration by humans. Bearing the high latency requirements, the necessity for integrated group key management and the balance between efficiency, feasibility and cost in mind, the authors propose an “application-aware approach to setting up multicast groups for power grid communications using network layer security”. The “paper is [thus] focused on multicast configuration and group management using a formal model based on application data dependency”. From a technological point of view, IPsec-based multicast is proposed with an integrated link to application specific configuration of power substations.

  The authors formally describe a publish-subscriber multicast model that controls the multicast configuration based upon configuration files that represent data requirements of subscribers. The control is done using algorithms that detect configuration anomalies. Thereby the following

anomalies are defined and supported by algorithms: ownership anomaly, publication redundancy, source anomaly, and data dissatisfaction. An ownership anomaly means that data is published that is not owned by the entity. Publication redundancy means that data gets published that is not subscribed to or consumed by any entity. This may violate the principle of least privilege. A source anomaly exists whenever a subscriber requests a subscription from a source that does not exist in the system. Data dissatisfaction occurs in two cases. The first case means that not all data requested by a subscriber's request gets published. The second case means that the subscriber cannot receive all data using a single subscription. The latter case is again vulnerable to a violation of the principle of least privilege. Any anomalies detected during the design phase result in the need to revise the system's configuration.

The authors then describe their case study SecureSCL for 61850 substations. SCL as such allows to "obtain all information about the substation network topology, communication protocols, peer associations, and payload contents." SecureSCL integrates the anomaly detection algorithms and also a group policy and key exchange engine as well as an IPsec multicast module for the initialization and running phases. Thereby SCL is used as a basis and extensions concerning credentials and group management are specified. All this is then used to protect GOOSE on the network layer. The authors finally claim that the IPsec approach is able to maintain even high latency requirements like the 4ms barrier for substation networks of increasing size.

Although they represent only a fraction of scientific publications, the above listed publications already show that there are many issues to be considered when authentication shall be deployed within the different technical domains of the Future Internet based Smart Grid, especially within time-critical environments. They also show that currently there exists no general solution or approach that fits all environments and their specific constraints. The search for suitable authentication protocols in time-critical environments is ongoing. Even solutions that are currently deployed in some environments need to be analyzed again in regard to their applicability for future scenarios.

FINSENY in general analyzes forthcoming scenarios within the Future Internet based Smart Grid and almost all of them require some form of authentication. The Smart Grid will be built upon the current power grid that already gets adapted to future scenarios, at least regionally. Thus FINSENY has to take the available and even possible future security building blocks for authentication into account when analyzing its scenarios. If an authentication building block can be found, that fits to a certain set of requirements of a scenario use case, this building block should be used, if it is future-proof as well, i.e. if the current state of security analysis shows enough security margin for the future. If no building block is available for a special set of requirements, a new one has to be designed. For the latter task, design principles for Smart Grid security building blocks like the ones given by [87] are of special importance.

This document now lists possible security elements for authentication that may be used within the FINSENY functional architecture to fulfill authentication requirements. These security elements are divided into authentication elements that provide the prerequisites for authentication, and authentication services that use authentication elements to provide a service for entity or message authentication.

**Authentication Elements** for FINSENY may be:

- Passwords
  Passwords, or in general passphrases, are strings that have to be memorized and kept secret by their owner and are needed to access certain resources. The resource has to manage its database of valid passwords in a secure way as well. Passwords should be random and long enough to withstand brute-force guessing attacks. This is often supported by password policies (cf. 4.4.2.2.1)
- Software-based personal security environments (Soft-PSEs)

  Soft-PSEs are special data container that allow to store cryptographic keys in software. They use encryption technology based upon user passwords to secure the cryptographic key values stored within the PSE. Soft-PSEs need strong passwords and can only protect the storage of the keys while not in use. PKCS#12 [109] is a widely used standard for Soft-PSEs.
- Smartcards
  Smartcards offer the possibility to securely store keys or verification data like passwords in

hardware. Access to these secrets can be controlled on a fine-grained level. The secrets may be read out using secure channels or access may be restricted in a way that they can only be used to internally execute cryptographic functionality.

- HSMs
  Hardware security modules (HSMs) do comprise smartcards but may have many different form factors. HSMs are often used within business environments to speed up cryptographic computations while securely storing the secrets they use. HSMs also often implement some tamper-responsive mechanisms that are able to securely delete any secrets if a physical attack scenario occurs. The secret data stored in HSMs may be used for user or message authentication. Usage of the secret data can be regulated by various access control mechanisms.

- TPMs
  The Trusted Platform Module (TPM) may as well be seen as a HSM that is able to provide security functionality based upon the Trusted Computing Group (TCG) specifications (cf. [95]). Such a module may e.g. be used to support platform integrity and authentication. The current Trusted Computing Group Trusted Platform Module specification version 1.2 is published as ISO/IEC 11889 Parts 1-4 [96]. Usage of a TPM is restricted to the TPM API (see part 4 of the standard).

- Embedded security microcontrollers

  Embedded security microcontrollers are the core of smartcards or TPMs. They may e.g be directly integrated into embedded systems. However, it is to be checked whether the integration still provides the secure storage of secrets.

- FPGA/ASIC IP cores for authentication

  If a device is based upon an FPGA or ASIC design, a special IP core may be integrated that handles authentication. IP cores are reusable units licensed by their respective developer to a third party. The third party may then use the authentication building block within its own chip or FPGA logic design. Again, secure storage of secrets has to be analyzed individually.

- RFID token

  Radio-frequency identification mainly offers a contactless interface according to ISO/IEC 14443 for communication with a token (cf. [96] to [100]). The token in turn may offer authentication functionality using a security microcontroller. Security of the contactless communication is a special task for such token.

- NFC token

  Near-field communication comprises a set of standards for radio communication of devices that are brought into close proximity. These standards comprise ISO/IEC 14443 (cf. [96] to [100]), ISO/IEC 18092 [101], ISO/IEC 21481 [102], or ISO/IEC 15693 (cf. [105] to [107]). NFC allows two-way communication between the devices. The NFC Forum (http://www.nfc-forum.org/home/) additionally standardized data formats. A standard for NFC security is e.g. represented by ISO/IEC 13157 (cf. [103] and [104]).

- One-time password generator

  A one-time password generator represents a functionality that is able to compute one-time passwords locally for a client or entity in a way that they can e.g. be checked at a central server. The mechanism thus needs some kind of synchronization. This synchronization may be time-based or based upon some initial seed and counters that determine the list of acceptable passwords. It must not be possible to reuse already used one-time passwords. It must as well not be possible to compute a future one-time password based upon a list of already generated passwords with non-negligible probability. A one-time password generator may be realized in software or on a special hardware token.

- Authentication using physical unclonable functions (PUFs)

  PUFs are based upon some inherent physical property of a product that somehow provides randomness. As the randomness is intrinsic to the production and/or authentication process, a single instance of a PUF should practically be unclonable. Several realizations of PUFs were proposed, but some of them are broken (see e.g. [111], [112]). Different mathematical models

and definitions for PUFs are available. Apart from authentication, PUFs may as well be used within the context of secure key storage and key agreement. If a PUF is used directly within a challenge/response (C/R) protocol, a centralized approach and management of previously calculated C/R pairs are needed. If a PUF is used indirectly for secret key derivation, the derived secret key may be used within a state-of-the-art authentication protocol.

- Biometric sensors and corresponding software

  Biometric sensors are used to record a biometric feature that is later on used for authentication. A microphone and software that is able to process speaker recognition algorithms is one example. Another example is a fingerprint sensor that is able to process fingerprint minutiae.

**Authentication Services** for FINSENY that use authentication elements like the ones listed above, may be:

- User ID and Password

  "User ID and password" is certainly the most prominent and well-known authentication service today. It needs some database of valid pairs of user IDs and passwords. As storage of passwords in plain text results in a high security risk, passwords are often processed by a salted cryptographic hash function and only the output of this function is stored together with the salt. To compare a given password with the stored value, the same function gets executed again and the result is compared to the stored reference data. Passwords have to be handled securely at all time, otherwise the system is compromised. Thus the systems that process plain text passwords have to implement corresponding security measures and the password holder has to be trusted to securely manage passwords as well.

- User ID and biometric template verification

  This service is based upon some biometric feature and a corresponding sensor that are used by a software to generate biometric templates. These templates can be seen just like passwords with the distinction that the users do not need to remember their verification data and that the template can only be changed in a very restricted manner like one out of ten possible fingerprint templates. It has to be noted that there may be enrollment problems for certain combinations of biometric features and users. A quite obvious example is the usage of fingerprints for disabled persons that lost their hands. It also has to be noted that biometric authentication almost always raises privacy concerns of users.

- One-time password verification

  This service uses an infrastructure that is capable of handling one-time passwords to verify an entity. It may use a special infrastructure based upon some dedicated server or handles the verification locally. Special care has to be taken concerning synchronization of passwords to avoid denial of service scenarios. Examples for one-time password schemes are given in RFC 4226 (HOTP, [120]) and RFC 6238 (TOTP, extends HOTP by a time-based moving factor, [124]). These have been specified by the Initiative for Open Authentication (OATH, http://www.openauthentication.org/).

- Secrets on security chips controlled using passwords, biometric or PUF-based verification

  This service is based upon the secure storage functionality of a security chip that is able to process the secrets as well. Access control is done using passwords (or PINs), biometric or PUF-based verification of reference data. The possibility to provide correct verification data must be restricted to the user or group of users that shall be able to authenticate by using the securely stored secret. Integration of this service needs communication with the security chip. This may be done with the help of a middleware, that e.g. provides some PKCS#11 [109] interface, or by direct communication, e.g. via ISO 7816 [108] based APDU commands transferred using T=1 [108]. Common examples for this authentication service are current eID smartcards like the German electronic ID card that offer authentication functionality. Please refer to https://www.bsi.bund.de/EN/Topics/ElectrIDDocuments/eIDcard/eIDcard_node.html for further information on the German eID.

- Challenge/response protocols

Challenge/response protocols comprise a great number of protocols that have an interactive nature. They are based upon a challenge that is sent from one party to another party or a group of parties and the verification of a response that can only be given by some previously authorized receiving party. The range of challenge/response mechanisms goes from delivery of passwords to sophisticated cryptographic protocols based upon some intractability assumption. Thus challenge/response protocols are more a collective term for interactive authentication protocols.

- Kerberos based authentication

  Kerberos has been originally designed as a tool for protection of resources in distributed networks. Kerberos mainly uses symmetric cryptography, but initial authentication may be done using public-key cryptography as well (PKINIT, see [62]). Kerberos is based upon so-called tickets that allow access to services. Thereby an initially obtained ticket granting ticket is used to issue the actual service tickets. The ticket granting ticket itself, which expires at some specified point in time, gets issued based upon so-called initial authentication, which is the part of Kerberos classified as authentication service in the context of this document. In the Kerberos realm, this authentication service is part of the Key Distribution Center. See http://web.mit.edu/kerberos/ for further information on Kerberos.

- MAC based authentication

  A message authentication code is based upon a symmetric key that is used to compute a reference value over a message, which can only be verified against the correct message. This means that the receiver of a message and a corresponding MAC can only correctly re-compute the MAC based upon his own copy of the secret key, if the message he received had not been altered.

- IAM integrated authentication services

  Authentication services are a prerequisite for the access management part of identity and access management and may be managed using its identity management part. As the approach is able to use more than one specific authentication service provided by different parties, it is more a meta authentication service. The FI-WARE approach for instance uses exactly this type of meta authentication service for its Identity Management Generic Enabler (see sections 6.1.5.6 and 6.2.1 as well).

- Trusted execution environment based authentication

  This is another meta authentication service. Its characteristic lies within the execution environment that serves as a secure environment for the secrets used during authentication. The trusted execution environment has to provide all measures needed to separate the authentication service and its element from other services. Examples are realizations for smartphones that use virtualization to isolate a security relevant functionality from other functionalities.

- Extensible Authentication Protocol (EAP)

  EAP has been standardized by the IETF within RFC 3748 [118]. It can be seen as a general framework for authentication services over a network. It provides a protocol description and containers for the exchange of authentication messages between a client (EAP peer) and an authentication server (EAP server). The specific authentication mechanism that gets negotiated is called an EAP method. EAP has been designed for environments that do not provide the Internet Protocol (IP), e.g. when the Point-to-Point Protocol (PPP) is used or within WLAN environments. EAP-TLS (see RFC 5216 [119]) is a prominent example for an EAP method, especially within wireless scenarios.

- IEEE 802.1X

  IEEE 802.1X (see http://www.ieee802.org/1/pages/802.1x-2004.html) on the one hand specifies how to encapsulate EAP messages within IEEE 802 LANs, known as EAPOL (EAP over LAN). EAPOL takes place between the client (supplicant) and the authenticator that controls access to the network.
  On the other hand the authenticator uses RADIUS to communicate with an authentication server. In essence, authentication messages are exchanged between the supplicant and the authentication server, whereby the authenticator only grants access to the network after successful authentication, i.e. after an “accept” message from the authentication server.

- Challenge-handshake authentication protocol CHAP

  CHAP has been standardized for the Point-to-Point Protocol (PPP) by the IETF within RFC 1994 [113]. Two vendor-specific variants are published as informational RFC 2433 (MS-CHAPv1, [114]) and RFC 2759 (MS-CHAPv2, [115]) as well. CHAP uses a 3-way handshake to authenticate a client against a server. Incrementally changing identifier and random challenges are used together with a cryptographic hash function and a secret value known by both sides to authenticate the client. As CHAP uses symmetric secrets, RFC 1994 [113] assesses it as not very useful for large installations.

  Regarding MS-CHAPv2 the Microsoft Security Advisory 2743314 [127] needs to be taken into account before deployment.

- RADIUS / Diameter

  RADIUS and its extensions are standardized by the IETF in a number of RFCs. The Remote Authentication Dial In User Service (RADIUS) core RFC is RFC 2865 [113]. This RFC "describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server." RADIUS has been designed to be able to maintain only a single database of users. A so-called network access server acts as RADIUS client to a RADIUS server. Nevertheless a RADIUS server may act as a proxy to another authentication server as well. Diameter is an alternative to RADIUS that was designed to overcome some of its limitations. RFC 3588 [117] specifies the Diameter Base Protocol, which is currently under revision.

- TESLA

  Timed Efficient Stream Loss-Tolerant Authentication (TESLA) is a protocol that is designed for data origin authentication and thus also data integrity within multicast environments. It has been standardized by the IETF within the informational RFC 4082 [119]. The protocol needs to be bootstrapped by using a data authentication system like digital signatures and is based upon one-way chaining using cryptographic MACs and PRFs (pseudo-random functions). The sender has to buffer messages until it receives the key disclosure message. This leads to a delay before the messages can be accepted as valid messages. The delayed key disclosure after a pre-defined time is essential to the protocol. TESLA cannot provide for non-repudiation.

- OTS

  One-Time signatures shall offer an alternative to digital signatures based upon asymmetric cryptography. They are mainly based upon a one-way function, e.g. using a symmetric block cipher algorithm in practice, and are claimed to be more efficient than public-key based schemes. The security lies in the strength of the underlying one-way function. Many OTS schemes have been designed in the past. A prominent example that has been analyzed within power grid multicast environments (see beginning of section) is TV-OTS and its one-way hash chain branch TV-HORS (see [128] for both schemes)

- OpenID / OAuth

  OpenID (cf. http://openid.net/) is an open-source technology for web-based environments. An identity provider authenticates the user by e.g. password verification and then confirms this identity to websites that would otherwise need to start their own login process. OpenID is based upon HTTP(S) and its core protocol is called OpenID Authentication. "OpenID Authentication provides a way to prove that an end user controls an Identifier. It does this without the Relying Party needing access to end user credentials such as a password or to other sensitive information such as an email address." (Citation from the OpenID website) The OAuth protocol (cf. http://oauth.net/) as an open standard for authorization complements OpenID.

- SAML authentication assertions

  The Security Assertion Markup Language (SAML) has been standardized by OASIS. The current version is SAML v2.0 (cf. https://www.oasis-open.org/standards#samlv2.0). SAML uses XML to transfer authentication and authorization information about a user from one domain to another domain based upon some policy and trust relationship. SAML specifies amongst others a

so-called authentication assertion that transfers information about the identity of a user and the method that had been used to authenticate this user at a certain point in time. Assertions are digitally signed by their respective issuer.

- IEEE 802.1AE (MACsec)

  IEEE 802.1AE specifies media access control (MAC) security. According to http://www.ieee802.org/1/pages/802.1ae.html, the scope of MACsec "is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients (as specified in IEEE Standards 802, 802.2, 802.1D, 802.1Q, and 802.1X)." It has been designed to meet the security requirements of data communicated using Ethernet LANs.

- (D)TLS

  Transport Layer Security (TLS) is a widely used protocol for communication security over the Internet. It can be used to provide confidentiality and integrity of messages e.g. based upon mutual authentication. TLS is standardized by the IETF. RFC 5246 [123] represents the current TLS version 1.2. TLS uses a handshake protocol together with a so-called record protocol and needs an underlying reliable transport protocol like TCP. TLS is e.g. used by ISO/IEC 62351-3 [27] or ISO/IEC 15118-2 [17].

  The Datagram Transport Layer Security (DTLS) protocol (cf. RFC 6347 [125]) is a variant for datagram protocols like UDP.

- IPsec

  The core of Internet Protocol Security (IPsec) is standardized by the IETF as RFC 4301 "Security Architecture for the Internet Protocol" [121]. IPsec provides security services like authentication and confidentiality at the IP layer (IPv4 and IPv6). It essentially uses Security Associations (SA), the Internet Key Exchange (IKE) as well as the two protocols Authentication Header (AH) and Encapsulating Security Payload (ESP) that are also standardized by the IETF. RFC 4301 states that "The suite of IPsec protocols and associated default cryptographic algorithms are designed to provide high quality security for Internet traffic."

The lists above already comprise a great number of options that may be used to provide authentication elements and services to the FINSENY functional architecture as required by the scenario specific work packages WP2 to WP6. Nevertheless, the lists do not provide a comprehensive handling of all available options. The concrete scenario gives the constraints that have to be considered when choosing between all options available. As one could see by the analysis of current scientific literature at the beginning of this section, it may eventually even turn out that new solutions have to be designed.

As the FINSENY functional architecture in general follows the goal to take FI-WARE Generic Enablers (GE) into account before possibly designing domain specific solutions, the following subsection now summarizes the current scope of FI-WARE GEs that include authentication elements and services.

### 6.2.1 FIWARE GEs for authentication

From the list of FI-WARE Generic Enablers, the main item concerning authentication is the Identity Management Generic Enabler (see 6.1.5.6 as well). The FI-WARE security wiki (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Security) amongst others includes the following statement regarding the target usage of the IdM GE in the context of authentication:

"This enabler provides authentication/access control and identity/attribute assertions as a service to relying parties. […] Furthermore, the authentication feature of the enabler also covers the authentication of things for services, other objects or users as relying parties, and the authentication of users, services and other things for things as relying parties. It also supports user SSO across multiple things."

The functional description of the IdM GE within the FI-WARE security wiki (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FI-WARE_Security) adds:

"User Authentication: Provides a set of functionalities that a service can use to authenticate a user. There are a number of open standards that will be supported which include in a first phase: Open ID, OAuth, Oasis / SAML, user id and password.
Adaptation to specific API's or support of other standard interfaces might be considered on request."

The first version of the IdM GE takes a user-centric view (citation from http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Identity_Management_Generic_Enabler: “Identity Management (IdM) encompasses a number of aspects involved with users' access to networks, services and applications, including secure and private authentication from users to devices, networks and services, Authorization & Trust management, User Profile management, Single Sign-On (SSO) to service domains and Identity Federation towards applications. ”). The IdM GE may be self-managed or used as a cloud service. It shall provide “a bridge between IdM systems at connectivity-level and application-level”. The IdM GE supports user life-cycle management, which is a basis for credentials used in authentication protocols, e.g. by enforcement of policies. The Identity Provider within the IdM GE provides a native login as well as integration support for multiple 3rd party authentication providers. Single sign-on as well as federation shall as well be achieved by the IdM GE.

The authentication framework of the IdM GE “consists of the Extractor and the Authentication Pipeline. The Extractor extracts the authentication data from different sources. Each one of them is specialized in extracting a special kind of data. There exists a pipeline of authentication data extractors.” (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Identity_Management_Generic_Enabler).

The IdM authentication pipeline currently lists the following possible options (Source: http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Identity_Management_Generic_Enabler):

- **SAML** 2.0 using the following authentication flow:

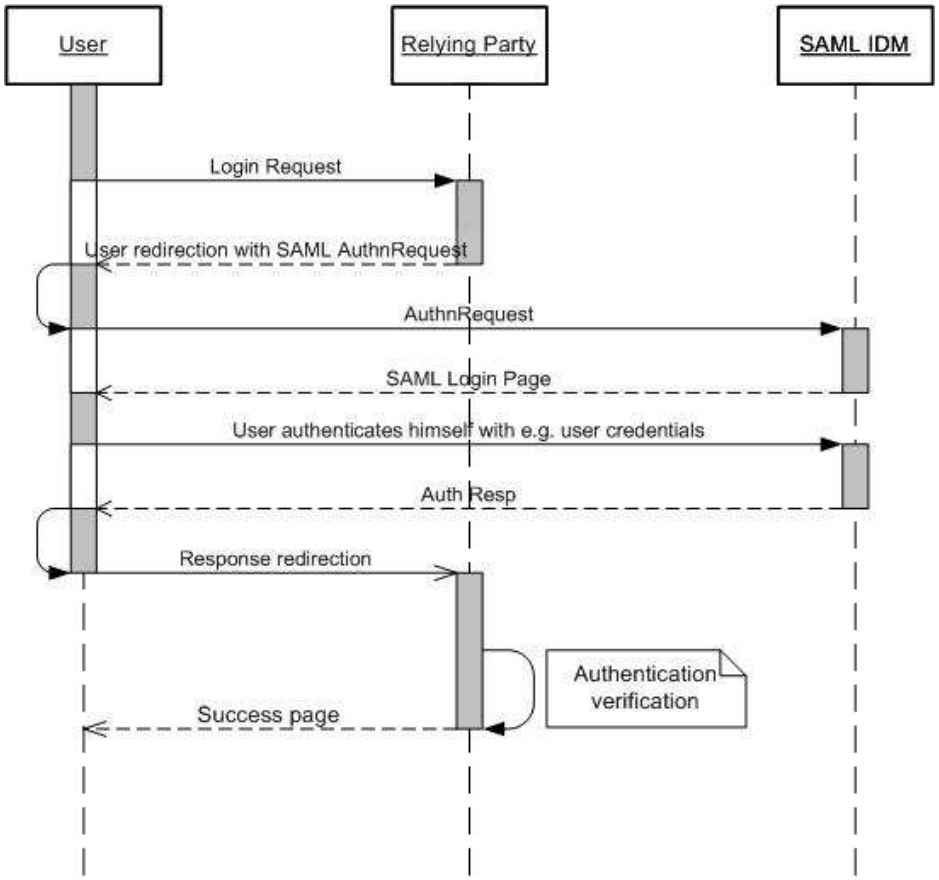


**Figure 30: SAML authentication flow by FI-WARE**

- **OAuth** 2.0 using the following authentication flow:

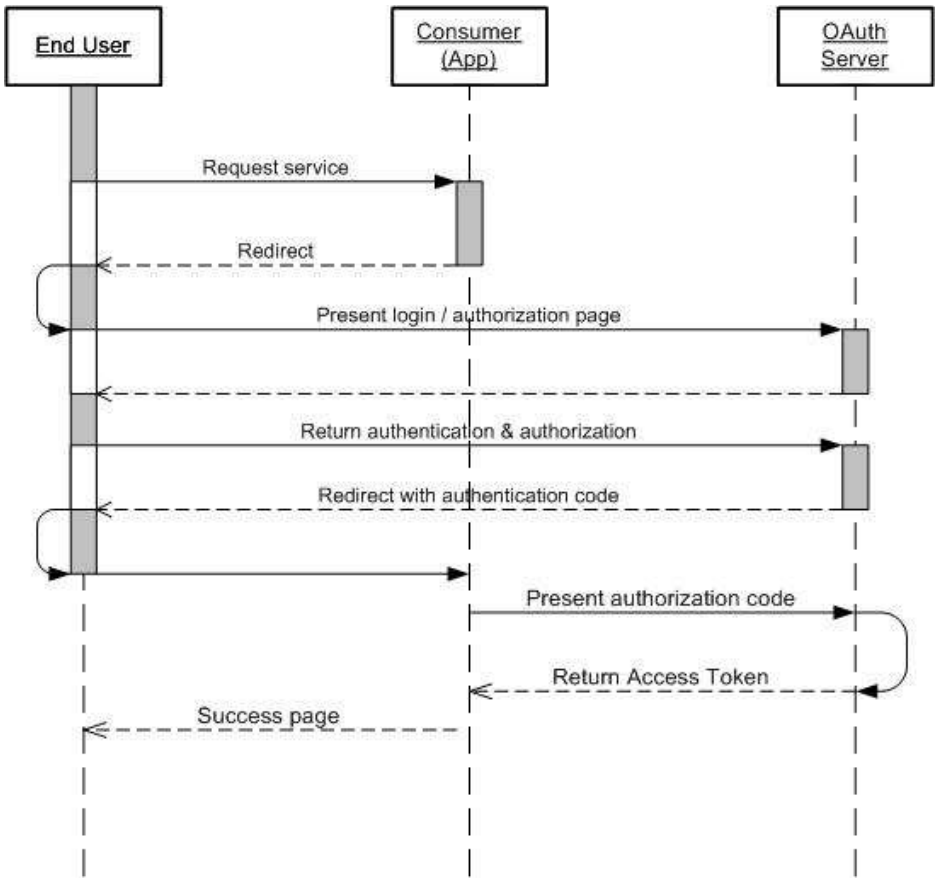


**Figure 31: OAuth authentication flow by FI-WARE**

- **OpenID** using the following authentication flow:

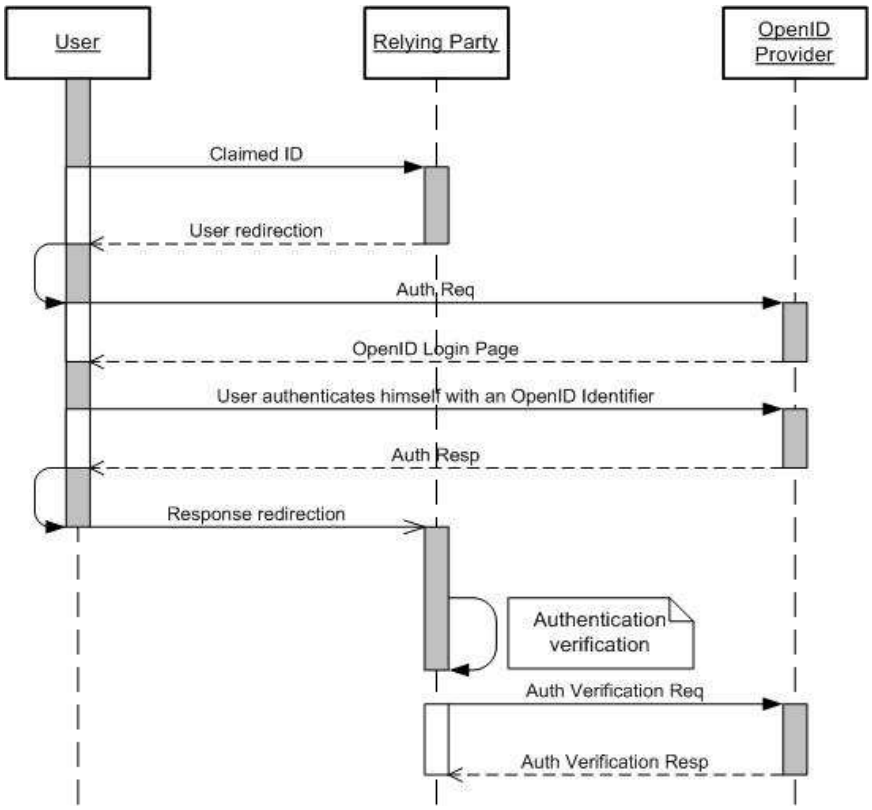


**Figure 32: OpenID authentication flow by FI-WARE**

- **Username / Password**

- eID – **smartcards** compliant to STORK (cf. http://www.eid-stork.eu)
  The following shows the access portal message flow when eID authentication is used:

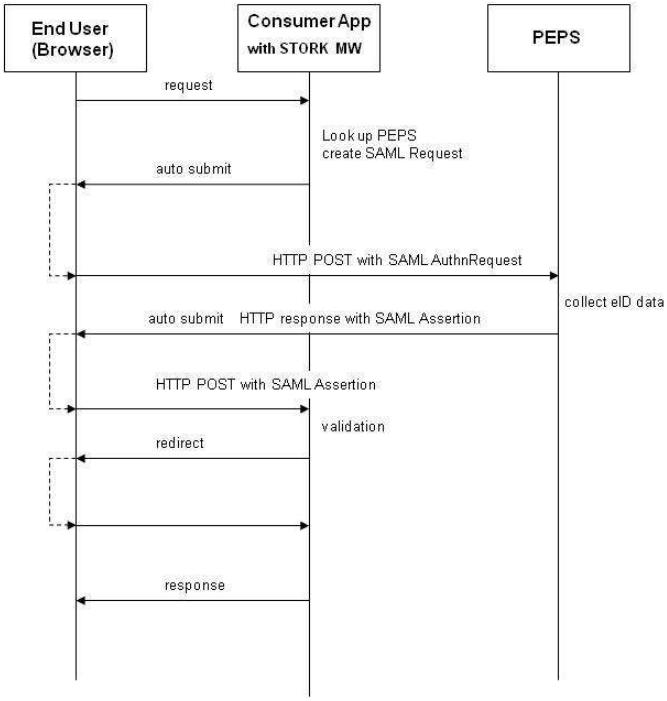


**Figure 33: STORK eID authentication flow by FI-WARE**

- **other**, i.e. flexibility to integrate further options for authentication.

Additionally, FI-WARE provides the following notes regarding authentication:

- within the current version of the FI-WARE Gateway Data Handling Generic Enabler: "Data Access Policy component is based on XACML (eXtensible Access Control Markup Language) supported by OASIS. Based on XML this standard provides access rights control based on policy rules without to manage directly authentication which could be assumed with SAML."

  (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.OpenSpecification.IoT.Gateway.DataHandling)

- within the current version of the FI-WARE Media-enhanced Query Broker Generic Enabler: "Authentication is NOT supported in Version 1 - This feature is foreseen to be incorporated in the future.
  At that time each HTTP request against the QueryBroker will require the inclusion of specific authentication credentials. The specific implementation of this API may support multiple authentication schemes (OAuth, Basic Auth, Token) and will be determined by the specific provider that implements the GE. Please contact them to determine the best way to authenticate against this API. Remember that some authentication schemes may require that the API operate using SSL over HTTP (HTTPS)."

  (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Query_Broker_Open_RESTful_API_Specification_%28PRELIMINARY%29)

Thus, from a point of view of authentication FI-WARE GEs support “user id and password”, Open ID, OAuth, SAML, and STORK eID smartcards. Whenever one of these authentication services is appropriate within the energy domain, it may be realized using a corresponding instance of a FI-WARE Generic Enabler.

## 6.3 Security aspects of an IPv4/IPv6 interworking

IPv6 has been defined to solve the address and other problems in the existing Internet Protocol and it is meant to replace IPv4 in the future. However, IPv4 and IPv6 networks are not directly interoperable. IPv6 is not backward compatible with IPv4, and IPv4 hosts and routers are not able to deal directly with IPv6 traffic and vice-versa. Transition from IPv4 to IPv6 requires change of technology where lots of infrastructure, both hardware and software, have to be upgraded and such a big shift cannot be done overnight. Both of the networks will coexist for years and to facilitate the shift, several interoperation and transition mechanisms have been specified, such as Stateless IP/ICMP Translation (SIIT), 6rd, Transport Relay Translation (TRT), NAT64, DNS64, 6in4, or 6to4.

During the transition time the nodes of IP network only run one of IPv4, IPv6 stacks or both of them. Basically they belong to the following categories:

- Dual stack (running IPv4 and IPv6 stacks simultaneously)
- Tunneling (IPv6 over IPv4 and IPv4 over IPv6)
- Translation (IPv6 to IPv4 and IPv4 to IPv6)

Coexistence and interoperation of IPv4 and IPv6 networks bring various security issues related to IPv6 protocol and the transition mechanisms. The issues are discussed in this section.

### 6.3.1 Tunneling mechanisms

Tunneling mechanisms (e.g. 6in4, 6to4, 6rd) have been mostly used for encapsulation interconnection of IPv6 sites over IPv4 networks. Unfortunately, sometimes tunneled IP traffic may not receive correct level of examination by network-based security devices unless such devices are specifically tunnel aware. This applies to all network-located devices or to any end-host-based firewalls whose existing mechanisms would not show them the IP packet stream after the tunnel client does decapsulation or before it does encapsulation.

Some of the mechanisms are vulnerable to packet injection what can be used e.g. for DoS attacks, or distributed reflected denial of service attack (DRDoS). The attacks are possible due to the fact that the tunneling endpoints do not have preconfigured association.

Tunneling makes possible service thefts in which an unauthorized malicious user may make use of some services. The situation is worse in case of UDP, as UDP may allow passing through NAT’s and firewalls, and especially when the datagram’s payload is encrypted (e.g. when IPsec or SSL/TLS is used) as there is no technique to examine the payload. In case of some of the mechanisms (e.g. 6to4) the routers are not aware of the fact whether relays are legitimate.

Spoofing, sniffing and eavesdropping of traffic going through tunnel may be possible in some cases, as in automatic tunneling all network receiving nodes accept and decapsulate packets sourced from anywhere (e.g. 6to4).

Some tunnel mechanisms (6to4, 6rd, ISATAP and Teredo) are vulnerable against DNS attacks in case tunnel end-points are discovered via DNS.

Some of the commonly used operating systems (e.g. Windows Vista) enable tunneling by default and if the end users are not aware of this autoconfiguration, the malicious traffic may bypass firewalls or IDS (Intrusion Detection System).

All the above issues do not imply that tunnels should not be used. It only means that they have to be used properly and the threats have to be mitigated. The measures that can be taken in order to secure the operation of IPv6 tunnels are discussed e.g. in [143].

There is no efficient mechanism for network-based devices which are not the tunnel endpoints. For that reason (if a network wishes to monitor IP traffic) to inspect the contents of all tunneled data packets, tunneling across (as opposed to tunneling in) the security boundary is not recommended. To provide an IPv6 transition solution, the network should provide native IPv6 connectivity or a tunnel solution that encapsulates data packets between hosts and a router within the network boundaries.

Another mean to mitigate the tunneling vulnerabilities is the setup of appropriate filtering at the tunnel end-points, e.g. regarding the source IPv4 and IPv6 address. Also IPsec for all tunnel traffic, but with additional security services such as authorization at the tunnels endpoints may be used to protect the ongoing traffic.

The mitigation methods often depend on the transition mechanisms. For instance some of the tunneling mechanisms like 6to4 can be secured by blocking an IP packet which contains 41 as protocol field value in the IPv4 header [129], while Teredo-based tunneling can be secured by blocking UDP port 3544. In general, manual tunneling is less vulnerable than automatic as it allows the administrator to establish a trust association between tunnel endpoints. The endpoints must be configured so that the encapsulated packets can get through of the security policy enforcement points (IDS, gateways, filters).

### 6.3.2 Translation mechanisms

To the most commonly used translation mechanisms belong such as SIIT, TRT, NAT64 or DNS. The framework for IPv4/IPv6 translation is presented in [139], while security issues are addressed in i.e., [137], [140], [141] or [142].

In general, IPv4/IPv6 translators can be seen as special routers and are exposed to the same risks, and can implement the same mitigations as in case of routers. However, one threat that directly derives from the practice of embedding IPv4 addresses in IPv6 is address spoofing. An attacker could use an IPv4-embedded IPv6 address as the source address of malicious packets. After translation, the packets will appear as IPv4 packets from the specified source, and the attacker may be hard to track. The mitigation is to implement reverse path checks and to verify throughout the network that packets are coming from an authorized source.

Some firewalls and other security devices filter traffic based on IPv4 addresses what enables an attackers to send IPv6 packets to or from IPv6 addresses that translate to the filtered IPv4 addresses. If the attack is successful, traffic that was previously blocked might be able to pass through the firewalls disguised as IPv6 packets. In all such cases packets that are sent to or from IPv4-embedded IPv6 addresses should be filtered as those directly sent to or from the embedded IPv4 addresses.

Protocols that protect IP header information cannot be used with mechanisms that translate network addresses. This means that e.g. end-to-end IPsec AH (Authentication Header) in both, transport and tunnel mode, cannot be used by SIIT or NAT64, while IPsec ESP (Encapsulating Security Payload) transport mode will fail unless checksum-neutral addresses are used. Different is the situation with ESP tunnel mode of IPsec where the translation is possible as tunnel mode ESP does not depend on header fields preceding the ESP header. End-to-end IPsec protection can be restored, using UDP encapsulation as described in [130].

The translation device itself can be a source of DoS attacks. For instance NAT64 device has a limited number of IPv4 addresses that it uses to create the bindings, so it is possible for an attacker to consume all the IPv4 transport addresses by sending IPv6 packets with different source IPv6 transport addresses.

### 6.3.3 Dual stack

IPv6-IPv4 dual stacks increase the potential for security vulnerabilities as their nodes must have two separate protocol stacks, IPv4 and IPv6, so have to face two infrastructures with specific security problems. This implies that consistent security policies have to be defined and implemented for both cases. Otherwise, if e.g. a firewall is not configured to apply the same level of screening to IPv6 packets as for IPv4 packets, the firewall may let IPv6 pass through to dual-stack hosts within the enterprise network, potentially exposing them to attack. In spite of the threats dual stack is often recommended (see e.g. [129]) as the transition mechanisms due to the fact that security issues of IPv4 and IPv6 are generally better understood and policy implementations can be simpler.

The threats can be mitigated by usage of firewalls and IDS with appropriate filtering and detection rules applied for both IPv4 and IPv6 protocol sites.

### 6.3.4 IPsec

IPv6 and IPv4 are using the same security mechanisms with regard to IPsec. The services are defined in [133] and [132], where IP AH and ESP are specified. Use of IP AH provides integrity, authentication and non-repudiation if used with authentication algorithms that provide encryption and digital signatures. Use of ESP provides integrity, confidentiality and authentication if used with authenticating encryption algorithms. IPsec can be implemented in a host-to-host transport mode, as well as in a network tunnel

mode. In transport mode, only the payload of the IP packet is encrypted and/or authenticated. In tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. IPv4 offers IPsec support but it is optional whereas in IPv6 its implementation (but not the usage) is mandatory.

The usage of IPsec in translation mechanisms has been already mentioned in the corresponding section. However, there are additional security issues related to the fact that IPsec in transport mode does not verify the contents of the payload itself. This means that e.g. in IPv6-in-IPv4 tunnels two nodes using IPsec transport mode can spoof the inner payload. The packet will be decapsulated successfully and accepted. As the IPv6 source addresses are carried in the payload it can be spoofed. This threat can be partially mitigated by IPv6 ingress filtering ([135]).

In case of IPsec tunnel mode used with IPv6-in-IPv4 tunnels, the outer IPv4 address may be spoofed. However, as the outer address spoofing may be irrelevant ([135]) as long as the decryption succeeds and the inner IPv6 packet can be verified to have come from the right tunnel endpoint.

### 6.3.5 Privacy

As user privacy is one of the biggest concerns related to Smart Grid security, it is important that privacy will not be degraded during and after transition to IPv6. IPv6, like IPv4, supports globally unique static IP addresses. However, in IPv4, IP addresses have no relationship to the addresses used for underlying data link layer network technologies, additionally NAT provided some privacy by hiding internal structure of private networks from potential intruders. A host that connects to a TCP/IP network using an Ethernet network interface card has an Ethernet MAC address and an IP address, but the two numbers are distinct and unrelated in any way. IP addresses are assigned manually by administrators without any regard for the underlying physical address. Different may be the situation in IPv6. There on system startup, a node uses IPv6 stateless address autoconfiguration to create automatically the IP address using EUI-64 address format using the network interface (MAC address). IEEE EUI-64 uses the MAC address as input to the algorithm that generates EUI-64 address for network interfaces. A global address for the interface is then generated by combining the network identifier with the EUI-64 address.

From an EUI-64 address, an attacker could potentially reveal the type and model of a remote machine as well as user activity, as most devices are used by a single user. To mitigate the risk, addresses can be created manually and non-predictable addresses should be created by making use of cryptographic algorithm (e.g. Cryptographically Generated Address) or assigning addresses dynamically with DHCPv6. However, even though the manually assigned address will not have the node's hardware info, it is (contrary to IPv4) usually global instead of local, which allows to identify and track a single user through the IP address.

[136] discusses concerns associated with the embedding of non-changing interface identifiers within IPv6 addresses and describes so-called privacy extensions to stateless address autoconfiguration that can help to mitigate those concerns for individual users and in environments where such concerns are significant. Use of the extensions causes nodes to generate global scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node. Privacy extensions are enabled by default in several operating systems (e.g. Windows, Mac OS X, some Linux distributions).

### 6.3.6 Configuration issues

Several operating systems enable IPv6 by default, e.g. Microsoft Vista (2007), Linux 2.6 kernel, Apple OS/10.3 (2002). Users/administrators may not be aware of this so protection against IPv6 attacks may not be in place. In addition, many firewalls permit UDP traffic, allowing IPv6 over UDP to get through firewalls without the knowledge of administrators. Some firewall products are only capable of filtering IPv4 traffic and not IPv6 traffic. Attackers can exploit this loophole and hence compromise the network by using IPv6 packets.

In some networks, e.g. home networks, it may be desirable to include devices which offer for IPv6 the same level of protection as NAT did for IPv4. This means adding a stateful firewall that has a default configuration that does not allow new connections from the outside, which allows inside devices to set up new connections and allow established sessions to communicate. The IETF has published [134] and [138] to explain how these devices should be configured.

For host security on IPv4-IPv6 mixed networks, it should also be noted that applications are subject to attacks in both IPv6 and IPv4 networks. In such scenarios, administrators should assure that packets sent to or from IPv4-embedded IPv6 addresses are subject to the same filtering as those directly sent to or from the embedded IPv4 addresses.

### 6.3.7 Best practices

To the main recommendation (see e.g. [130]) for best practices in maintaining secure IP networks during the transition time belong:

- Network designers should match their IPv6 policy to IPv4 IP policy options.
- Usage of dual stack as preferred migration choice, as the security issues for native IPv4 and IPv6 networks are better understood and policy implementation can be simpler. If that is not possible, tunneling mechanisms could be deployed to interconnect IPv6.
- Usage of static rather than dynamic tunneling as this allows the administrator to establish a trust relationship between endpoints.
- To inspect encapsulated traffic within tunnels, security devices that can understand tunneled traffic have to be deployed. Moreover, security policies should be enforced at both the inbound and outbound of the tunnel.
- Unnecessary services should be filtered at the firewalls.
- If traffic blocking is required, it is necessary to block traffic for both IP versions on any host control systems (firewalls, VPN clients, intrusion detection or prevention systems, and so on).
- Network traffic should be monitored, router and neighbor solicitations should be audited to detect the insertion of any rogue router or unauthorized device to the network.
- All IPv6 (IPv4) traffic on IPv4-only (IPv6-only) networks should be blocked.
- Host and application security should be maintained with a consistent security policy for both IPv4 and IPv6 networks.

## 6.4 Secure discovery and connectivity to Smart Grid devices

Service, neighbor and resource discovery are among the most important protocols for constrained resources self-organizing networks, including various sensor networks as well as the Home Area Networks (HANs), Building Area Networks (BANs), and Field Area Networks (FANs). Many discovery protocols exist, and in this section we try to identify which are the most appropriate for Smart Grids and the security that can be offered.

### 6.4.1 Neighbor discovery

IPv6 is a candidate of choice for Smart Grid communications. The Neighbor Discovery Protocol (NDP [150]) is used by IPv6 nodes on the same link to discover each other's presence, determine each other's link-layer address, find routers and maintain reachability information about the paths to active neighbors. More precisely, it defines mechanisms for solving the following problems:

- Router Discovery;
- Prefix Discovery;
- Parameter Discovery;
- Address Autoconfiguration;
- Address Resolution;
- Next-hop Determination;
- Neighbor Unreachability Detection;
- Duplicate Address Detection;
- Redirection.

NDP has no specific security mechanisms and is vulnerable to various attacks. The Secure Neighbor Discovery (SEND [151]) protocol is a security extension of the NDP protocol. Its intent is to provide an alternate mechanism for securing NDP with a cryptographic method that is independent of IPsec. In [152], the authors review the SEND protocol.

SEND offers three additional features to NDP:

- address ownership proof (Via cryptographically generated addresses CGA, so that the receiver can validate the proper binding with the public key);
- message protection;
- router authorization mechanism (using authorization delegation discovery to validate and authorize IPv6 routers to act as default gateways and specifies authorized IPv6 prefixes);

However, according to the authors, SEND faces limitations regarding computation, implementation, deployment and security:

- CGA and SEND security constraints (vulnerabilities in CGA verification, time-memory trade-off attacks, or attacks on router authorization, protection against address scanning);
- CGA privacy constraints (no big issues);
- computation exhaustion and bandwidth consumption;
- several implementations of the SEND protocols are available, but none have yet achieved a high quality level.

Finally, the authors make proposals to facilitate SEND deployment in order to mitigate the aforementioned problems.

### 6.4.2 Service discovery

Service discovery protocols aim to the automatic configuration and detection of devices, and the services offered by these devices. In many cases discovery is performed by constrained devices with limited power, memory and processing resources.

RFC 6272 [149] reviews the key infrastructure protocols of the Internet Protocol Suite for use in the Smart Grid. It has a dedicated section to service and resource discovery and states that service discovery is most often concerned with the resolution and distribution of host names via multicast DNS ([156]) and the automatic location of network services via DHCP, the DNS Service Discovery (DNS-SD [157]) and the Service Location Protocol (SLP [160]).

Multicast DNS and its companion technology DNS-SD were created to provide IP Networking with ease of use and autoconfiguration. Multicast DNS is very similar to the existing DNS protocol, reusing structure, syntax and operation codes of the protocol, but without configuring a traditional DNS server. The client machine sends multicast query messages to all the hosts on the local network, and the host replies with a multicast message announcing itself. DNS-SD is the other half of the solution, and specifies how DNS resources are named and structured to facilitate service discovery (it is compatible with both multicast DNS and existing unicast DNS).

The internet drafts for DNS-SD and multicast DNS both have a security considerations section. They propose for the participating nodes to use IPsec signatures and/or DNSSEC [158]. The MITRE Corporation (http://www.mitre.org) has published a technical report on securing the multicast DNS [159]. They state that DNSSEC is inadequate for securing multicast DNS and that DNS CERT records would be a better solution. According to the report, DNSSEC fails because it requires a hierarchical trust structure, and this would require at some point two nodes to trust each other if there is no pre-existing direct trust between each other. The paper also opens future research topics, especially for specifying a system that could discover a service and then query for its trusted identity.

The Service Location Protocol (SLP) provides a scalable framework for the discovery and selection of network services. Client applications are modeled as User Agents and services are advertised by Service Agents (the Directory Agent provides scalability to the protocol). Each service has a URL that is used to locate the service and the services are grouped together using scopes. The basic idea is that User Agent sends a unicast request for a service, to which the Service Agents unicast a reply containing the service's location. SLP contains a mechanism for signing service announcements but is rarely used. [161] provides an overview of security of SLPv2, including authentication using digital signatures, authentication block, signature generation and verification, and discusses it. It proposes some modifications to the specification against replay attacks, and discusses about the difficulty for establishing key information trust.

### 6.4.3 Resource discovery

Resource discovery aims at the discovery of resources offered by end-points and is especially important in machine-to-machine applications, with no human intervention. The goals are:

- simplicity of creation and maintenance of resources;
- commonly understood semantics;

- conformance to existing and emerging standards;
- international scope and applicability;
- extensibility;
- interoperability among collections and indexing systems.

RFC 6272 [149] foresees Constrained Application Protocol (CoAP [153]) as the main protocol for dealing with these goals. CoAP is an application layer protocol intended to be used in very simple electronic devices that allows them to communicate interactively, and is targeted for small low power sensors, switches and similar components that need to be remotely controlled or supervised.

CoAP provides both unicast and multicast resource discovery, which is achieved through well-known resources that describe the links offered by a CoAP server (for example a query such as [GET /.well-known/r?n=Voltage] returns the resources with the name Voltage). CoAP makes the assumption that all CoAP servers listen on default port or have been discovered using some general service discovery (see previous section).

CoAP base specification outlines how to use DTLS (Datagram Transport Layer Security) and IPsec for securing the protocol but [154] provides an overview of papers dealing with CoAP security and outlines some challenges regarding implementation difficulties, practical provisioning problems, and layering and communications problems. It also proposes a deployment model, security architecture and an initial sketch of protocol extensions for tackling these problems.

In “Security for practical CoAP applications: Issues and Solution Approaches” [155], two security issues related to end-to-end security and secure group communication are discussed, as well as possible solutions.

So far, security for CoAP is still an active research field, and no fully specified secured version of the protocol has been found.

## 6.5 Migration aspects when introducing security

Ideally, every system should consider security from the design phase (see 4.4.13). Unfortunately, these rarely happens in practice, for various reasons like building on existing technologies, lack of time / budget, … Moreover, the security of a system should be reconsidered during its lifetime, due to:

- evolution of security standards and best practices;
- discovery of new vulnerabilities that might need updating software or lead to the obsolescence of used technologies;
- migration of technologies to newer ones, implying the need of reconsidering the security of the system;
- new regulations and laws occurring during the lifecycle of the system;
- …

It is thus often necessary to consider migration aspects when introducing new security controls. This process is much easier when using a systemic approach to system security. Moreover, such migrations are rarely seen as “value-added” activities, but rather as a “necessary evil”, therefore makes necessary to bring together all the pieces of the puzzle, from staffing, vendor support to tests and performance metrics. The following steps are often taken to realize the introduction of new security into a system:

1. definition of security measures to apply to the system;
2. planning for the integration;
3. testing of the new security elements in lab environment;
4. integration into legacy system, possible backups;
5. verification of the upgraded system (tests and performance metrics).

### 6.5.1 Information system security review

This step is used to identify the changes made necessary by developments in the information systems or the threats that face them. It shares a lot in common with the threat and risk assessment methodology introduced to identify FINSENY security requirements, since it considers the different assets and the corresponding security requirements in order to identify the attacks to consider, the potential damages and the implied security counter measures.

There are some differences though, that need to be considered:

- Existing architecture, hardware and software used in the system: the threat and risk analysis is not performed during the system definition phase, but is based on a running system.
- Also the practical security assessment is not performed during the test phase, but in the operational phase
- Necessity to take into account the expertise and resources available
- Necessity to take into account the costs of the possible countermeasures and what the most important priorities are
- Capitalization of the experience gained from having used the system in production (known exploitation and security problems / difficulties)

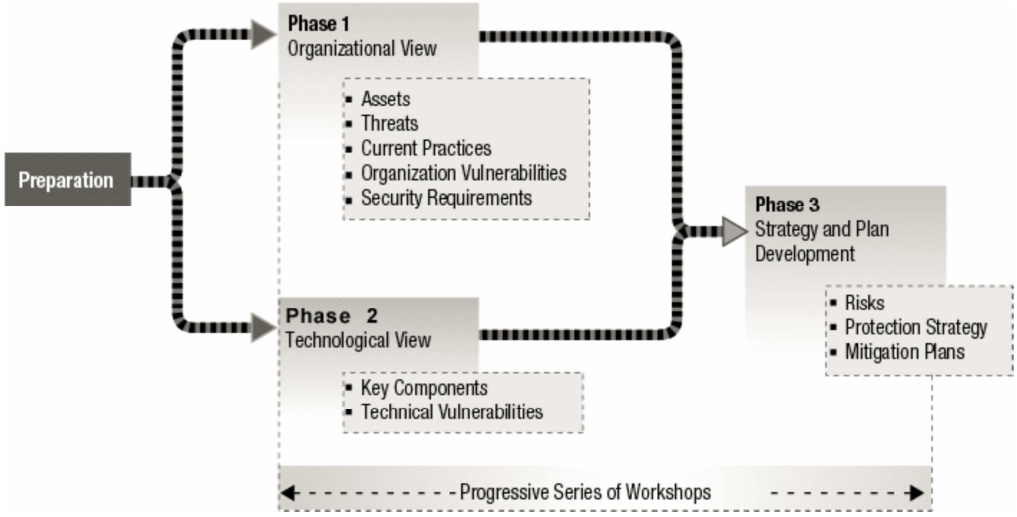


**Figure 34: Three OCTAVE method phases**

Different methods exist in order to achieve the information system security review. For example OCTAVE [146] (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques and methods for risk-based information security strategic assessment and planning. The SKiP [148] method (Security Knowledge in Practice method) is a method developed at the CERT Coordination Center using 7 steps to secure network software, harden a network and improve a system based on a review of events.

### 6.5.2 Strategy and plan development

The next phase consists in preparing a plan for mitigating the risks that have been identified, prioritized by their impact, importance and feasibility.

The main goal of this strategy is to minimize, to the lowest level possible, any risks to an organization while still managing to maintain the optimum behavior of the system. The plan will also track progress of the implementation of the security controls, prepare future evolutions of the system, that is be sure that the security of the system is regularly assessed and that the upcoming needed changes are foreseen as early as possible.

One example of such constraints could be for access control. While smartcards solutions are valid, their PUSH model puts the role information in the smartcard. An easier to implement solution might be to use a central repository, from which the role information can be fetched, while the user authenticates with username / password.

Another important thing to take into account is the possibility to rollback to a previous state if the migration of one of the aspects is inconclusive. For example, it should be possible for the previous example to disable authentication if problems occur. For data migration, the old data source should be backed up, and interfaces and processing occurring on the source shouldn’t be discontinued and activated on the target before the new data source has been verified.

During this design phase, a number of tools are developed in order to facilitate and verify the migration:

- Tools used for migration (such as data transformation tools when migrating data)
- Tools for testing the good behavior of the system (like correctness of migrated data, correct authentication, performance tests, …)
- Definition of the acceptance tests for the go / no-go decision and / or rollback decision

### 6.5.3 Applying new security controls

Security controls can be more or less hard to implement, depending on their impact on the architecture of the system. To various degrees, following milestones occur:

- Tests in lab environments
- Deployment phase
- Running acceptance tests
- Possible rollback

Usually, corrections required to host based vulnerabilities are the simplest ones, since they involve few interactions with external components. They must of course be tested beforehand in lab environment before being applied to production systems. This is especially the case for host system protection components like antiviral software, application layer firewalls, host based Intrusion Detection Systems … and for system patching / system updates. They usually require no or only low downtime for the system. For some cases though, this might be more tricky, e.g. for critical systems measuring data in real time, which could require to plan balancing on other systems.

Network based countermeasures like firewalls, network IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) have more impact on the network. Also every update / change in the protocols used most of the time requires intensive tests driven in lab environments before being applied to the production system, and may imply significant downtimes.

Data migrations imply minor downtimes, as it is often possible to migrate the data from one source to another and check if the migration has occurred correctly while still having data interfaces and data processing occurring on the old source.

Once a migration has occurred, several tests have to be carried out (covering of course the correct behavior of the new system, but also more indirect metrics like performance). These tests should be defined in the previous phase and can lead to a go / no-go decision (for example before switching a data source), or a rollback decision (if things are not working properly anymore). On a more global level, the overall progress of the security migration is tracked and migration plan might be updated accordingly.

## 6.6 Security technologies to protect customer privacy in Smart Grids

### 6.6.1 General approach: Privacy by design

Assuring privacy protection by complying with legal frameworks only is a quite difficult task, especially since privacy protection legislation may differ from one country to the other. Privacy by design offers alternatives to build privacy protection in products and architectures from the ground up. The idea is to embed privacy protection into the design specifications of IT systems, business practices, and physical design. This may be achieved by following the foundational principles defined in [144]:

1. proactive not reactive; preventative not remedial;
2. privacy as the default;
3. privacy embedded into design;
4. full functionality – positive-sum, not zero-sum;
5. end-to-end security – lifecycle protection;
6. visibility and transparency;
7. respect for user privacy.

One the one hand, the privacy by design approach covers the use of mechanisms to evaluate systemically system designs and practices in regard to privacy in order to correct them prior to any operation. A way to achieve this is, for example, to carry out a so-called data protection impact assessment (DPIA) in order to assess the privacy risks which may occur while deploying new Smart Grid systems or changing existing ones. For this purpose, EG2, the expert group of the Smart Grid Task Force (SGTF) responsible for regulatory recommendations for privacy, data protection and cyber-security in Smart Grids has defined a DPIA template for Smart Grid environments [145]. The following threats to be assessed have been identified by EG2:

| Data protection threats | Examples |
|---|---|
| Unspecified or unlimited purpose | (1) Collecting, storing and using a client's load profile data without clear specification of the purposes for which the data may be processed;<br>(2) Collecting data for the specific purpose of billing the client but later deciding to reuse it for profiling individuals for marketing purposes. |
| Collection exceeding purpose | Collecting more detailed load profile data for the purpose of monthly billing, where much less detailed data would be sufficient to achieve the same objective. |
| Incomplete information or lack of transparency | Information available to consumers that lacks clear information on how data is processed and used, the identity of the operator, or the user's rights. |
| Combination exceeding purpose | Information in smart metering load profile used for billing is combined with personal data obtained from a third party. |
| Missing erasure policies or mechanisms; excessive retention periods | Detailed metering data is kept in a database for longer than necessary to achieve its purpose and/or longer than required by law, for example, because of the absence of automatic deletion of obsolete data or because excessive retention periods have been established, without due regard to data protections requirements. |
| Invalidation of explicit consent | (1) Customer is only offered significantly higher tariffs unless he accepts the use of his load profile data for marketing purposes;<br>(2) Customer is not informed of the possibility that his load profile data may be disclosed to third parties for marketing purposes when requested to opt in to half-hourly readings;<br>(3) Customer is required to give consent to detailed (e.g. half-hourly) meter readings even when he does not wish to sign up for a time-of-use tariff. |
| Undeclared data collection by Smart Grid operator | Reading of detailed load profile without the awareness of consumer. |
| Lack of granting access to personal data<br>or<br>Inability to respond to requests for subject access, correction or deletion of data in a timely and satisfying manner. | Consumer does not have access to his personal data stored at utility. |
| Prevention of objections | Consumers cannot opt out to reading of detailed energy load profiles. |
| A lack of transparency for automated individual decisions | Remote disconnect is performed without clear explanation provided to the user on the reasons why. |
| Insufficient access control procedures | After a change of supply the former supplier has still valid access credentials to read out meter data. |
| Insufficient information security controls | The profile is not end-to-end encrypted and data could be read and processed by unauthorized third party, e.g. a network provider. |

| Data protection threats | Examples |
|---|---|
| Non legally based personal data processing | A Smart Grid operator shares collected information with a third party without notice, consent or as otherwise legally allowed. |
| Insufficient logging mechanism | It is not logged who has accessed the meter load profile. |
| Breach in security implementation | A faulty implementation of security mechanisms (locally or on a centralized server) enables hackers to access a memory area containing identifiable meter load profile history. |
| Unjustified data access after change of tenancy or change of supply | In case the tenant changes, the data from previous tenant is made available to the new tenant.<br>In case of change of supply, old supplier still has access to data. |
| The protection of data is compromised outside the EU | |
| Smart Grid data is processed by government departments, local authorities and law enforcement agencies without a legal basis. | Police may need data when investigating possible criminal activity within a household or a tax authority may wish to know whether a house is unoccupied, used as a primary or secondary residence, or rented out. |
| Lack of unification in subject access requests mechanisms | |
| Lack of quality of data for the purpose of use | For billing on a daily basis data should be registered on a daily basis.<br>For cutting of electricity supply the location and reasons should be conclusive. |

**Table 9: Data protection threats (source: [145])**

On the other hand, privacy by design implies minimizing the collection, use, retention, and disclosure of personal data and setting as default the highest privacy protection level possible. This means, for example:

- if not required for the stated purpose, no collection of identifiable information at all, but only pseudonyms, or even better anonymous data;
- minimized retention by not recording or storing personal data if not needed;
- minimized retention by destroying personal data as soon as the transaction for which they are needed is completed;
- appropriate measures to ensure that personal data are only used for the stated purposes (e.g. sticky policy – see section 6.6.2);
- installation of required functionalities only, to avoid excessive data collection;
- no implementation of functionalities not required for the defined data processing purposes (e.g. profiling) or reliable blocking against unauthorized use;
- proper erasure procedures by erasing unencrypted data in the persistent memory of malfunctioning devices before they are given to external maintenance service and by overwriting data carriers several times or physically destructing them;
- schedules for the erasure of personal data;
- no transfer of the source data, but of the results only;
- no transfer of the source data to a central system, but directly from source to end.

Moreover, privacy by design also covers the effective integration of privacy protection measures into the design and architecture of IT systems and business practices so that they do not reduce the functionality of the whole system and cannot be bypassed. Regular audits should be planned accordingly to verify the protection level achieved by the measures in use.

Additionally, strong security measures are essential to privacy. Organizational measures include, for instance, the definition of appropriate security policies and the information of employees about the defined security measures followed by regular training sessions. A comprehensive list of technical measures is provided in section 5.1, including state-of-the-art IT security measures for storing and transmitting personal data in a secure way.

Finally, privacy by design requires systems and operations to be transparent to users. This may be done by setting strong privacy defaults, providing user-friendly options, giving the individual control over his data, for example by a secure web portal, etc.

Based on all these privacy by design principles, some FI-WARE Generic Enablers will be first examined in regard to privacy and some innovative solutions dedicated to Smart Grids will then be presented.

### 6.6.2 FI-WARE GEs for data privacy protection

In this section, some FI-WARE general enablers providing services which may be used in Smart Grids to preserve data privacy will be discussed.

The **Privacy GE** is not expected to provide external functionalities, but enhances the functionalities provided by the Identity Management GE and the Data Handling GE in regard to data privacy protection. However, it will not be part of the first FI-WARE release and only little documentation is available yet at http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Privacy_Generic_Enabler.

The **Identity Management GE** has already been presented extensively in sections 6.1.5.6 and 6.2.1. In the second FI-WARE release, it will offer privacy enhanced user management and authentication functionalities, but these are not documented yet. Currently two Identity Management GEs are available in the FI-WARE catalogue:

- The Global Customer Platform (GCP) of Deutsche Telekom (https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Identity_Management_GCP_-_User_and_Programmer_Guide - see also section 6.1.5.3)

  GCP is dedicated to webshops. In general, it performs authentication on the basis of the OpenID (2.0) protocol. Moreover, it includes a customer self-care service which gives the user the possibility to administrate his personal data in a very transparent way.
  However, as it is offered as a Cloud service, careful attention should be paid prior to the use of the service in FINSENY. As only little information is available, it is not clear how personal data (incl. login data) are transmitted, nor where and how they are stored. Therefore, it should be verified that customer data are transmitted and stored securely and that only authorized instances (i.e. content provider, the customer himself) have access to personal data. Generally, the cloud provider must not have access to data without a contract stating the necessity and purposes of data handling.

- One-IDM of Nokia Siemens Networks (https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Identity_Management_One_IDM_-_User_and_Programmer_Guide and see also section 6.1.5.2)

  OneIDM is also dedicated to webshops. It offers SAML authentication based on username and password. As no documentation could be found regarding data protection, no evaluation statement can be made at the present time.

The **Data Handling GE** provides a mechanism for controlling the usage of data in client/server applications by ‘sticking’ a data usage policy to the data to which it applies. The policies are expressed using PPL (privacy policy language). Prior to data access by an application, a matching is done between the intended use of the data and the policy. If a third party server then wants to collect some data from the data controller server, a filtering is performed, according to the sticky policy attached to data.
In the current FI-WARE catalogue, one Data Handling GE is mentioned, having been developed by SAP (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Data_Handling_GE_-_User_and_Programmer_Guide). Its matching with the privacy policy is depicted in the following figure:

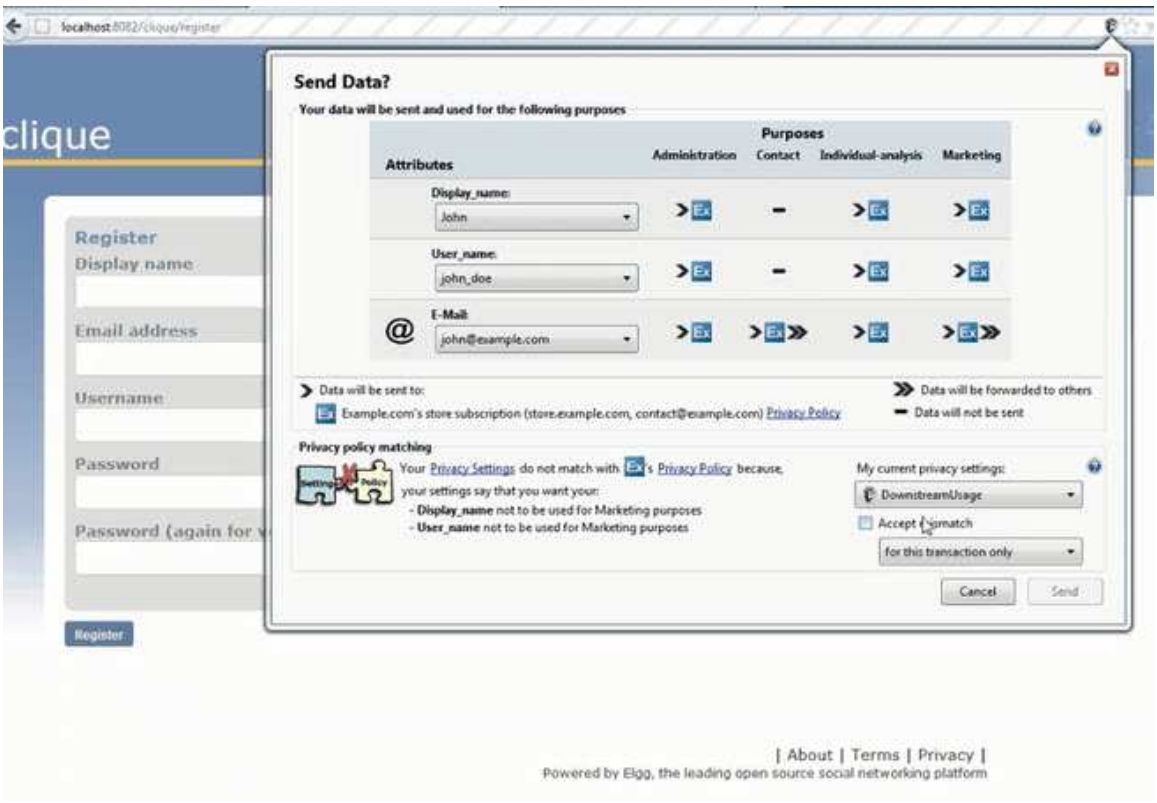


**Figure 35: Privacy policy matching of the Data Handling GE (picture from FI-WARE website)**

Such a technology has the advantage to give users transparency on the handling of their personal data. Though, the specification of a suitable policy may not be straightforward since privacy preferences settings are often specific to a given type of personal data. This might especially become very complex when data might be shared or not between different data controller and third-parties. The mechanism also requires that a dedicated Data Handling GE is available for each involved instance (i.e. client, data controller server, third-party servers), without direct access to the stored data. Essential is also that the link between the sticky policy and the data is preserved during communication, storage in databases and further data sharing.

The **Context-based Security & Compliance GE** aims at supporting additional security requirements requested by end user applications (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Context-based_security_%26_compliance). The concept is based on requests of applications including their requirements and a context description to obtain from the GE the security solutions that best fulfill them. Such security solutions must be registered in the FI-WARE marketplace and describe their features by using the USDL-SEC language to be successfully discovered by the GE. As the security service is deployed into the end user environment, the GE also instantiates a runtime monitor which detects anomalous behavior or non-conformance. This GE would be particularly interesting to fulfill specific requirements of national data protection laws and check their enforcement. Nevertheless, it will not be part of the first FI-WARE release and no information is provided about the security services which will be available then.

An optional security enabler which may play a role in preserving policy is the **DB Anonymizer** (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Optional_Security_Enablers.DBAnonymizer), a SAP tool checking in anonymized databases whether personal data are still included and if data correlation may possibly lead to re-identification. It needs as inputs a database dump of the data to be tested and an XML policy file specifying what might be disclosed or not. This GE might be interesting for FINSENY to evaluate anonymization functionalities if some are being used or developed. In such a case, a first check should be made prior to operation and then, at regular time intervals to verify the suitability of the anonymization policy since data and applications may evolve with time. The DB Anonymizer GE is provided as a web service. Ideally, all checks should be better carried out locally and by the data owner only to avoid any data leakage in case of insufficient anonymization.

A further optional security enabler which may be interesting for data privacy protection in FINSENY scenarios is the so-called **Secure Storage Service** (http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.ArchitectureDescription.Security.Optional_Security_Enablers.SecureStorageService), an application-level filter which authorizes read access depending on the identity of the requester and on the sensitivity of the requested data. It assumes that data are labeled as private or public for instance before being stored. No implementation is currently available in the FI-WARE catalogue.

### 6.6.3 Domain-specific measures for data privacy protection

Smart meters play an essential role in Smart Grid infrastructures. On the one hand, frequent meter readings will be very useful to optimize the grid, but on the other hand, such a monitoring of electricity consumption also introduces the possibility of collecting detailed information on personal activities and behaviors at home (e.g. when the occupants are at home, when they are asleep, etc.) based on their electricity usage profile and using it for other purposes than for supplying electricity, which would be against data privacy protection legislation.

Designing smart meters and the related infrastructures according to the privacy-by-design principles presented in section 6.6.1 is the objective of some current research on privacy-preserving metering protocols and components. As smart meters have got rather limited bandwidth and computation resources, such protocols and components are designed to put as less workload on the meters themselves as possible, while preserving the privacy of consumption profiles.

For example, [162] describes a privacy-enhancing smart meter architecture consisting of household smart meters, neighborhood gateways, and remote utility servers. Meters readings are transmitted to utility companies by the neighborhood gateways, without revealing their origin. Any communication between the architecture components takes place over a secure channel. The utility servers also communicate once per billing cycle with the smart meters via a Zero-Knowledge protocol to negotiate billing: “The protocol allows a smart meter to report its bill, computed from fine-grained measurements, without revealing how or when electricity was used, while guaranteeing to the provider that customers do not under-report their usage.” [162].

A similar approach is presented in [163]: so-called data concentrators in the neighborhood can get aggregated measurements of all connected customers in the neighborhood without revealing the individual household meter readings. The implemented protocol relies on homomorphic encryption and additive secret sharing to preserve the privacy of individual meter readings. By comparing the aggregated measurements with the actual neighborhood consumption, fraud can be detected.

A further approach based on meters and aggregators computing the sum of consumption or comparing it to a given value is provided in [164]. Four different protocols are presented: “(1) a protocol that offers unconditional security based on secret sharing; (2,3) two protocols based on Diffie-Hellman key exchange that allow blinding to be verifiably done outside the meter; (4) finally a protocol based on computations on the meter, but with negligible communication overhead.” [164].

In [165] a set of privacy-preserving protocols between an energy provider, a user agent, and a tamper-proof smart meter is presented, using commitments and zero knowledge proofs to prove the correctness of bills in a privacy-preserving manner. The smart meter outputs certified readings to the user. For billing purposes, the user combines those readings with a certified tariff policy. The bill is then transmitted to the energy provider together with a zero-knowledge proof ensuring that the bill is correct.

Similarly, [166] introduces a plug-in privacy component which intercepts smart meter readings, removes the plaintext consumption profile, then uses external tariff information to calculate the billing amount, and finally sends invoice, the signed commitments and a Zero Knowledge proof to the energy provider. The actual consumption profiles are not communicated to the provider (or to any other third party).

Additionally to the general privacy-by-design principles, the following general recommendations given in [167] are especially applicable to smart meters:

- Personal data should be used as less as possible and only the ones necessary for the given services. This is even more critical for data to be provided to third parties. For instance, neighborhood average computations may not need the exact location, but only the first digits of a zip code.
- Pseudonymized or even better anonymized data should be used whenever possible instead of the real name of the individual.

- Secure channels of transmission are necessary along the Smart Grid.
- End users must have control over the data which are transmitted to third parties.
- Third parties should commit themselves to the non-correlation of data without the user's consent.
- End users should receive clear instructions from the energy provider and third parties on the privacy safeguards available (e.g. login based on user name and password), on the way to access or delete their personal data.

Electric vehicle charging is another example of Smart Grid scenarios where personal information of the user (vehicle owner or driver) is collected, e.g. for billing purposes. Besides, further value-added services may be offered to users based on the extensive information and communication infrastructure of charging spots (see Figure 36). Vehicle, user, charging spot and service provider must communicate with each other. The generated and exchanged information provides very informative insights into the user's privacy. A combination of these data may result in user profiles disclosing habits (e.g. daily charging near a HIV clinic), special inclinations (e.g. visiting certain shops), etc.

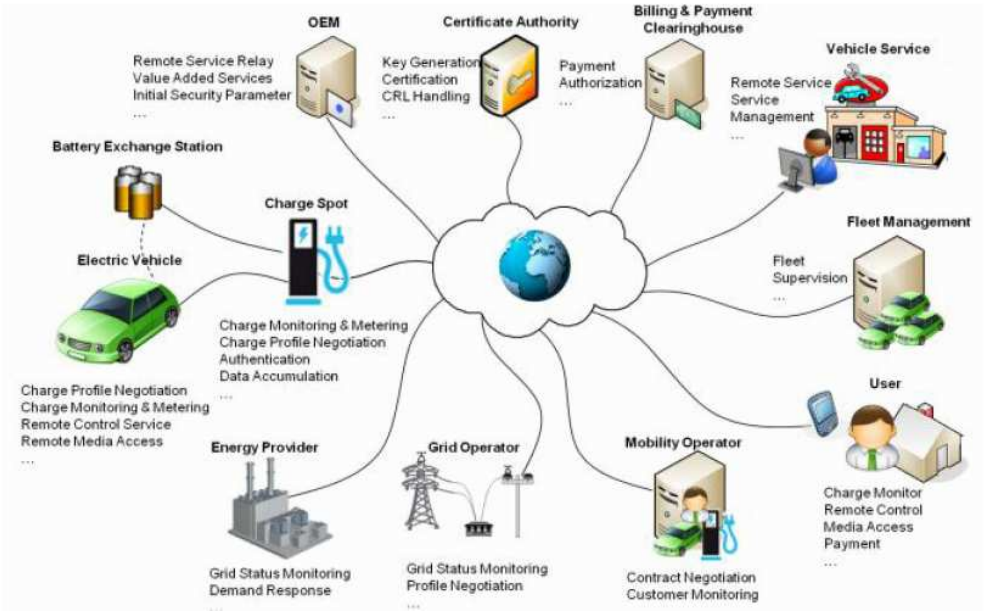


**Figure 36: Communication channels of a charging spot (source: [168])**

[169] introduces a privacy-preserving technique for vehicle charging based on group signatures [170]. Car manufacturers or energy providers – depending on the business model – must initially provide users with keys for group signatures. Such keys may be stored within the vehicle, in mobile devices (e.g. smartphones), or in access tokens (electronic vehicle key). For each service, the charging sport or the back-end can verify whether the vehicle or the user belongs to a given customer group entitled to use the service.

As soon as the user and the charging spot have provided a valid group signature, the service provider can put a charging or value-added service at disposal, needing to know neither the exact location of the charging spot nor the identity of the user. Only if the user acts in a way contrary to the contractual obligations or in otherwise duly justified cases, the service provider or government agencies may ask a trustful third party to re-identify the person by "opening" the signatures.

This solution based on group signatures has got various advantages: first, it protects data privacy by allowing users to charge their electric vehicles or use value-added services without revealing their identity towards the charging spot. Secondly, it excludes user profiles. Finally, the verification of different group signatures is much easier and more secure than a pseudonym-based solution which requires the regular and secure update of the database containing the confidential mapping of pseudonyms and users' clear names.

# 7. FINSENY Functional Architecture including Security

This section provides an example of mapping security functionalities to the Smart Grid Architecture Model developed by the European SG-CG. The actual mapping to the FINSENY functional architecture is being done in each Dx.3 deliverables of the WP 2-WP6 and not repeated here. Moreover, this document provides a catalog of security elements which are proposed to be used to address the security specific requirements specified by WPs.

## 7.1 Mapping of security elements to SGAM

### 7.1.1 SGAM overview

The Smart Grid Architecture Model (SGAM) developed by the European SG-CG consists of five layers representing business objectives and processes, use case functions, information models, communication protocols and components. Each layer is divided into domains and zones. The intention of this model is to allow the presentation of the current state of implementations in the electrical grid, but furthermore to present the evolution to future Smart Grid scenarios by supporting the principles of universality, localization, consistency, flexibility and interoperability. More information about SGAM and an introduction of each layer is provided in [84].

Typically the model is applied in the following way:

1. Identify functions based on selected scenario use cases;
2. Investigate in business needs in terms of related requirements, e.g., stemming from regulation;
3. Distribute functions and sub functions to appropriate locations in the Smart Grid Plane by identifying domains and zones affected by the scenario use case;
4. Identify components to be used for functions identified in 1;
5. Distribute components to appropriate locations based on the function distribution;
6. Further elaborate on Information and Communication layers;
7. Verify that all layers are consistent and there are no gaps; all entities are connected.

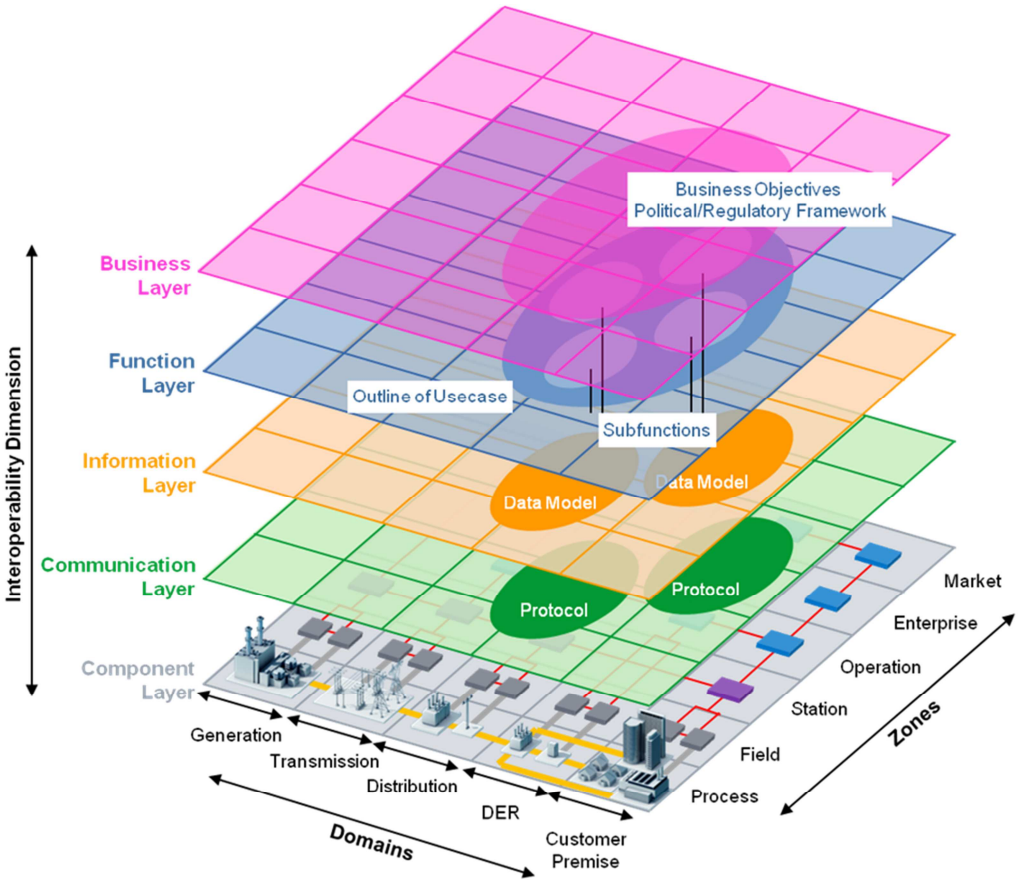


**Figure 37: Smart Grid architecture model [83]**

Security is one property, which is available in all layers, zones and domains. For the FINSENY scenario use cases, security is applied to the functional architectures defined in the use cases WPs. This document provides a catalog of security architecture elements which can be mapped to the component, communication and information layer.

Nevertheless, there are certain security specific use cases, for which the mapping can be provided as well. These security specific use cases comprise for instance the management of credentials used for authentication and access control. If for these credentials certificates and corresponding private keys are applied, the necessary components and functionalities can be depicted as part of the SGAM as well. This approach is being followed in the following subsection and provides an example based on role-based access control, defined in IEC 62351-8.

### 7.1.2 SGAM Application for Role-based Access Control

Role-based access control is often required for the operation of critical infrastructures. This is being requested by regulation and also by standards and guidelines addressing Smart Grid. In the following SGAM is used to identify the requirement for support of role-based access control based on business requirements as well as a mapping of a technical solution to the remaining SGAM layers.

- Business layer reflects requirements from regulation, standards, guidelines, and best practices. The stated documents relevant for Smart Grid uses cases require the application of RBAC during operation. Note that especially the regulations may be a country specific matter.

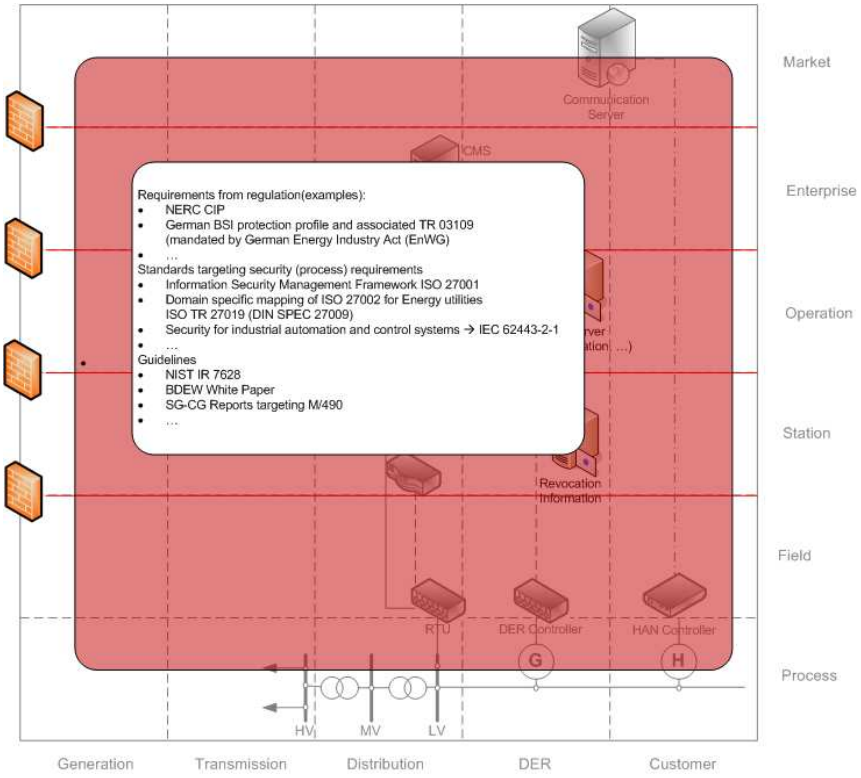


**Figure 38: RBAC on SGAM business layer**

Based on the requirements stemming from the business layer, the functional layer reflects the functional security requirements for role-based access control related to dedicated zones and domains. Through the mapping to different zones one can already distinguished between local and remote access.

- Function layer comprises access control to components but also command execution authentication and authorization control as functional requirements. Functional requirements are typically posed to an existing functional architecture during the design of an appropriate security architecture addressing discovered potential security risks.

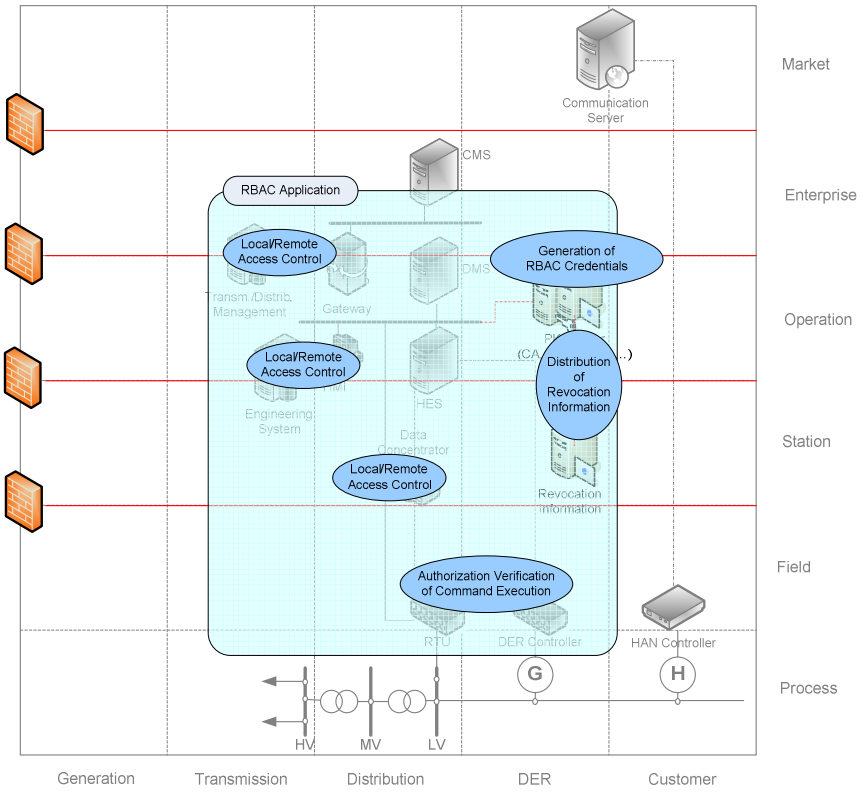


**Figure 39: RBAC on SGAM functional layer**

The following mappings to the remaining three layers of SGAM show the application of IEC 62351-8 in the context of power Smart Grid systems applying protocols like IEC 61850 or IEC 60870-5-104. It has been chosen here to provide an example of the application of SGAM in the context of identifying security requirements as well as mapping special solutions to these requirements.

IEC 62351-8 addresses the integration of role-based access control to ease the burden of access management in power systems. It enables the verification of authorization before command execution, e.g., in substation automation in terms of who has authorized and performed a dedicated switching command. This information can be required, e.g., for auditing purposes.

The roles are bound to different credentials as defined in IEC 62351-8. The standard distinguishes between:

- Public Key (Identity) certificate with included role information;
- attribute certificate bound to an identity certificate;
- software token (HMAC-protected structure, Kerberos like).

The standard IEC 62351-8 describes merely the token providing the role information as well as a set of mandatory roles (and associated rights):

- VIEWER;
- OPERATOR;
- ENGINEER;
- INSTALLER;
- SECADM;
- SECAUD;
- RBACMNT.

This list of roles and associated rights can be extended with own specific role and rights information. The predefined list above is intended for interoperability between different components. It is expected that all enhancements are installed on the involved entities, to keep the interoperability.

- Information layer requires RBAC credential specification and also requires mapping of entities to roles. As stated IEC 62351-8 provides predefined roles and associated rights. Nevertheless, these role definitions and rights associations can be enhanced according to the deployment needs.

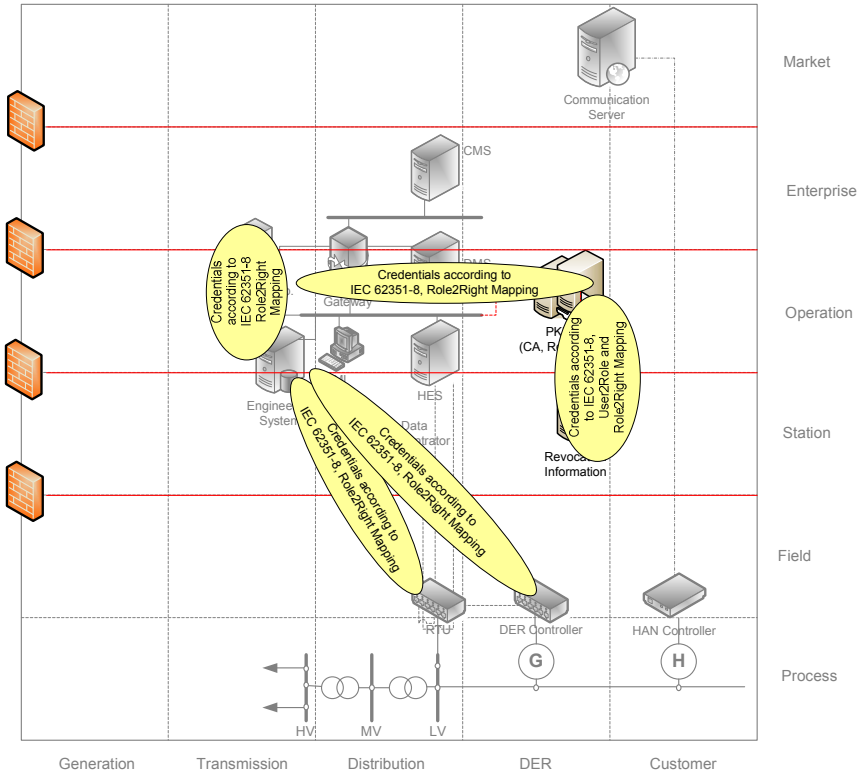


**Figure 40: RBAC influence on SGAM information layer**

- On Communication layer roles are transmitted bound to credentials within IEC protocols. IEC 62351-6 defines the structure of the RBAC token and also guidance how to transmit this token as part of utilized protocols. One example is the application of X.509 attribute certificates bound to X.509 Public Key certificates.

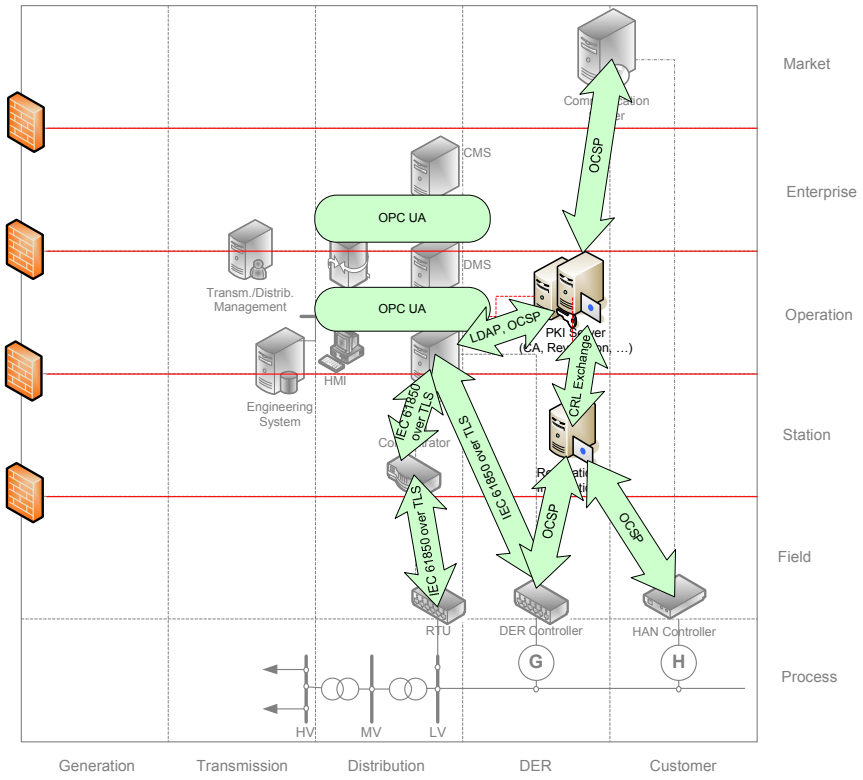


**Figure 41: RBAC influence on SGAM communication layer**

- Component layer comprises power systems like IED, RTU, etc. utilizing role information. Also required are additional components for credential handling like the generation or revocation of X.509 key material. This task is commonly performed by a PKI. The additional components needed here comprise a Certification Authority issuing the X.509 certificates including the role information and also a repository for querying the RBAC information. Also needed is a component for storing revocation information for the case a RBAC credential is being revoked before its validity period has ended.

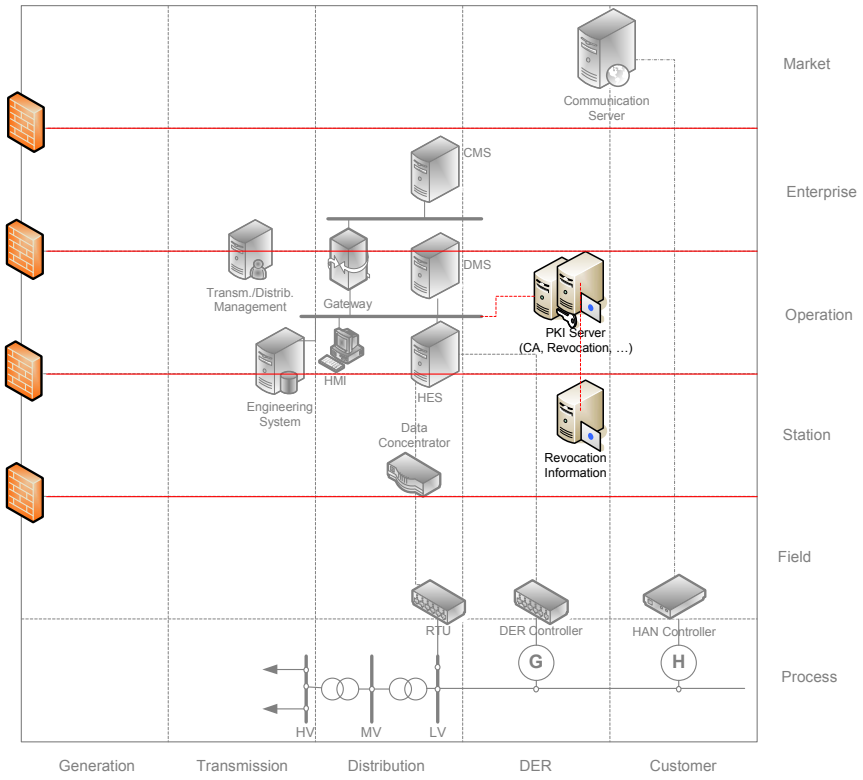


**Figure 42: RBAC influence on SGAM component layer**

As shown above, IEC 62351-8 can be used to provide for the requirements to support RBAC in Smart Grid Systems. Nevertheless, regarding IEC 62351-8 there are also gaps, which can be identified:

- for interoperability reasons a mandatory profile for RBAC support is necessary. The standard currently defines three different profiles, without requiring concrete support for at least one. This would be necessary to ensure interoperability and avoid a full implementation of this standard;
- transport profiles also for other protocols than TCP/IP (e.g., application for UDP/IP or even Ethernet based communication) may be outlined. The current standard only takes TLS as concrete example for application. Nevertheless, there are other standards utilizing X.509 certificates for authentication on transport but also on application layer. They may leverage the approach of enhancing either the X.509 public key certificate with the role information (as an extension) or by providing an attribute certificate containing the role information for a holder of a dedicated X.509 public key certificate.

# 8. Conclusion

This document is based on the results of the threat and risk analysis conducted by the WP1 security task and the interim security elements for the FINSENY architecture in D1.10 [181]. It aims at providing appropriate security counter measures for the scenario use case specific functional architectures.

D1.10 has mapped the identified threats to security controls without directly taking the functional use cases into account. Due to the fact that use case specific functional architectures where not advanced enough, at the time of investigating the individual use cases, this document maps the security controls to the thirteen security requirements identified and to the FI-WARE provided Generic Enablers. Nevertheless, the functional architectures defined in WP2-6 have been considered as much as possible.

A list of security counter measures and controls that can be used has thus been provided, along with an analysis on which security requirements are supported or met by which security controls. Some of the energy scenario specific security elements for FINSENY are also studied in more details. Finally, an example of how the functional architecture from FINSENY scenario work package 2 to 6 may be extended by the security elements.

The information retrieved and analyzed in this document is a valuable FINSENY output to support energy projects. In fact, it is being taken into account in eDASH project [173]. eDASH works on those ICT technologies and processes needed to achieve the real-time integration of "FEVs" in the European Electricity Grid. eDASH will become crucial to future electric road transport by providing the necessary intelligent charging system. ATOS is in charge of the design and development of an ICT tool for E-Mobility Brokering and shares with the eDASH consortium this document as a reference. eDASH benefits from the security functional architecture and considerations present in this document.

This document is also tightly linked with each Dx.3 deliverable (FINSENY scenario work packages functional architectures) where a dedicated security section is provided. This section describes use case specific security measures based on security counter measures and controls defined in this document, but while D1.11 analyses domain specific (Smart Grid) security architecture elements, the section 9 of each Dx.3 concentrates on scenario specific security elements.

# 9. References

## 9.1 General references


[1] NERC, North American Reliability Corporation, last access February 2011: http://www.nerc.com/page.php?cid=2|20

[2] BDEW – Bundesverband der Energie- und Wasserwirtschaft, Datensicherheit, last access January 2011: http://www.bdew.de/bdew.nsf/id/DE_Datensicherheit

[3] NIST, National Institute of Standards and Technologies, Smart Grid Interoperability Project, last access January 2011 http://www.nist.gov/Smart Grid/

[4] NIST Framework and Roadmap for Smart Grid Interoperability Standards, SP 1108, Version 2.0, last access January 2013, http://www.nist.gov/Smart Grid/upload/NIST_Framework_Release_2-0_corr.pdf
Stable Version 1.0, last access January 2012, http://www.nist.gov/Smart Grid/upload/FinalSGDoc2010019-corr010411-2.pdf

[5] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 1 Smart Grid Cyber Security Strategy, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[6] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 2 Security Architecture and Security Requirements, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

[7] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 3 Supportive Analyses and References, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

[8] NIST SP 800-30, Risk Management Guide for Information Technology Systems, July 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[9] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[10] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[11] NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, August 2009, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[12] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Draft, September 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

[13] RFC 4949: Internet Security Glossary, Version 2, R. Shirey, Aug. 2007.

[14] RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks, E. Rescorla, August 2008

[15] RFC 5878: Transport Layer Security (TLS) Authorization Extensions, M.Brown, R.Housley, May 2010

[16] ISO/IEC 15118-1: Road vehicles — Vehicle-to-Grid Communication Interface — Part 1: General information and use-case definition, Work in Progress

[17] ISO/IEC 15118-2: Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Technical protocol description and Open Systems Interconnections (OSI) layer requirements, Work in Progress

[18] ISO/IEC 15118-3: Road vehicles — Vehicle-to-Grid Communication Interface — Part 3: Physical layer and Data Link layer requirements, Work in Progress

[19] ISO-IEC 61850, Part 1: Introduction and Overview, May 2003

[20] ISO-IEC 61850, Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, May 2004

[21] ISO-IEC 61851-1: Electric vehicle conductive charging system – General requirements

[22] ISO-IEC 61851-21: Electric vehicle conductive charging system – Electric vehicle requirements for conductive connection to an A.C./D.C. supply

[23] ISO-IEC 61851-22: Electric vehicle conductive charging system – A.C. electric vehicle charging station

[24] ISO-IEC 61851-23: Electric vehicle conductive charging system – D.C. electric vehicle charging station

[25] ISO-IEC 61851-24: Electric vehicle conductive charging system – Control communication protocol between off-board D.C. charger and electric vehicle

[26] ISO-IEC IEC 61400, Part 25-4: Communications for monitoring and control of wind power plants – Mapping to communication profile, August 2008

[27] ISO-IEC 62351-4: Communication Network and System Security – Profiles Including MMS, October 2006

[28] ISO-IEC 62351-5: Security for IEC 60870 and Derivatives, February 2007

[29] ISO-IEC 62351-6: Security for IEC 61850, October 2006

[30] ISO-IEC 62351-7: Network and system management (NSM) data object models, October 2007

[31] ISO-IEC 62351- 8: Role-based Access Control, (TS) October 2011

[32] ISO-IEC 62351-10: Technical report on Security Architecture Guidelines for TC57 Systems, TR, October 2012

[33] GRAMMS, Uwe: SignIT. Slide Set, April 2008. – v1.0

[34] Performance of Optimized Implementations of the NESSIE Primitives, February 2003, https://www.cosic.esat.kuleuven.be/nessie/deliverables/D21-v2.pdf

[35] Hacking the lights out, Scientific American, July 2011, http://www.scientificamerican.com/article.cfm?id=hacking-the-lights-out

[36] EU Task Force Smart Grid, Expert Group 2: Regulatory recommendations for data safety data handling and data protection, http://ec.europa.eu/energy/gas_electricity/Smart Grids/doc/expert_group2.pdf

[37] M/490, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment, http://ec.europa.eu/energy/gas_electricity/Smart Grids/doc/2011_03_01_mandate_m490_en.pdf

[38] Guide to security log management, NIST SP800-92, September 2006, http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[39] ISO 27001, ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information Security Management System, http://www.iso27001security.com/html/27001.html

[40] ISO 27002, ISO/IEC 27002:2005 Information technology -- Security techniques – Code of practice for an Information Security Management System, http://www.iso27001security.com/html/27002.html

[41] ISO/IEC TR 27019 “Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002”, http://www.iso27001security.com/html/27019.html

[42] ISO-IEC 62351, Part 1-10, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62351&part=&se=

[43] Frances Cleveland: “IEC TC57 WG15: Security Standards for the Power System’s Information Infrastructure”, WG 15 White Paper, June 20072012, http://xanthus-consulting.com/Publications/documents/IEC%20_TC57_WG15_White_Paper.pdf

[44] IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, http://Smart Grid.ieee.org/standards/approved-ieee-Smart Grid-standards

[45] IEEE 802.1X: Port Based Network Access Control, http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

[46] IEEE 802.1AE: IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Security, http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf

[47] IEEE 802.1AR: IEEE Standard for Local and metropolitan area networks—Secure Device Identity, http://standards.ieee.org/getieee802/download/802.1AR.-2009.pdf

[48] XML Signature Syntax and Processing, Second Edition, 2008, http://www.w3.org/TR/xmldsig-core/

[49] XML Signature Syntax and Processing, Candidate Version 1.1, 2012, http://www.w3.org/TR/xmldsig-core1/

[50] XML Encryption and Processing, 2002, www.w3.org/TR/xmlenc-core/

[51] XML Encryption and Processing, Working Draft 0.5, 01/2012, http://www.w3.org/TR/xmlenc-core1/

[52] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT (last accesses on 13/02/2012)

[53] "Commission proposes a comprehensive reform of the data protection rules," 25/01/2012 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (last accessed on 13/02/2012)

[54] German Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), as of June 2010 http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile (last accessed on 13/02/2012)

[55] David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, The University of North Carolina Press; Chapel Hill, Reprint edition, 1992.

[56] Links to German state data protection acts http://www.datenschutz.de/recht/gesetze/ (German, last accessed on 13/02/2012)

[57] Energy Industry Act - Energiewirtschaftsgesetz (EnWG) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 2 des Gesetzes vom 16. Januar 2012 (BGBl. I S. 74) geändert worden ist http://bundesrecht.juris.de/enwg_2005/index.html (German, last accessed on 13/02/2012)

[58] Metering Access Ordinance - Messzugangsverordnung (MessZV) vom 17. Oktober 2008 (BGBl. I S. 2006), die durch Artikel 2 der Verordnung vom 3. September 2010 (BGBl. I S. 1261) geändert worden ist http://www.gesetze-im-internet.de/messzv/index.html (German, last accessed on 13/02/2012)

[59] Ordinance on Electricity Grid Access - Stromnetzzugangsverordnung (StromNZV) vom 25. Juli 2005 (BGBl. I S. 2243), die zuletzt durch Artikel 10 des Gesetzes vom 28. Juli 2011 (BGBl. I S. 1634) geändert worden ist http://www.gesetze-im-internet.de/stromnzv/index.html (German, last accessed on 13/02/2012)

[60] Ordinance on General Terms Regulating Universal Service for Household Customers and Replacement Supply via the Low Voltage Network – Stromgrundversorgungsverordnung vom 26. Oktober 2006 (BGBl. I S. 2391), die zuletzt durch Artikel 3 des Gesetzes vom 4. November 2010 (BGBl. I S. 1483) geändert worden ist (StromGVV) http://www.gesetze-im-internet.de/stromgvv/ (German, last accessed on 13/02/2012)

[61] Low Voltage Connection Ordinance - Niederspannungsanschlussverordnung vom 1. November 2006 (BGBl. I S. 2477), die zuletzt durch Artikel 4 der Verordnung vom 3. September 2010 (BGBl. I S. 1261) geändert worden ist (NAV) http://www.gesetze-im-internet.de/nav/index.html (German, last accessed on 13/02/2012)

[62] L. Zhu, B.Tung, RFC 4556, Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), June 2006

[63] Charles Raab and Benjamin Goold, Equality and Human Rights Commission Research report 69, "Protecting information privacy," 2011 http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf (last accessed on 15/02/2012)

[64] Human Rights Act 1998 http://www.legislation.gov.uk/ukpga/1998/42/contents (last accessed on 15/02/2012)

[65] Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29 (last accessed on 15/02/2012)

[66] Freedom of Information Act 2000 http://www.legislation.gov.uk/ukpga/2000/36/contents (last accessed on 16/02/2012)

[67] Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23 (last accessed on 16/02/2012)

[68] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14 http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf (last accessed on 15/02/2012)

[69] "The 'Durant' Case and its impact on the interpretation of the Data Protection Act 1998," Information Commissioner's Office http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf (last accessed on 16/02/2012)

[70] ebXML Technical Architecture Project Team, ebXML Technical Architecture Specification v1.0.4, February 16th 2001, http://www.ebxml.org/specs/ebTA.pdf (last access February 20th 2012)

[71] Web Services Reliable Messaging TC, WS-Reliability 1.1, OASIS Standard, 15 November 2004, http://docs.oasis-open.org/wsrm/ws-reliability/v1.1

[72] Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.2, OASIS Standard, 2 February 2009, http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.2-spec-os.pdf (last access February 20th 2012)

[73] Electricity Act 1989 http://www.legislation.gov.uk/ukpga/1989/29/contents

[74] Gas Act 1986 http://www.legislation.gov.uk/ukpga/1986/44/contents

[75] Energy Act 2011 http://www.legislation.gov.uk/ukpga/2011/16/contents

[76] "New UK Government re-emphasises commitment to smart meters/grids", 13.05.2010 http://www.law-now.com/law-now/2010/Smart Gridmay2010.htm?cmckreg=true

[77] „Smart Meter Implementation Programme – Response to Prospectus Consultation, Supporting Document 1 of 5 Data access and privacy", March 2011 http://www.decc.gov.uk/assets/decc/Consultations/smart-meter-imp-prospectus/1477-data-access-privacy.pdf

[78] Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) http://www.commoncriteriaportal.org/cc/

[79] Export Administration Regulations Database http://www.gpo.gov/bis/ear/ear_data.html (last accessed on 27/02/2012)

[80] Wassenaar arrangement on export controls for conventional arms and dual-use goods and technologies http://www.wassenaar.org/introduction/index.html (last accessed on 27/02/2012)

[81] Dual-use list category 5 – part 2 http://www.wassenaar.org/controllists/2009/WA-LIST%20%2809%29%201/08%20-%20WA-LIST%20%2809%29%201%20-%20Cat%205P2.doc (last accessed on 27/02/2012)

[82] EAR §740, supplement 3, „License Exception ENC Favorable Treatment Countries" http://ecfr.gpoaccess.gov/cgi/t/text/text-

idx?c=ecfr&sid=ba2d5996d28cc22033ea2bfb857555cc&rgn=div5&view=text&node=15:2.1.3.4.25&idno=15#15:2.1.3.4.25.0.1.21.30 (last accessed on 27/02/2012)

[83] Smart Grids Coordination Group Technical Report on Reference Architecture for the Smart Grid, Version 1.0, 2012-03-02

[84] Working Group Smart Grid Information Security - Report on SGIS requirement standards and SGIS toolbox, Version 0.7, 2012-12

[85] ISO-IEC 11770-1: Information technology — Security techniques — Key management Part 1: Framework, December 2009

[86] NIST SP 800-130: A Framework for Designing Cryptographic Key Management Systems, Draft, June 2010

[87] Himanshu Khurana, Rakeshbabu Bobba, Timothy M. Yardley, Pooja Agarwal, Erich Heine: Design Principles for power grid Cyber-Infrastructure Authentication Protocols. HICSS 2010, pp. 1-10

[88] Carl H. Hauser, Thanigainathan Manivannan, David E. Bakken: Evaluating Multicast Message Authentication Protocols for Use in Wide Area power grid Data Delivery Services. HICSS 2012, pp. 2151-2158

[89] Qinghua Li, Guohong Cao: Multicast Authentication in the Smart Grid With One-Time Signature. IEEE Transactions on Smart Grid, Vol. 2, No. 4, Dec. 2011

[90] Jianqing Zhang, Carl A. Gunter, C.A. (2011): Application-aware secure multicast for power grid communications. International Journal of Security and Networks (IJSN), Vol. 6, No. 1, 2011, pp. 40-52

[91] Xiang Lu, Wenye Wang and Jianfeng Ma: Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems. International Journal of Distributed Sensor Networks, April 2012 (article in press)

[92] Sean W. Smith, "Cryptographic scalability challenges in the Smart Grid (extended abstract)", ISGT, pp. 1-3, 2012 IEEE PES Innovative Smart Grid Technologies, 2012

[93] Depeng Li, Zeyar Aung, John R. Williams, Abel Sanchez, "Efficient authentication scheme for data aggregation in Smart Grid with fault tolerance and fault diagnosis", ISGT, pp.1-8, 2012 IEEE PES Innovative Smart Grid Technologies, 2012

[94] Shailendra Fuloria, Ross Anderson, Fernando Alvarez, Kevin McGrath, “Key Management for Substations: Symmetric Keys, Public Keys or No Keys?”, PSCE 2011: Presented at the IEEE Power Systems Conference & Exposition, March 2011, Phoenix, Arizona, USA, http://www.cl.cam.ac.uk/~sf392/publications/IEEE-PSCE.pdf

[95] Trusted Computing Group Website: http://www.trustedcomputinggroup.org, Development of TCG Standards: http://www.trustedcomputinggroup.org/trusted_computing/standards_development

[96] ISO/IEC 11889: Information technology -- Trusted Platform Module – Parts 1-4, 2009

[97] ISO/IEC 14443-1:2008, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 1: Physical characteristics

[98] ISO/IEC 14443-2:2010, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface

[99] ISO/IEC 14443-3:2011, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision

[100] ISO/IEC 14443-4:2008, Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol

[101] ISO/IEC 18092:2004, Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)

[102] ISO/IEC 21481:2012, Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)

[103] ISO/IEC 13157-1:2010, Information technology -- Telecommunications and information exchange between systems -- NFC Security -- Part 1: NFC-SEC NFCIP-1 security services and protocol

[104] ISO/IEC 13157-2:2010, Information technology -- Telecommunications and information exchange between systems -- NFC Security -- -- Part 2: NFC-SEC cryptography standard using ECDH and AES

[105] ISO/IEC 15693-1:2010, Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics

[106] ISO/IEC 15693-2:2006, Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization

[107] ISO/IEC 15693-3:2009, Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol

[108] ISO/IEC 7816: Identification cards -- Integrated circuit cards -- Parts 1 – 13 and 15

[109] Public-Key Cryptography Standards (PKCS), http://www.rsa.com/rsalabs/node.asp?id=2124

[110] Near Field Communication Forum, http://www.nfc-forum.org/home/, link to specifications: http://www.nfc-forum.org/specs/spec_dashboard/

[111] H. Busch, M. Sotakova, S. Katzenbeisser, R. Sion : The PUF Promise, in: 3rd International Conference on Trust and Trustworthy Computing (TRUST 2010), Springer, p. 290-297, Mai 2010.

[112] Stefan Katzenbeisser, Ünal Kocabas, Vladimir Rožic, Ahmad-Reza Sadeghi, Ingrid Verbauwhede and Christian Wachsmann: PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Poured in Silicon, in: Workshop on Cryptographic Hardware and Embedded Systems (CHES), Springer, Spetember 2012.

[113] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996, http://www.ietf.org/rfc/rfc1994.txt

[114] Zorn, G. and Cobb, S., "Microsoft PPP CHAP Extensions", RFC 2433, October 1998, http://www.ietf.org/rfc/rfc2433.txt

[115] Zorn, G., "Microsoft PPP CHAP Extensions, Version 2", RFC 2759, January 2000, http://www.ietf.org/rfc/rfc2759.txt

[116] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial in User Service (RADIUS)", RFC 2865, June 2000, http://www.ietf.org/rfc/rfc2865.txt

[117] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003, http://www.ietf.org/rfc/rfc3588.txt

[118] Aboba, B., Blunk, L., Vollbrecht, J., et al., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004, http://www.ietf.org/rfc/rfc3748.txt

[119] Perrig, A., Song, D., Canetti, R., Tygar, J., and B.Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", RFC 4082, June 2005, http://www.ietf.org/rfc/rfc4082.txt

[120] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", RFC 4226, December 2005, http://www.ietf.org/rfc/rfc4226.txt

[121] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005, http://www.ietf.org/rfc/rfc4301.txt

[122] Simon, D., Aboda, B., and Hurst, R., "The EAP-TLS Authentication Protocol", RFC 5216, March 2008, http://www.ietf.org/rfc/rfc5216.txt

[123] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt

[124] M'Raihi, D., Machani, S., Pei, M., and Rydell, J., " TOTP: Time-Based One-Time Password Algorithm", RFC 6238, May 2011, http://www.ietf.org/rfc/rfc6238.txt

[125] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012, http://www.ietf.org/rfc/rfc6347.txt

[126] ISO-IEC 62351-3: Communication Network and System Security – Profiles Including TCP/IP, June 2007

[127] Microsoft Security Advisory 2743314: Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure, Published: Monday, August 20, 2012, Version: 1.0, http://technet.microsoft.com/en-us/security/advisory/2743314

[128] Wang, Q., Khurana, H., Huang, Y., Nahrstedt, K., "Time Valid One-Time Signature for Time-Critical Multicast Data Authentication", University of Illinois at Urbana-Champaign, INFOCOM 2009, pp. 1233-1241

[129] P. Shanmugaraja, S. Chandrasker, Accessible Methods to Mitigate Security Attacks on IPv4 to IPv6 Transitions, European Journal of Scientific Research, ISSN 1450-216X Vol.77 No.2 (2012), pp.165-173

[130] S. Convery, D. Miller, IPv6 and IPv4Threat Comparison and Best-Practice Evaluation, http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

[131] RFC 3948: UDP Encapsulation of IPsec ESP Packets, A. Huttunen, B. Swander, V. Volpe, L. DiBurro, M. Stenberg, January 2005

[132] RFC 4303: IP Encapsulating Security Payload (ESP), S. Kent, December 2005

[133] RFC 4835: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), V. Manral, April 2007

[134] RFC 4864: Local Network Protection for IPv6, G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, May 2007

[135] RFC 4891: Using IPsec to Secure IPv6-in-IPv4 Tunnels, R. Graveman, M. Parthasarathy, P. Savola, H. Tschofenig, May 2007

[136] RFC 4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, T. Narten, R. Draves, S. Krishnan, September 2007

[137] RFC 6052: IPv6 Addressing of IPv4/IPv6 Translators, C. Bao, C. Huitem, M. Bagnulo, M. Boucadair, October 2010

[138] RFC 6092: Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service, J. Woodyatt, Ed., January 2011

[139] RFC 6144: Framework for IPv4/IPv6 Translation, F. Baker, X. Li, C. Bao, K. Yin, April 2011

[140] RFC 6145: Tunnels, IP/ICMP Translation Algorithm, X. Li, C. Bao, F. Baker, April 2011

[141] RFC 6146: Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, P. Matthews, I. van Beijnum, April 2011

[142] RFC 6147: DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, A. Sullivan, P. Matthews, van Beijnum, April 2011

[143] RFC 6169: Security Concerns with IP Tunneling, S. Krishnan, D. Thaler, J. Hoagland, April 2011

[144] "Smart Grid Privacy 101: Privacy by Design in Action — Power Morning", Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, Jerusalem, October 25, 2010 http://www.privacybydesign.ca/content/uploads/2010/10/2010-10-25-PbD-Jerusalem.pdfhttp://www.privacybydesign.ca/content/uploads/2010/10/2010-10-25-PbD-Jerusalem.pdf

[145] SGTF EG2, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, 07-JAN-2013

[146] OCTAVE website http://www.cert.org/octave/

[147] Information System Security Review methodology, A guide for reviewing information system security in government organization, INTOSAI, 1995

[148] Securing Networks Systematically – The SKiP method, CERT coordination center www.cert.org/archive/pdf/SKiP.pdf

[149] RFC 6272: Internet Protocols for the Smart Grid, F. Baker, D. Meyer, June 2011 http://tools.ietf.org/html/rfc6272

[150] RFC 4861: Neighbor Discovery for IP version 6 (IPv6), T. Narten, E. Nordmark,W. Simpson, H. Soliman, September 2007 http://tools.ietf.org/html/rfc4861

[151] RFC 3971: Secure Neighbor Discovery (SEND), J. Arkko, J. Kempf, B. Zill, P. Nikander, March 2005 http://tools.ietf.org/html/rfc3971

[152] A. Alsa'deh, C. Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations", IEEE Security & Privacy, pp. 26 – 34, August 2012

[153] Internet Draft: Constrained Application Protocol (CoAP), Z. Shelby, K. Hartke, C. Bormann, B. Frank, 2012 http://tools.ietf.org/html/draft-ietf-core-coap-13

[154] Internet Draft: CoAP Security Architecture, J. Arkko, A. Keranen, 2011 http://tools.ietf.org/html/draft-arkko-core-security-arch-00

[155] M. Brachmann, O. Garcia-Morchon, M. Kirsche, "Security for practical CoAP applications: Issues and Solution Approaches", Proceedings of the 10th GI/ITG KuVS Fachgespraech Sensornetze, 2011

[156] RFC 6762: Multicast DNS, S. Cheshire, M. Krochmal, 2013 http://tools.ietf.org/html/rfc6762

[157] RFC6763: DNS-Based Service Discovery, S. Cheshire, M. Krochmal, 2013 http://tools.ietf.org/html/rfc6763

[158] RFC 4033: DNS Security Introduction and Requirements, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, 2005 http://tools.ietf.org/html/rfc4033

[159] Michael John kristan, "Securing multicast DNS – Study into the feasibility of trusted multicast DNS for service discovery", MITRE technical report, 2009

[160] RFC 3224: Service Location Protocol, version 2, E. Guttman, C. Perkins, J. Veizades, M. Day, 1999 http://tools.ietf.org/html/rfc3224

[161] M. Vettorello, C. Bettstetter, C. Schwingenschlögl, „Some notes on security in the service location protocol version 2 (SLPv2)"

[162] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin: Private memoirs of a smart meter. In: 2nd ACM Workshop on Embedded Sensing Systems for Energy- Efficiency in Buildings (BuildSys 2010), Zurich, Switzerland (November 2010)

[163] Flavio D. Garcia and Bart Jacobs. Privacy-friendly energy-metering via homomorphic encryption. Technical report, Radboud Universiteit Nijmegen, February 2010.

[164] Klaus Kursawe, George Danezis, and Markulf Kohlweiss, "Privacy-Friendly Aggregation for the Smart-Grid", in: Privacy Enhancing Technologies, 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27-29, 2011 Proceedings, S. Fischer-Hübner and N. Hopper (Eds.), Lecture Notes in Computer Science 6794, 2011, Springer Verlag, pp.175-191

[165] Alfredo Ria and,George Danezis: Privacy-preserving smart metering. Technical Report MSRTR-2010-150, Microsoft Research (November 2010)

[166] Marek Jawurek, Martin Johns, and Florian Kerschbaum, "Plug-In Privacy for Smart Metering Billing" in: Privacy Enhancing Technologies, 11th International Symposium, PETS 2011, Waterloo, ON, Canada, July 27-29, 2011 Proceedings, S. Fischer-Hübner and N. Hopper (Eds.), Lecture Notes in Computer Science 6794, 2011, Springer Verlag, pp. 192-210

[167] A. Cavoukian, J. Polonetsky, and C.Wolf, "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation", 17 Nov 2009. http://www.ipc.on.ca/images/Resources/pbd-smartpriv-Smart Grid.pdf

[168] Fries Steffen, Rainer Falk: „Electric Vehicle Charging Infrastructure – Security Considerations and Approaches", Siemens AG, IARIA, 2012. ISBN: 978-1-61208-204-2

[169] Santiago Suppan, Dr. Jens-Uwe Bußer, Dr. Fabienne Waidelich, " Verfahren, Vorrichtung und Dienstleistungsmittel zur Authentifizierung eines Kunden für eine durch ein Dienstleistungsmittel zu erbringende Dienstleistung," patent application: DE 102012221288.4

[170] Prof. Dr. Mark Manulis, Nils Fleischhacker, Felix Günther, Franziskus Kiefer, Bertram Poettering: "Group Signatures: Authentication with Privacy", Technische Universität Darmstadt /

Bundesamt für Sicherheit in der Informationstechnik, 2012 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/GruPA/GruPA.pdf;jsessionid=815480B8B17D500CAD2F74C2BF87221C.2_cid294?__blob=publicationFile

[171] RFC 6749 "The OAuth 2.0 Authorization Framework", http://tools.ietf.org/html/rfc6749

[172] SAML: Security Assertion Markup Language, Entry for further information: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[173] eDASH project: http://www.edash.eu

## 9.2 FINSENY related references

[174] D5.1 Electric Mobility Scenario building blocks, http://www.fi-ppp-finseny.eu/deliverables/

[175] D6.1 Electronic Market Place for Energy Building Blocks, http://www.fi-ppp-finseny.eu/deliverables/

[176] T6.2 – IR6.1: ICT requirements of WP6, Excel-Sheet V1.0 (23.09.2011, 18:01), IR6.1_WP6-ICT-Requirements_v1.0.xls

[177] D7.1 – First set of consolidated ICT Requirements to the Architecture Board, Version 1.0, October, 15, 2011, D7.1_First set of consolidates ICT requirements to AB_v1.0.doc

[178] T6.3 – Functional Architecture, PowerPoint presentation, version 0.8, February 14, 2012, T6.3-Functional Architecture_v0.8.pptx

[179] WP6 scenarios Transparency in the Green Market + Colored Ethical Bid + Trading for the Good of All, PowerPoint presentation, Version 0.2, February 16, 2012, TI PPT about scenarios drill down according SGAM.pptx

[180] D6.3 – Electronic Marketplace for Energy Functional Architecture, http://www.fi-ppp-finseny.eu/deliverables/

[181] D1.10 – Interim Security Elements for the FINSENY Functional architecture, http://www.fi-ppp-finseny.eu/deliverables/

[182] D5.3 – Electric mobility functional ICT Architecture Description, http://www.fi-ppp-finseny.eu/deliverables/

[183] D4.3 – Smart Building Functional Architecture, http://www.fi-ppp-finseny.eu/deliverables/

[184] D2.3 – Distribution Network Functional Architecture Description, http://www.fi-ppp-finseny.eu/deliverables/

[185] D3.3 – Microgrid Functional Architecture Description, http://www.fi-ppp-finseny.eu/deliverables/

[186] D2.1 – Distribution Network Building Blocks, http://www.fi-ppp-finseny.eu/deliverables/

[187] D3.1 – Microgrid Scenario Building Blocks, http://www.fi-ppp-finseny.eu/deliverables/

[188] D4.1 – Smart Buildings "scenario" definition, http://www.fi-ppp-finseny.eu/deliverables/

## 9.3 FI-WARE related references

[189] FI-WARE Security, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Security

[190] List of FI-WARE open specifications from Security Chapter http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Summary_of_FI-WARE_Open_Specifications#Security_Chapter

[191] FI-WARE Security Chapter, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Summary_of_FI-WARE_Open_Specifications#Security_Chapter

[192] Identity Management Generic Enabler API Specification, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Identity_Management_Generic_Enabler_API_Specification#Introduction_to_the_Identity_Management_GE_API

[193] Network Identity Management, http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Network_Identity_Management