DOMINOES – DELIVERABLE

D1.2 ICT platform and connected energy network reference architecture design

This project has received funding from the European Union's Horizon 2020 research and innovation programme under **Grant Agreement No. 771066.**

Deliverable number:	D1.2
Due date:	31.08.2018
Nature[1]:	O
Dissemination Level1:	PU
Work Package:	WP1
Lead Beneficiary:	VPS
Contributing Beneficiaries:	Empower, ISEP, LUT, UoL, EDPD
Reviewer(s):	CNET

[1] **Nature:** R = Report, P = Prototype, D = Demonstrator, O = Other
Dissemination level PU = Public
PP = Restricted to other programme participants (including the Commission Services)
RE = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)
Restraint UE = Classified with the classification level "Restraint UE" according to Commission Decision 2001/844 and amendments
Confidential UE = Classified with the mention of the classification level "Confidential UE" according to Commission Decision 2001/844 and amendments
Secret UE = Classified with the mention of the classification level "Secret UE" according to Commission Decision 2001/844 and amendments

Version	Date	Description
0.1	09/04/2018	Initial outlines by VPS
0.2	15/05/2018	Added section 3 by UoL
0.3	31/05/2018	Section 2.1.2.1 and 2.1.2.2 by Empower and added SGAM Approach and reference architecture
0.4	28/06/2018	On GA we identified the need to change the DOMINOES Platform area in SGAM Approach.
0.5	23/06/2018	Add changes after workshop meeting
0.6	30/07/2018	Add results of review from review from LUT, EMPOWER, EDPD and UoL
1.0	09/08/2018	First release for internal review
1.1	24/08/2018	Review of executive summary and new Data handling section
1.2	29/08/2018	Final release

Authors: Ana Guimarães, VPS
Jorge Landeck, VPS
Huiyu Zhou, UoL
Olli Kilkki, Empower
Salla Annala, LUT
Samuli Honkapuro, LUT
Célia Trocato, EDPD
Francisco Melo, EDPD
Nuno Medeiros, EDPD
Pedro Manuel Nunes, EDPD

Executive Summary

This deliverable describes the Reference Architecture of DOMINOES platform from the ICT connected energy network technology perspective. It includes the definition of the main platform components and how they communicate to meet interoperability, reliability and data protection requirements. The deliverable is strongly connected to the local market reference architecture and business requirements, considering namely the identified stakeholders and roles, regulations and rules, and the main interactions between market players and other markets.

The design of the Reference Architecture is guided by the SGAM framework, defined by the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG), which is particularly helpful in the delimitation of the platform scope (functionality and relationships) in the overall context of the Smart Grid.

A logical block diagram, comprising the static approach of the system, presenting all the architectural system elements that provide the different functionalities for the final users, complements the design. This diagram (Figure 1) decomposes the system into smaller manageable components with well-defined responsibilities (in terms of data handling) and interfaces (in terms of data exchange) described in detail.

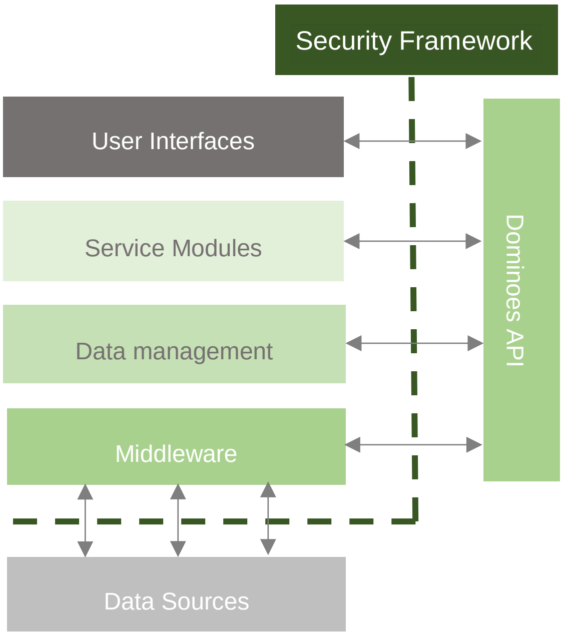

Figure 1 - Diagram of architectural system elements

In general terms, the proposed architecture for the DOMINOES platform is firstly subdivided in three distinct layers. At the bottom, the Data Source layer comprises the external operational platforms and data systems that will be used as providers of information and also as interfaces with the physical world. In the middle, the Modular Service Platform comprises the core data processing components of the system and

data storage. At the top, the User Interface layer comprises the web and mobile applications used by the end users.
The Modular Service Platform is also divided in three layers of identical functionality in which a module (service or component) is one layer can communicate with other modules in the same layer, provides services to the upper layer, and uses services of the lower layer. The communication between modules should use the common API although some specific external (micro) services may be invoked.

The comprehensiveness of proposed components is thoroughly demonstrated by mapping the reference architecture components to each use case scenario.

To conclude, secure data handling requirements are reviewed and considered. In particular privacy and data protection are described before discussing their importance and impacts on the community in the context of the Smart Metering.

In short, the document identify the main ICT network components, including an architecture diagram with its connections and also the requirements to meet interoperability and reliability, as well as the definition of secure data handling requirements.

List of Acronyms

API - Application Programming Interface

BEMS - Building Energy Management System

BRP – Balance Responsible Party

CIS – Customer Information System

CIM - Common Information Model

CSP - Concentrating Solar Power

DER - Distributed Energy Resources

DMS - Distribution Management System

DPA - Data Protection Authorities

DR - Demand Response

DRMS - Demand Response Management System

DSO - Distribution System Operator

ECSP – Energy Community Service Provider

EDPB - European Data Protection Board

EMS – Energy Management System

ESMS – Energy Storage Management System

GDPR - General Data Protection Regulation

ICT - Information and Communication Technology

M2M - Machine to Machine

MDMS – Meter Data Management System

NRA - National Regulatory Authorities

OMIE - Operador Mercado Ibérico de Energia

SCADA - Supervisory Control and Data Acquisition

SG-CG - Smart Grid - Group Coordination

SGAM - Smart Grid Architecture Model

TSO - Transmission System Operator

Introduction

1.1 Purpose and scope of the deliverable

This deliverable aims to provide a description of the overall architecture of the DOMINOES framework. The main goal is to define the architectural layers of the DOMINOES project to provide all the information related to the components of the architecture and identify all possible relationships between them. Additionally, to provide recommended structures and integrations of the DOMINOES solution as well as to facilitate the collaboration and communication between partners, when the concern is the implementation of the DOMINOES solution. The outcome of D1.2 will be the reference to start the implementation and integration regarding development tasks that will be performed in WP2.

1.2 Structure of the deliverable

Section 2 presents a short introduction to SGAM framework and then uses it to develop the DOMINOES reference architecture, particularly in terms of scope and interaction in the smart grid environment. As a complement, a logic block diagram of the architecture is also presented. The modules of services of each layer are described and an API is proposed as a common communication link.

Section 3 maps the uses cases to the components of the architecture to show that there is a thorough coverage. For the user interfaces, the key stakeholders are also associated with the proposed modules.

Section 4 refers to the security data handling requirements on the DOMINOES Platform. Regarding all the external data sources that will be integrated with this solution and all type of accesses, security is an important concern: the strategy description, the key pieces of information that make it possible to establish the priorities, a structure and how the software’s training should be done in a way to guarantee the platform security.

Section 5 provides a set of conclusions about the architecture and its future implementations.

1.3 Relation to other tasks and deliverables

The deliverable *D1.1 Local market reference architecture and business requirements* [DOM18] was an important source of information about energy markets for the identification of all modules and functionalities in the Architecture Reference platform.

The outcome of this work will also be the basis for the design and development of the DOMINOES platform such as *D1.3 - Use cases and application scenarios requirements*, D2.2 and D2.3 *Scalable local energy market architecture*, D2.4 *Information exchange processes and solutions between local and centralized energy markets*, D2.5 *Tools for local energy market and end-user interaction* and D2.6 *Design and implementation of a data security framework*.

2 DOMINOES Reference Architecture

To deal with the Smart Grid complexity and diversity several frameworks have been developed. The design of the reference architecture is guided by the SGAM framework, defined by the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) [CEN11], because it was has already been used in D1.1 [DOM18] to identify the roles and responsibilities of the stakeholders. The framework is particularly helpful in the delimitation of the scope (functionality and relationships) of the DOMINOES platform in the overall context of the Smart Grid.

2.1 Introducing SGAM Framework

SGAM describes three different levels/dimensions of abstraction within a Smart Grid: SGAM Domains, Zones and Interoperability layers.

The framework identifies a set of principles to help the mapping of systems onto the model based on the following topics:

- The definition of the “Generic use cases” which the system can/may support;
- The drawing of the typical architecture and components used by the system (component layer);
- A list of standards to be considered for interfacing each component within this system as shown in [SG-CG/G].” [CEN12]

Figure 2 illustrates a general system mapping.

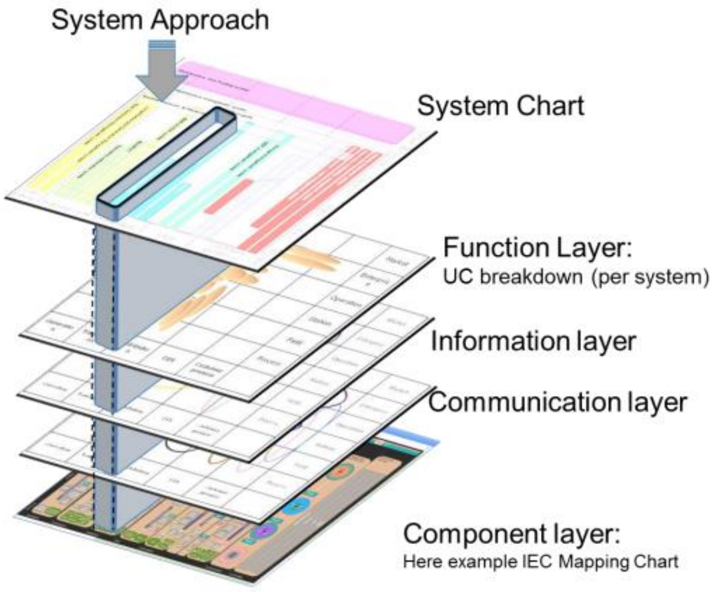

Figure 2 - Mapping principles of systems over the SGAM planes

The **Domains** focus on the “physical” path that energy travels from its production to its consumption:

- **Generation** – Representing generation of electrical energy in bulk quantities typically connected to the transmission system, such as by fossil, nuclear and hydro power plants, off-shore wind farms, large scale solar power plant (i.e. PV, CSP).
- **Transmission** – Representing the infrastructure which transports electricity over long distances.
- **Distribution** – Representing the infrastructure which distributes electricity to customers.
- **DER** – Representing distributed electrical resources directly connected to the public distribution grid, applying small-scale power generation and consumption technologies (typically in the range of 3 kW to 10,000 kW). These distributed electrical resources may be directly controlled by e.g. a TSO, DSO, an aggregator or Balance Responsible Party (BRP).
- **Customer Premises** – Hosting both end users of electricity and local producers of electricity. The premises include industrial, commercial and home facilities (e.g. chemical plants, airports, harbours, shopping centres, homes). Also generation in form of e.g. photovoltaic generation, electric vehicles storage, batteries, micro turbines.

The **Zones** focus on the “physical” location of the information:

- **Process** – Including the physical, chemical or spatial transformations of energy (electricity, solar, heat, water, wind) and the physical equipment directly involved e.g. generators, transformers, circuit breakers, overhead lines, cables, any kind, of sensors and actuators which are part or directly connected to the process.
- **Field** – Including equipment to protect, control and monitor the process of the power system, e.g. protection relays, bay controller, any kind of intelligent electronic devices which acquire and use process data from the power system.
- **Station** – Representing the areal aggregation level for field level, e.g. for data concentration, functional aggregation, substation automation, local SCADA systems, plant supervision.
- **Operation** – Hosting power system control operation in the respective domain, e.g. DMS, EMS in generation and transmission systems, micro-grid management systems, virtual power plant management systems, electric vehicle fleet charging management systems.
- **Enterprise** – Including commercial and organizational processes, services and infrastructures for enterprises (utilities, service providers, energy traders …), e.g. asset management, logistics, work force management, staff training, customer relation management, billing and procurement.
- **Market –** Reflecting the market operations possible along the energy conversion chain, e.g. energy trading, retail market.

The interoparibility layer comprises:

- The **Business layer** represents the business view of the smart grid model. This layer can be used to map different stakeholders within the zones and domains. In addition, their roles and responsibilities can be categorized and mapped.
- The **Function Layer** includes services and function derived from the business view, independent from involved actors.
- The **Information Layer** is focused on the description of the information exchanged between systems and actors.
- The **Communication Layer** describes the protocols and mechanism for the interchange of data between components.
- The **Component Layer** pays attention to the components in the Smart Grid context, including system actors, components, applications, power system equipment, smart meters, etc.

For the lower layer of the model (component layer), SGAM offers a tool that can be used to select the proper standards to connect components and devices as shown on the Figure 3. This tool enables the selection of groups that are composed by components, devices, protocols, standards, and use cases.

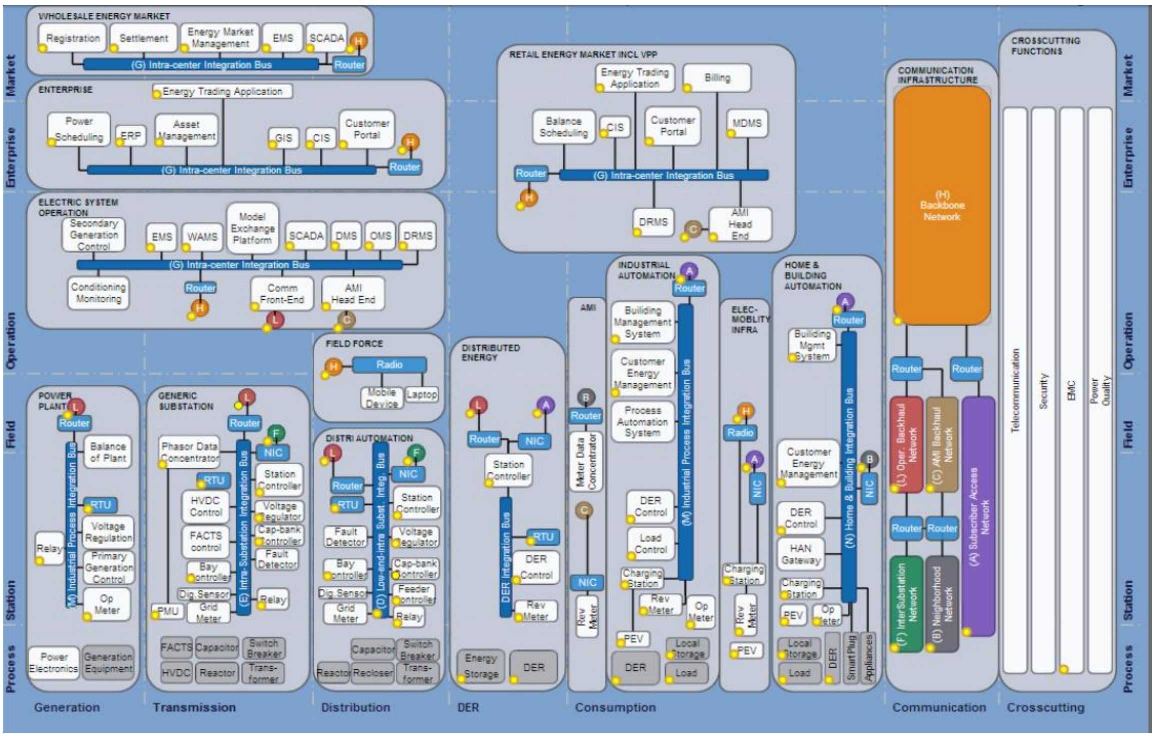

Figure 3 - IEC Smart Grid mapping tool

2.2 Applying SGAM Framework

Considering the roles and responsibilities identified in D1.1 and the requirements described in D1.3, the DOMINOES platform matches three Zones (Operation, Enterprise, and Market) and three Domains (Distribution, only partially, DER, and Customer Premises) that are highlighted in Figure 4.

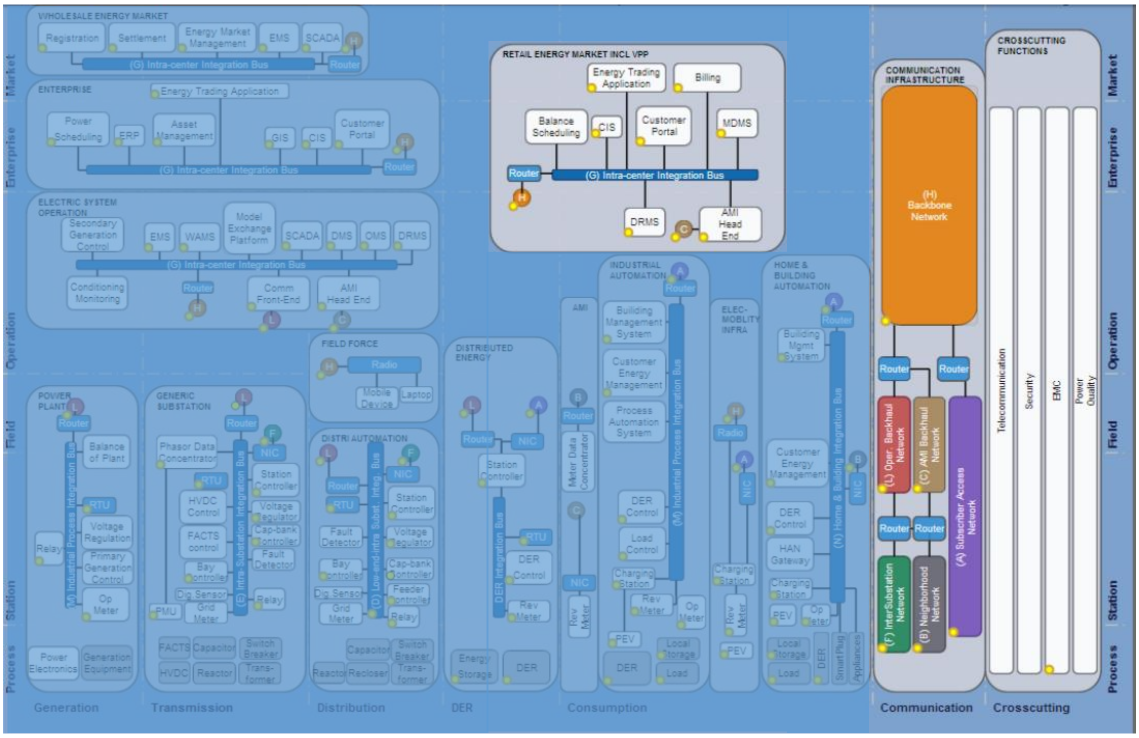

Figure 4 - DOMINOES platform roles and requirements over SGAM framework

This mapping can be used to identify the standards that can be used on the development of the platform and, mainly, to visualize the relationship between the platform and the various other systems already in place.

Following the SGAM approach the next step - system breakdown – of mapping the DOMINOES platform consists in the definition of the System Chart and all the included layers (Function, Information, Communication and Component).

At this stage, it is possible to categorise two main classes of components: the data sources and the platform itself. The first class refers to all the project data providers and the second one mentions all the functionalities that will be available in the DOMINOES platform.

The mapping between these two groups and the SGAM matrix comprising zones and domains is depicted on Figure 5 below.

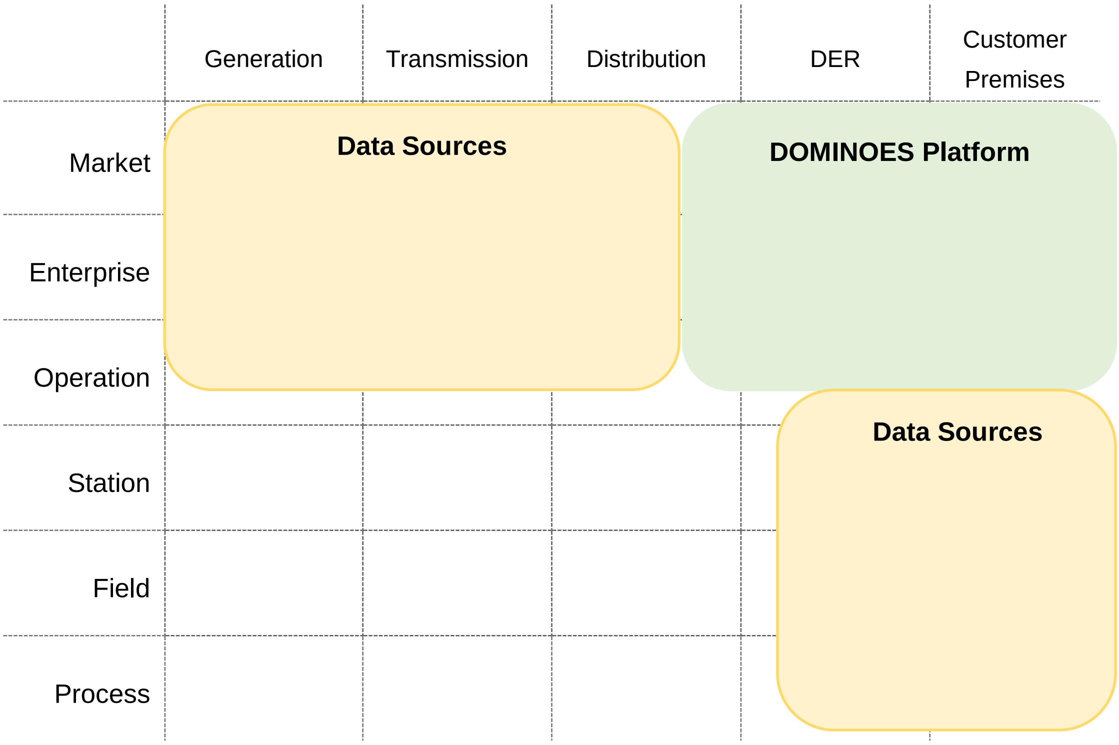

Figure 5 - DOMINOES SGAM System Chart

Continuing with the SGAM approach, the next step consists in defining the Function layer. This layer reflects the functional security requirements for role-based access control related to dedicated zones and domains. From the mapping one can immediately distinguish between local and remote access. The function layer comprises access control to components but also command execution authentication and authorization control as functional requirements. [CEN12]

The main function blocks of the DOMINOES platform are represented in Figure 6 below.

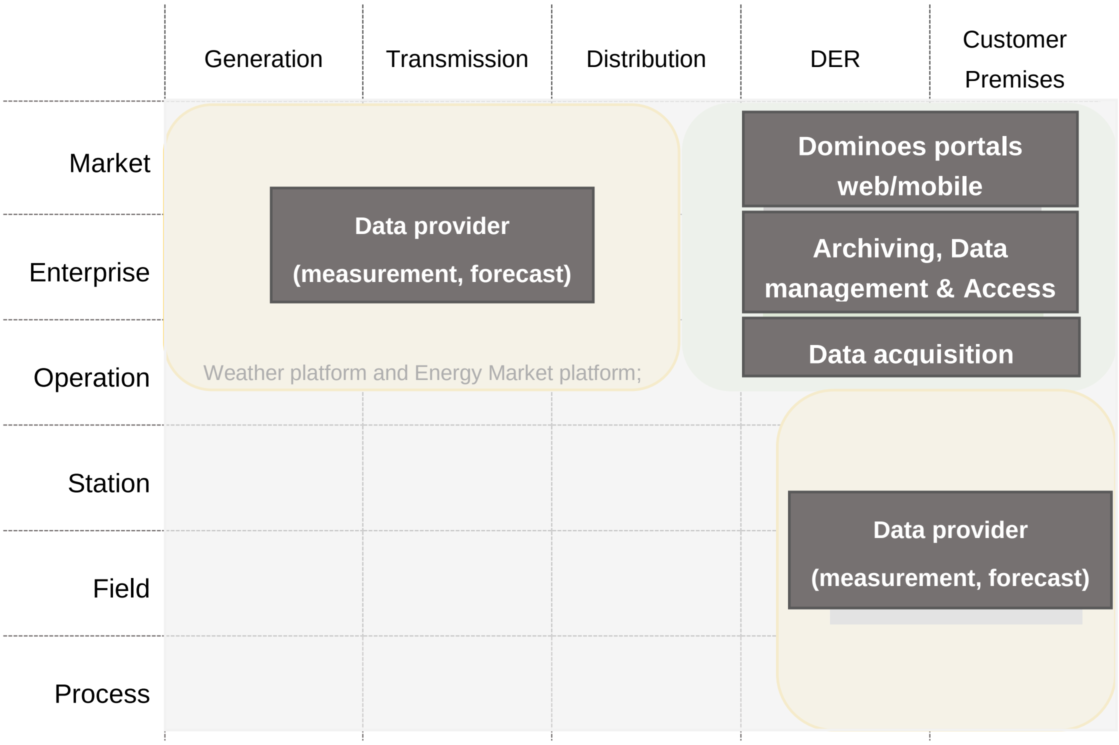
Generation
Transmission
Distribution
DER
Customer Premises
Market
Enterprise
Operation
Station
Field
Process
Data provider (measurement, forecast)
Weather platform and Energy Market platform;
Dominoes portals web/mobile
Archiving, Data management & Access
Data acquisition
Data provider (measurement, forecast)

Figure 6 - DOMINOES SGAM Function Layer

Data providers refer to all data sources that will be integrated in the DOMINOES platform. This data is composed of different types of information, including energy consumptions and productions, weather measurements and forecasts, energy prices and price forecasts, control commands and status signals.

These data providers can be grouped in accordance with the respective zone and domains. For example, weather data and energy market prices correspond to data providers on Generation, Transmission, and Distribution Domain, and on Operation, Enterprise, and Market Zone.

Other data providers that are localized in the SGAM matrix in the DER and Customer Premises Domain, and in the Process, Field, Station and Operation Zones refer to different system that can be integrated with the DOMINOES platform such as EMS/BEMS, ESMS, PVMS and WTMS as well as other operational platforms.

The **Data acquisition** refers to a middleware that is responsible for data gathering while guaranteeing an abstraction layer using open standard interfaces, needed for interoperability.

The modules represented by **Archiving, Data management, and Access control** are responsible for storing data, providing data processing and aggregation functionalities to all platform services and managing authorization and access.

Finally, the **DOMINOES portals** refer to all the frontend and backend portals that will provide access to data and information for all the stakeholders.

Following the SGAM framework, namely the System Approach, the next step involves the definition of the **Information layer** that describes the information being used and exchanged between functions, services and components. This layer contains information objects and the underlying canonical data models that represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means. [CEN12]

To describe this layer in some detail, it is assumed that the DOMINOES platform is composed of two main layers of components (User Interfaces and a Modular Service Platform) on top of the Data Sources layer as represented in Figure 7.

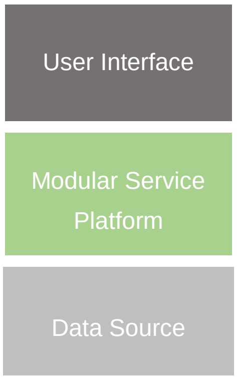

Figure 7 - DOMINOES Reference Architecture Layers

The **User Interface** layer refers to all the user interfaces that is web and mobile applications that interact with the users. These applications will exploit the services and data provided by the lower layers.

The **Modular Service Platform** is responsible for data gathering, storing, and processing, and for providing a uniform information access method to all the interfaces. This platform is also responsible for the implementation of the necessary business and control flows.

The **Data Source** layer is responsible for interfacing the external data providers with the DOMINOES platform. These data providers include weather, market, and operational platforms. Depending on implementation restrictions these data sources might provide real-time data and control.

Figure 8 represents the information exchanges between the main architecture layers identified, highlighting a suited access control mechanism from standards recommended by the framework. In fact, the technical scope of the IEC 62351-8 comprises the access control of users and automated agents to data object in power systems by means of role-based access control. [IEC51]

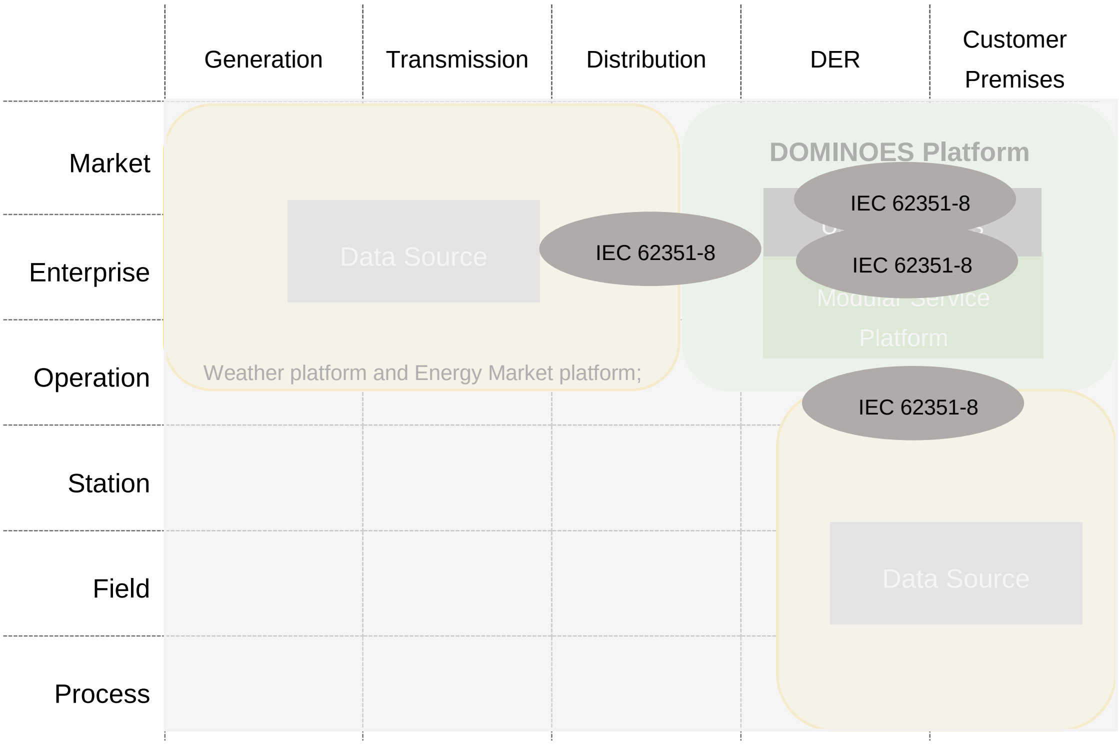

Figure 8 - DOMINOES SGAM Information Layer

Other equivalent access control mechanisms might be used depending on particular implementations. Yet the main functional characteristics should be preserved. A more in-depth analysis of the security and privacy issues can be found on chapter 4.

The next step of the SGAM approach is the definition of the **Communication Layer** that contains a description of protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models. [CEN12]

At this initial stage, several standard and widely used communication protocols were identified as valid alternatives for the implementation of this layer as represented in Figure 9. In particular, suitable protocols were identified for each main data exchange between components. During implementation some of these protocols might be replaced by similar or “equivalent” ones when other constraints are taken into account.

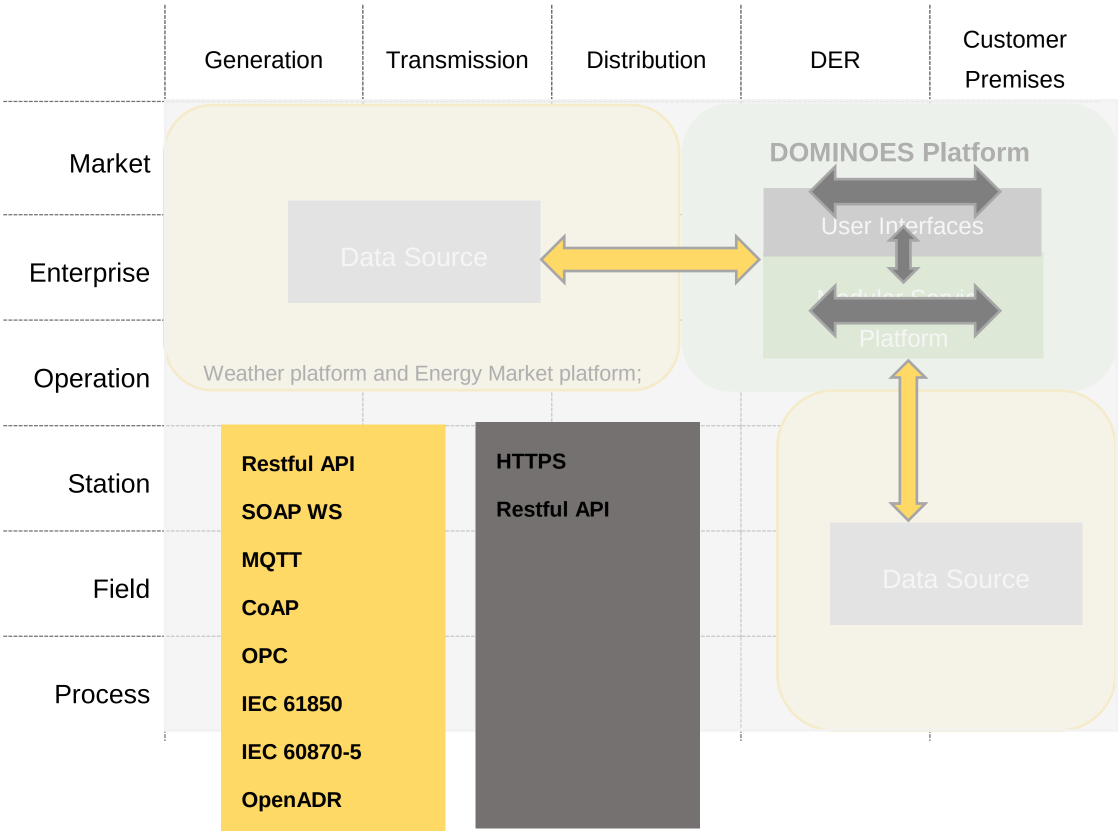

Figure 9 - DOMINOES SGAM Communication Layer

The user interface web applications will be accessed using an HTTPS encrypted link to guarantee privacy and integrity of the exchange data what is currently seen as a good practice.

In general terms, a similar link will be used to connect the user interface applications and the Modular Service Platform layer though a RESTful API when a simpler HTTP link is considered not secure enough.

Recent good practices recommend the implementation of REST APIs due to its simplicity and ability to provide a communication mechanism between applications developed for different operating systems and platforms, with a minimal overhead for the client side. The use of JSON (JavaScript Object Notation) to codify the structures of the parameters exchanged through the API is also recommended due to being lightweight and equally easy to use by humans and machines.

IEC 61968-100 defines a similar approach that specifies an implementation profile for the application of the other parts of IEC 61968 using common integration technologies, including JMS and web services. This international standard also provides guidance with respect to the use of Enterprise Service Bus (ESB) technologies. This provides a means to derive interoperable implementations of IEC 61968-3 to IEC 61968-9. [IEC68]

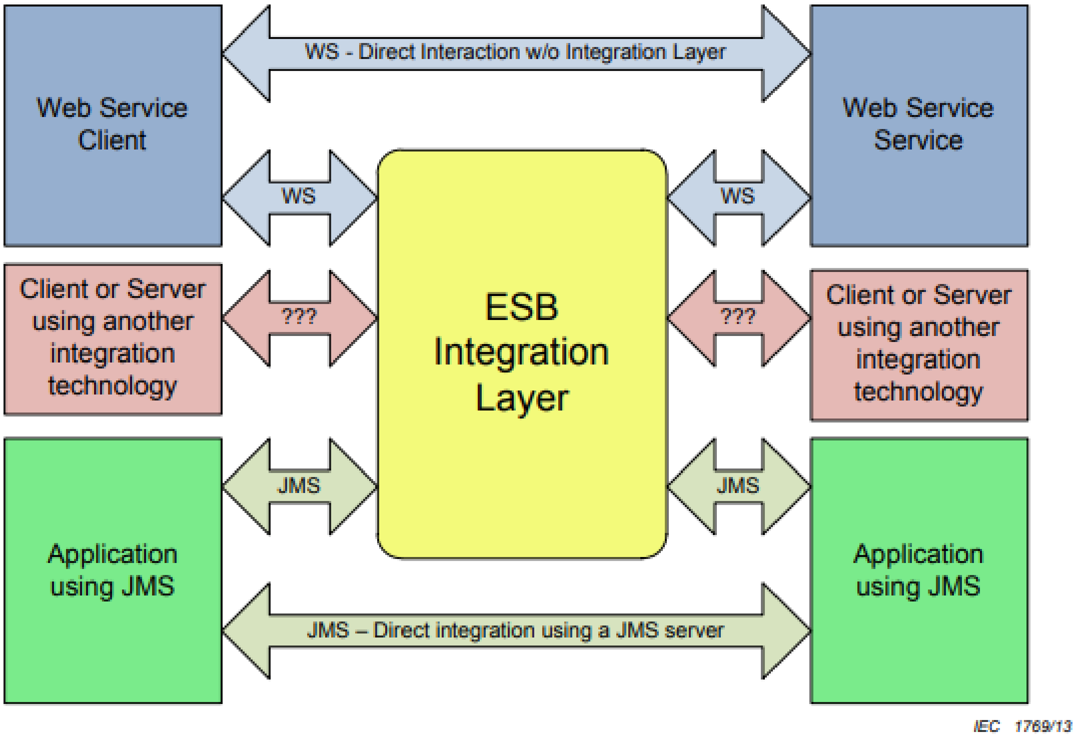
Web Service Client
WS - Direct Interaction w/o Integration Layer
Web Service Service
WS
WS
ESB Integration Layer
Client or Server using another integration technology
???
???
Client or Server using another integration technology
JMS
JMS
Application using JMS
JMS – Direct integration using a JMS server
Application using JMS
IEC 1769/13

Figure 10 - Overview of the IEC 61968 scope

Through the use of an ESB integration layer, the initiator of an information exchange could use web services and the receiver could use JMS, and vice versa. The integration layer also provides support for one-to-many information exchanges using publish/subscribe integration patterns and key functionality such as delivery assurances and security.

Complementarily, this standard can be leveraged beyond information exchanges explicitly described in the document to include other applications such as the integration of market or enterprise systems.

The **Data Source** layer refers to a set of platforms that will be integrated with the DOMINOES platform. The sources can use distinct technologies and have different ways to integrate and connect with the DOMINOES platform.

Typical and widely used standards for the integration with third party equipment, platforms and solutions include:

- **RESTful API** is a web service designed in accordance with the Representational State Transfer (REST) paradigm. It not directly linked with any particular platform or technology, although HTTP is the preferred communication protocol due to its widespread use.
- **SOAP WS** is web service implemented using Simple Object Access Protocol (SOAP) that is an application protocol specification that uses XML and a defined structure for exchanging messages through HTTP or SMTP.
- **MQTT** – Message Queuing Telemetry Transport – is an M2M/IoT connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging mechanism over TCP. [MQTT14]
- **CoAP** – The Constrained Application Protocol – is a specialized web transfer protocol for use with constrained nodes and constrained networks in IoT. It is a client/server protocol designed for M2M applications such as smart energy and building automation. [CoAP52]
- **OPC** is the interoperability standard for the secure and reliable exchange of data in the industrial automation space. It is platform independent and ensures the seamless flow of information among devices from multiple vendors. The OPC Classic specifications are based on Microsoft Windows technology using COM/DCOM (Distributed Component Object Model) for the exchange of data between software components. The specifications provide separate definitions for accessing process data, alarms and historical data. [OPC17]
- **IEC 60870-5** is a general protocol definition used mostly in electrical engineering and power system automation applications. Five different profiles (101 to 105) provide link and message exchange protocols for specific applications. [IEC70]
- **IEC 61850** is a multi-part standard that defines interoperable information exchanges between intelligent electronic devices from multiple vendors in electrical substations using TCP/IP. It is a reference architecture for electric power systems. The defined abstract data models can be mapped to a number of different protocols, like MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event), and SMV (Sampled Measured Values). [IEC50]
- **OpenADR** – Open Automated Demand Response – an open and standardized way for electricity providers and system operators to communicate DR signals with each other and with their customers using a common language over any existing TCP/IP based communications network. [OADR17]
- **IEEE 2030.5 (SEP 2.0)** is an industry effort to promote the interoperability between metering and home energy management systems, supporting device types like gateway, metering devices, and thermostat and load control devices. The standard uses IEC 61968 (CIM) as a “dictionary” and a RESTful architecture. [IEE30]

The last layer that has to be defined in the SGAM System Approach is the **Component Layer** that includes the physical distribution of all participating components in the Smart Grid context. These components comprise system & device actors, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.

Being mainly a data processing platform without any direct connection to process and field level devices, this layer is summarily represented in Figure 11, assuming that each component corresponds to one or several computer systems. A more detailed description of this layer is somewhat provided in the next section where the architecture logical diagram is presented.

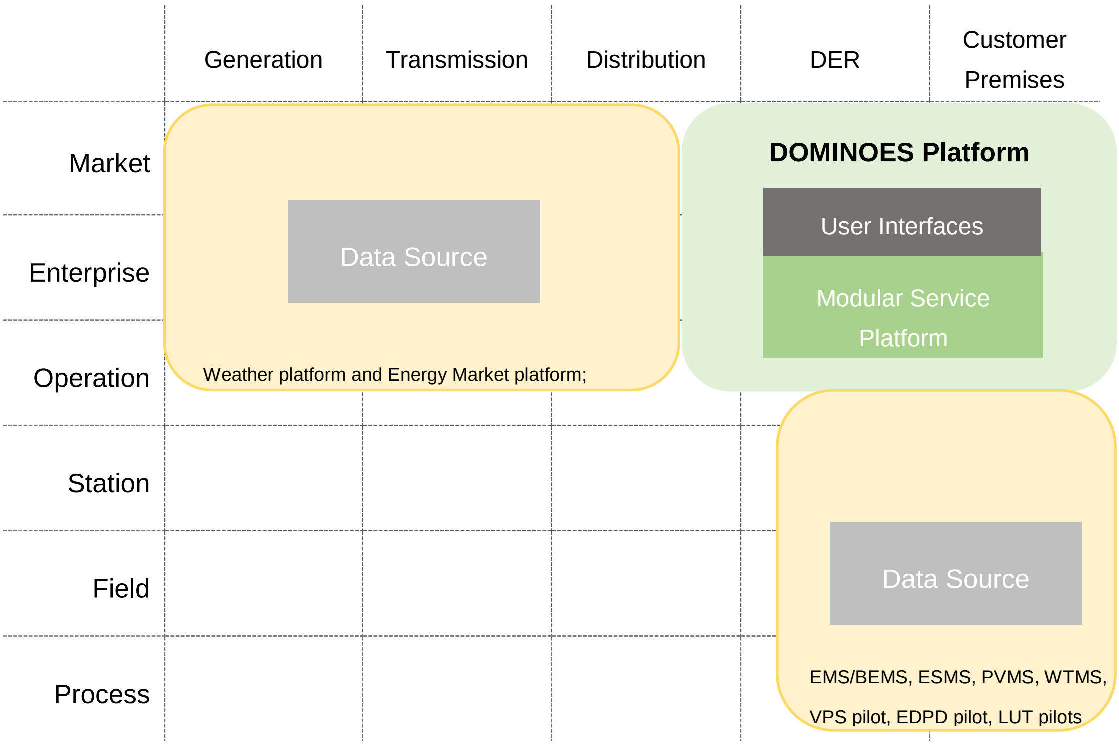

Figure 11 - DOMINOES SGAM Component Layer

2.3 Architecture diagram

To complement the architecture views developed in the previous section using the SGAM framework, a logical view, comprising the static approach of the system, presenting all the architectural system elements that provide the different functionalities for the final users, is described in this section in some detail.

The main goal of this diagram (Figure 12) is to present a logical decomposition of the system into smaller manageable components with well-defined responsibilities (in terms of data handling) and interfaces (in terms of data exchange). In the next chapter, these responsibilities are more closely associated with the recognised stakeholders in order to clarify certain roles and data flows.

On Appendix A these functional modules are associated with the planned project tasks.

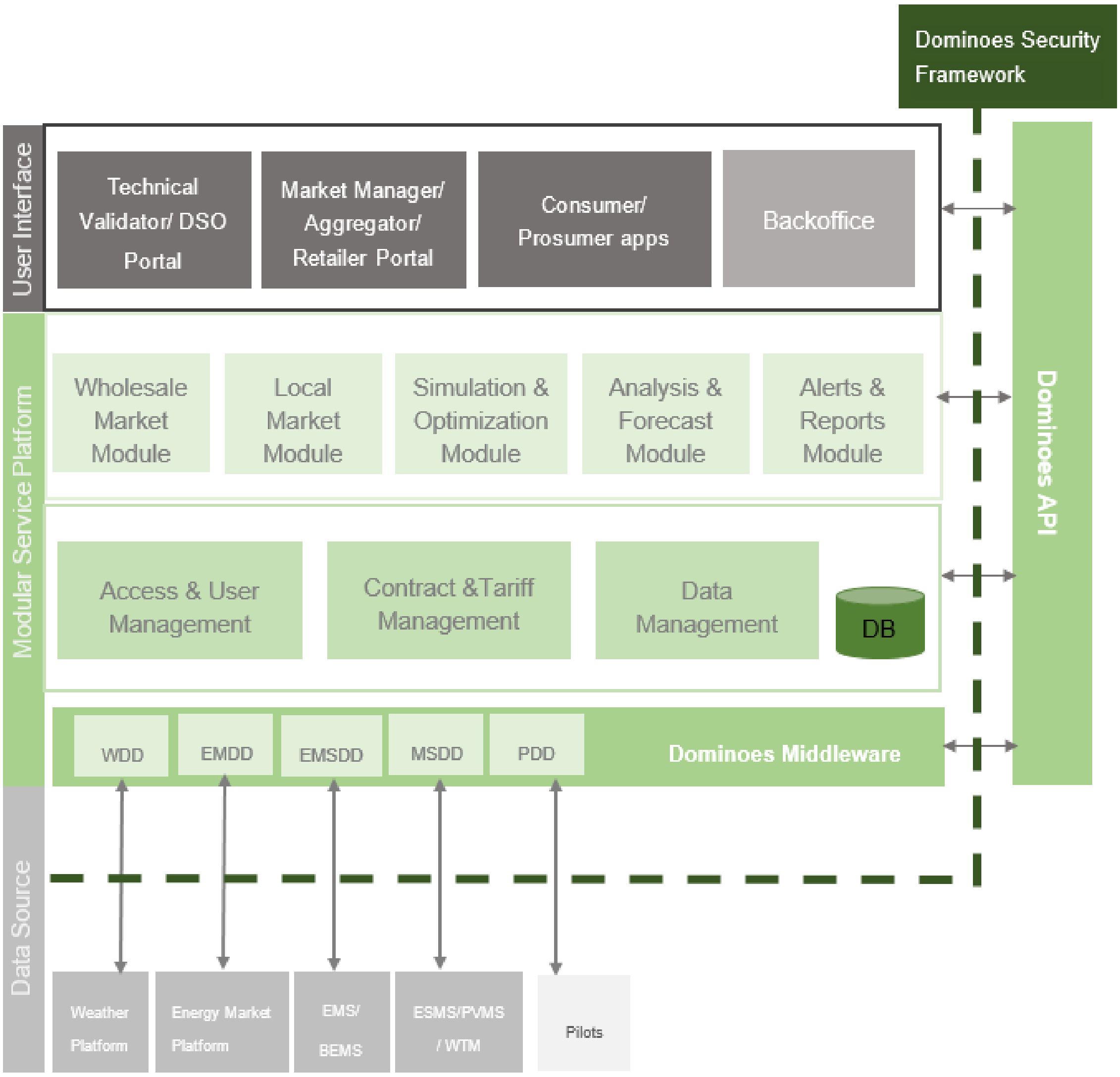

Figure 12 - Architecture diagram – logical view

In general terms, the proposed architecture for the DOMINOES platform is firstly subdivided in three distinct layers. At the bottom, the Data Source layer comprises the external operational platforms and data systems that will be used as information providers and also as interfaces with the physical world. In the middle, the Modular Service Platform comprises the core data processing components of the system and data storage. At the top, the User Interface layer comprises the web and mobile applications used by the end users.

2.3.1 Data Source

This layer includes all the external systems and platforms that are responsible for providing data, in some cases, and interacting with the field equipment, on other cases. In a strict sense, these systems although essential to the fulfilment of the project goals are not part of the DOMINOES platform and are managed and maintained by third parties. For this reason, a middleware layer capable of integrating and abstracting a varied set of external data sources is essential since it's still difficult to identify a set of standard data and communication protocols used by all the necessary interfaces.

The **Weather Platform** and the **Energy Market Platform** are good examples of data platforms that need to be integrated with the DOMINOES platform.

In this context, the Weather Platform refers to a system that can provide real-time, historical, and forecast weather data (temperature, solar irradiation, and other parameters) for specific locations.

Likewise, the Energy Market Platform refers to a system that can provide information about energy prices and tariffs, but also to a system that manages energy market transactions and auxiliary services offers/auctions.

Conversely the **EMS/BEMS** and **ESMS/PVMS/WTMS** are good examples of operational platforms that can provide data and control over physical devices and installations.

EMS (Energy Management System) or BEMS (Building EMS) are usually used to monitor and control services such as heating, ventilation and air-conditioning, ensuring the building operates efficiently.

ESMS (Energy Storage Management System) are used to manage large electrical energy storage units. PVMS (Photovoltaic Management System) and WTMS (Wind Turbines Management System) are platform developed to manage renewable energy production units.

This enumeration of data sources doesn't pretend to be exhaustive but still comprehensive and covering the requirements of the projected pilots. It should also be noted that in a real implementation more than a single weather platform, for example, could be connected to the platform.

2.3.2 Modular Service Platform

The Modular Service Platform (MSP) may be divided in three layers of identical functionality. In general, each module (service or component) in each layer communicate with other modules in the same layer, provide services to the upper layer, and use services of the lower layer. The communication between modules should use the common API although some specific external (micro) services may be invoked.

The lower layer corresponds to the modules that implement the interconnections with the Data Source layer systems as described above, being responsible for primary information processing. This group of modules constitutes the designated DOMINOES Middleware and can be implemented as isolated instances or as a set of coordinated modules. Each module should map a particular external platform or service.

The middle layer provides generic essential functionalities, well known by system designers, which are required by the majority of the higher modules including data management and access management.

- The **Database** represents the main data warehouse for the platform. It has to store configuration data as well as operation data gathered from the external sources and later processed and aggregated. In a practical implementation the database may be divided in different smaller instances rather than a single big one.
- The **Access and User Management** module is responsible for crossing the user account information with the existing profiles and data to guarantee that users having access to the correct portal and only the allowed information.
- The **Contract and Tariff Management** modules is responsible for dealing with energy contract and tariff issues that are shared by the other services.

In summary, this layer performs a set of functions that can greatly simplify the development and harmonize the interrelation of the more advanced and specific upper layer services, and including the user interfaces. In this sense, this layer ensures availability and responsiveness.

The top layer corresponds to specific functionalities selected from an analysis of the use cases descriptions. As a matter of convenience and implementation efficiency, similar functionalities where grouped in modules. In turn, each module is a collection of services. The module should provide the necessary mechanisms to coordinate the operation of the services, which might include a workflow mode and the flexibility to add (register) new services in the future as well as update the existing ones.

A detailed description of each module is presented next.

Wholesale Market Module

The Wholesale Market Module (WMM) module customizes the interactions workflow for each particular energy market (e.g. NordPool, EPEX, OMIE, Elexon). In general, the energy market services consist of multiple sub-services that enable the connection of the local market to wholesale energy market. Depending on which entity is in the role of the ECSP (Energy Community Service Provider), i.e. setting up the local market, the energy market service can provide different main functions:

- DSO as ECSP: distribution network balance settlement for local community scope.
- Retailer as ECSP: energy trading assistance, balance settlement.
- Aggregator as ECSP: reserve trading assistance

In general, the different functions offered by the energy market service enable trading, settlement, control and invoicing functions.

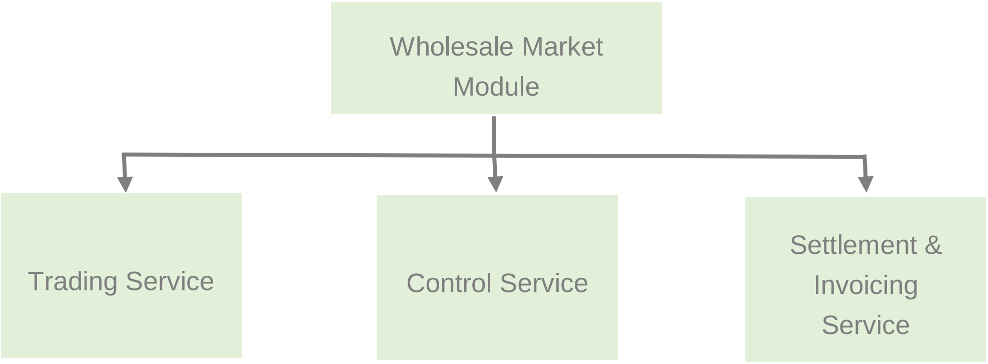

Figure 13 – Services of the Wholesale Market Module

The trading service provides functionalities for an aggregator or retailer in utilizing the local market for provision of services to e.g. the TSO or energy balancing of their own portfolios.

The settlement service enables the different acting parties to perform and receive market settlement procedures in the grid connection points. The settlement of local market actions (see below) are taken into account in conjunction with measurements of metered connection points.

The control service enables control of traded energy balancing and reserve activations during the operating day. The module can provide functionalities for e.g. disaggregation of reserve instructions to single households or devices.

The settlement and invoicing service provides functionalities for billing the customers based on the energy, grid access, and provided balancing costs and revenues, as well as local transactions.

Local Market Module

The Local Market Module (LMM) enables the different actors to harness the flexibility of the local market, as well as energy trading within the local community. The interfaces of the modules will be defined in more detail in following tasks.

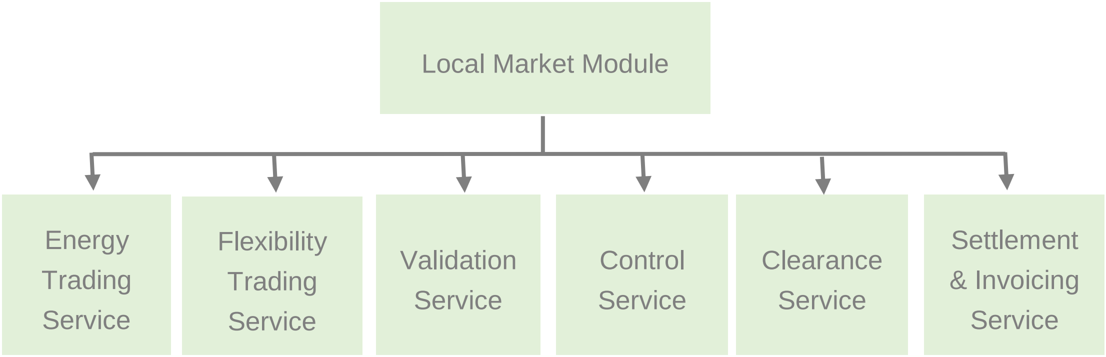

Figure 14 - Services of the Local Market Module

The energy and flexibility trading services enable the local trading and optimization of energy and flexibility of MV and LV resources within the scope of the local market. The module includes the required components and processes for the transaction management will be mainly defined in T2.2 (D2.2 & D2.3). The traded commodities will be defined in connection to wholesale market products enabling the utilization of flexibility of demand-side resources. The trading modules are utilized by the aggregators, the consumers/prosumers on the providing flexibility/energy. The DSO and aggregator can purchase the flexibility while the retailer and aggregator are purchasing energy.

The validation service performs the necessary technical validation of market transactions or programs. This validation may be required in advance or during the execution of the actions. The validation module includes the validation interfaces for the DSO as well as the implemented methods for constraining the local market transactions.

The control service defines the services for the control of the end-user resources either directly or through a device operator or an aggregator.

The clearance module implements services which clear the local market while taking into account the purchasing and selling bids as well as the constraints of the network. In the settlement and invoicing module, the settlement of the costs & tariffs of the performed transactions are calculated and invoicing launched. The clearance service provides the workflow involved in the process of transmitting, reconciling and, in some cases, confirming the transactions prior to settlement, in order to objectively establish the positions between the various stakeholders.

The settlement and invoicing service provides functionalities for billing the customers based on the market transactions taking in account the contract details.

Simulation & Optimization Module

The Simulation and Optimization Module (SOM) encapsulates simulation and optimization techniques that can be used in order to decide and recommend alternative planning and energy management strategies to the stakeholders.

RES generation profile simulations and load shifting strategies to reduce cost or maximize RES usage, using storage if available.

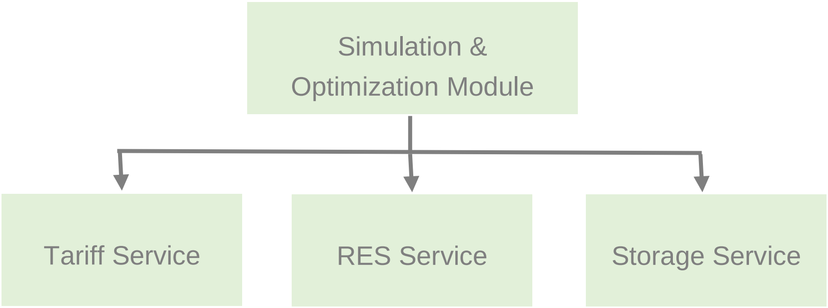

Figure 15 - Services of the Simulation and Optimization Module

The tariff service includes market tariff simulations based on generic or particular energy consumption profiles, including dynamic tariffs.

The RES service provides estimation of production profiles for a particular location and other indicators like self-consumption based on a consumption profile and ROI period if installation costs are available. A service focused on PV generation is necessary and suitable for the planned pilots.

The storage service provides estimation for storage capacity needed and usage based on particular generation/consumption profiles. Appropriate operational and financial indicators may also be provided.

Analysis and Forecast Module

The Analysis and Forecast Module (AFM) is responsible for the implementation of various advanced analytics and forecast algorithms that are useful to expedite the development of other modules, in particular, the user interfaces.

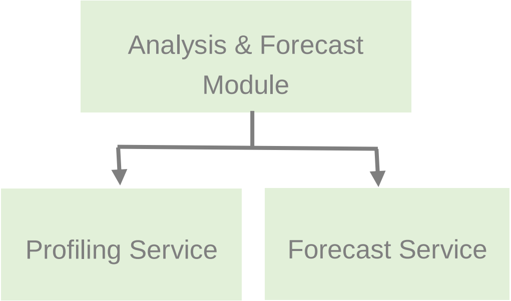

Figure 16 - Service of analysis & forecast module

The profiling service performs data aggregation, estimation, and clustering based on traditional and hybrid methodologies to generate data profiles based on different criteria for varied time intervals.

The forecast service supplies generation and consumption (load) forecasts using appropriate algorithms and external data sources if necessary.

Alerts and Reports

The Alerts and Reports Module (ARM) provides services that support the other modules in managing alerts and creating reports.

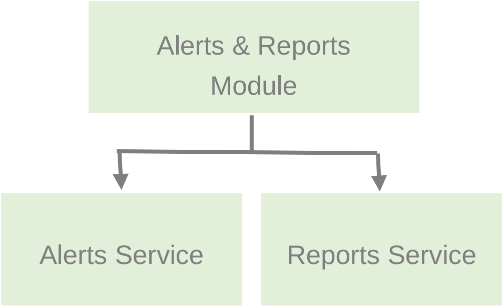

Figure 17 - Services of alerts & reports module

The alerts service is a generic alert management service with flexible condition definition, criticality based behaviour, and email notification.

The reports service creates reports (documents and spreadsheets) based on predefined templates and stored data, on demand or on a set schedule.

2.3.3 User Interface

The User Interface (UI) layer comprises the applications that interact directly with the end-users and being the visible part of the platform are, for this reason, most of the times taken as the platform itself. For this reason, it is advisable to develop these applications using recent web and mobile technologies to guarantee accessibility from different types of devices and environments. On the other hand, this development is greatly simplified by the availability of a RESTful API, as proposed.

Given that the platform will be used by distinct categories of users/stakeholders with different functionality and usability requirements it is foreseen that different applications should be developed instead of concentrating everything on a single monolithic application much more difficult to navigate and much less intuitive. Three distinct applications are suggested having in mind the key targeted end-user. The **DSO/Technical Validator Portal** and the **Market Manager/Aggregator/Retailer Portal** for professional users and **Consumer/Prosumer Apps** for the domestic, commercial and industrial users.

In this initial stage, some modules (functionalities) that must be part of the UIs include:

- **Market Dashboard –** a view containing a short summary of the general status of the current and near future market transactions. This view could complementarily present a short-term analysis of the market evolution in terms of aggregated values of generation/flexibility and settlement.
- **Market Analysis** – a view providing the possibility of aggregating and comparing market data based on a set of filters and time intervals.
- **Market Planning** – a view providing the tools needed for planning the next market transaction, offering appropriate forecast and recommendations.
- **Contract Management –** a view containing the necessary information to manage energy contracts, including form and workflow handling**.**
- **Contract Tracking** – a view providing information about the evolution of the contracts in terms of established goals and opt-in/opt-out settings.
- **Operation Dashboard –** a view containing information about operational details related with a contract execution, for example, unavailability or maintenance periods and validation issues.
- **Notifications –** a view containing a list of recent notifications related with market transaction or other types of alarms that may be defined.

The **Backoffice** user interface is required for the administration (setup and management) of the platform. The functionalities of this application include:

- User & Access CRUD (Create, Read, Update, and Delete) management.
- Contract & Tariff CRUD management.
- Data management status.

2.3.4 DOMINOES API

The RESTful API module offers a standard and open way to access data and metadata stored on the platform, as well as exposing much of the functionality provided by the services.

This API is a standard access to web applications data, providing a powerful yet simple tool to integrate different modules and sub-systems. This approach allows quick prototyping and interoperability capabilities between web applications and other systems in the physical world. This integration potential is enabled by the existing web infrastructure.

2.4 Data handling

The successful development of innovative products and services such as the implementation of the DOMINOES platform faces the same opportunities and challenges that other Smart Grid developments (smart metering, for example) confront.

One of the major difficulties arises from the required interaction between the energy sector and a heterogeneous ICT infrastructure, in general, and with the diverse data handling models that can be created (or supported) in future (or existing) energy markets, in particular. Expert Group 3 (EG3) within the Smart Grids Task Force reported on this last topic, identifying three distinct use cases and the concept of data hub, as standardized centralized or decentralized point for different market stakeholders to collect all operational and data as well as all necessary data to facilitate the market [EG313].

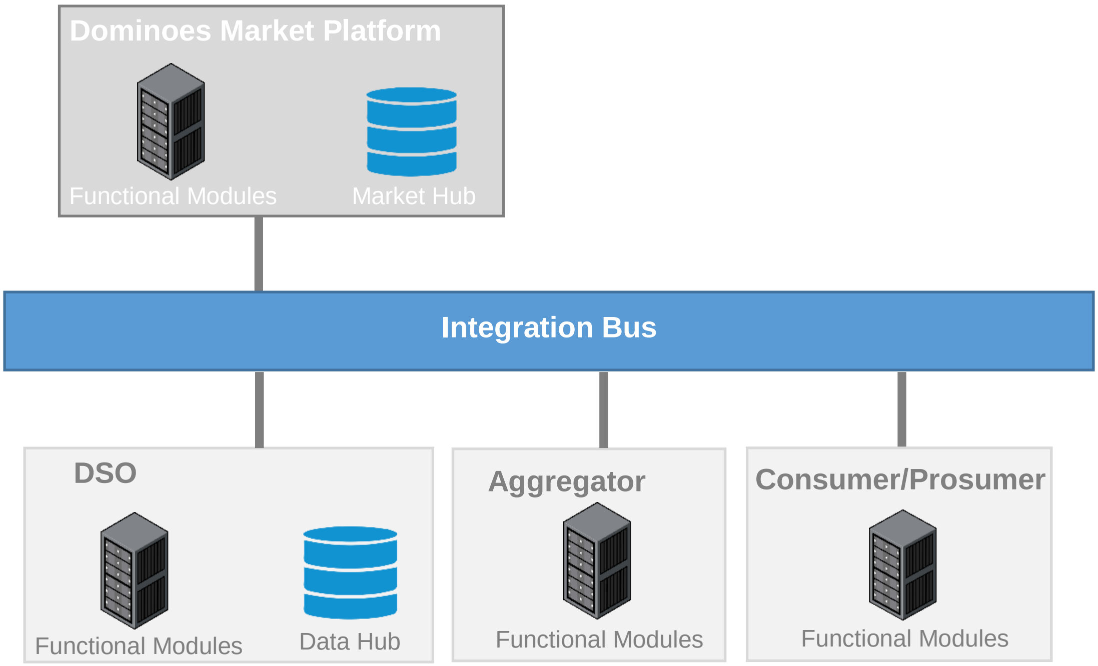

Figure 18 – Data handling – DSO as Market Facilitator

The proposed reference architecture can be deployed in any of the three use cases mentioned. Figure 18 represents this for the first use case: DSO as Market Facilitator. In this example, DOMINOES platform would constitute a Market Data Hub, complementing the DSO Data Hub and associated functionalities and responsibilities for the operational management of the grid.

3 Mapping the use cases

In this section, the uses cases are mapped to the reference architecture components. For each use case scenario, the associated services are identified. In the case of the user interfaces the association identifies the stakeholders for each use case.

In this way, the coverage of proposed components is thoroughly demonstrated. In fact, there are a few modules that seem as unnecessary at this stage. Yet, we think that it’s wise to include them for the sake of having a more comprehensive reference design.

3.1 Use cases vs services

Table 1 maps UC1 – Local market flexibility and energy distributed resources for optimal grid management.

Table 1: Use case 1 vs services association

	Module															
	WMM			LMM						SOM			AFM		ARM	
UC1 scenarios	Trading Service	Control Service	Invoicing & Settlement Service	Validation Service	Energy Trading Service	Flexibility Trading Service	Control Service	Clearance Service	Invoicing & Settlement Service	Tariff Service	RES Service	Storage Service	Profiling Service	Forecast Service	Alerts Service	Reports Service
Procurement of flexibility to solve local grid technical constraints						X	X		X		X	X	X	X	X	X
Emergency scenario activation by the Distribution Grid Optimizer due to a critical constraint					X	X	X		X		X	X	X	X	X	X

Table 2 maps UC2 – Local Energy Market Data Hub Manager and Technical Validator of market transactions.

Table 2: Use case 2 vs services association

	Module																
	WMM			LMM						SOM			AFM		ARM	
UC2 scenarios	Trading Service	Control Service	Invoicing & Settlement Service	Validation Service	Energy Trading Service	Flexibility Trading Service	Control Service	Clearance Service	Invoicing & Settlement Service	Tariff Service	RES Service	Storage Service	Profiling Service	Forecast Service	Alerts Service	Reports Service
Market data management					X	X							X	X	X	X
Technical validation of local market program				X	X	X									X	X
Transaction execution verification					X	X		X							X	X

Table 3 maps UC3 – Local community market with flexibility and energy asset management for energy community value.

Table 3: Use case 3 vs services association

	Module															
	WMM			LMM						SOM			AFM		ARM	
UC3 scenarios	Trading Service	Control Service	Invoicing & Settlement Service	Validation Service	Energy Trading Service	Flexibility Trading Service	Control Service	Clearance Service	Invoicing & Settlement Service	Tariff Service	RES Service	Storage Service	Profiling Service	Forecast Service	Alerts Service	Reports Service
Day-ahead	X		X		X	X			X		X	X		X	X	X
Intra-day	X		X		X	X			X		X	X		X	X	X
P2P transactions management					X				X							

Table 4 maps UC4 – Local community flexibility and energy asset management for retailer value

Table 4: Use case 4 vs services association

	Module															
	WMM			LMM						SOM			AFM		ARM	
UC4 scenarios	Trading Service	Control Service	Invoicing & Settlement Service	Validation Service	Energy Trading Service	Flexibility Trading Service	Control Service	Clearance Service	Invoicing & Settlement Service	Tariff Service	RES Service	Storage Service	Profiling Service	Forecast Service	Alerts Service	Reports Service
Optimization of energy sourcing	X		X		X				X							
Correction the deviation	X	X	X		X				X							

Table 5 maps UC5 – Local community flexibility and energy asset management for wholesale and energy system market value

Table 5: Use case 5 vs services association

	Module															
	WMM			LMM						SOM			AFM		ARM	
UC5 scenarios	Trading Service	Control Service	Invoicing & Settlement Service	Validation Service	Energy Trading Service	Flexibility Trading Service	Control Service	Clearance Service	Invoicing & Settlement Service	Tariff Service	RES Service	Storage Service	Profiling Service	Forecast Service	Alerts Service	Reports Service
Aggregator selling balancing services	X	X	X		X				X							
Prosumers selling flexibility	X	X	X		X				X							
Retail services	X	X	X		X				X							

3.2 Use cases vs user interfaces

Table 6 associates the key stakeholders of the foreseen user interfaces for each use case. This association reveals that the proposed distinct interfaces are well defined since there is almost a one to one relationship between end-users and portals.

Table 6: Use cases vs stakeholders association

	User Interfaces		
Use Cases	DSO/Technical Validator Portal	Market Manager/ Aggregator/Retailer Portal	Consumer/Prosumer apps
UC1 - Local market flexibility and energy distributed resources for optimal grid management	DSO		
UC2 - Local Energy Market Data Hub Manager and Technical Validator of market transactions	DSO	Market Manager	
UC3 - Local community market with flexibility and energy asset management for energy community	DSO	Retailer	Prosumer/Consumer
UC4 - Local community flexibility and energy asset management for retailer value		Retailer	
UC5 - Local community flexibility and energy asset management for wholesale and energy system market value	TSO DSO	Retailer	

4 Secure data handling requirements

4.1 Introduction

4.1.1 Legislation, regulations, standardisation

Privacy and data protection, though connected, are normally recognised as two separate rights. Here, we will provide necessary description of privacy and data protection before discussing their importance and impacts on the community. [EDPS18].

In the EU, human dignity has been considered as a fundamental right. In other words, privacy or the right to a private life, refers to the control of individual information. Privacy I not only an individual right but also a social value. Arguably, privacy is recognised as a universal human right but data protection is not.

Data protection is to protect information related to an identified or identifiable natural person, including names, ages, photographs and email addresses. Other information such as communication content and IP addresses may also be considered personal data due to their links with users of communication services. Both privacy and data protection are instrumental in preserving and promoting fundamental values and rights, and to involve other rights and freedoms, e.g. free speech or the right to assembly.

Privacy and data protection are two rights included in the EU Treaties and in the EU Charter of Fundamental Rights. The Charter clearly mentions the protection of personal data (Article 8), which becomes part of the Lisbon Treaty in 2009, leading to a formal legal value. In addition, Article 16 of the Treaty on the Functioning of the European Union obliges the EU to lay down data protection rules for the processing of personal data. [FREU18]

In April 2016, the EU adopted a new legal framework – the General Data Protection Regulation (GDPR) and the Data Protection Directive for the law enforcement and police area. Fully deployed in May 2018, the GDPR is the most comprehensive and progressive data protection legislation in the world, capable of dealing with the implication of the digital world.

In most countries, national Data Protection Authorities (DPAs) or Regulators have been established to be secure data protection. For the enforcement of data protection laws to be applicable, DPAs have been given the authority to investigate, detect and punish the violations whilst taking the responsibility to raise awareness of data protection rights and obligations. Moreover, close cooperation between DPAs (Article 29 Working Party, EDPB) guarantee certain consistency of data protection in the EU.

Currently, GDPR considers the following general data protection principles, compared to its early version in the Data Protection Act 1998 (the 1998 Act) [GDPR18]:

Table 7: GDPR considers the following general data protection principles

Principle	1998 Act	GDPR
1	Fair and lawful	Lawfulness, fairness and transparency
2	Purposes	Purpose limitation
3	Adequacy	Data minimisation
4	Accuracy	Accuracy
5	Retention	Storage limitation
6	Rights	No principle – separate provision in Chapter III
7	Security	Integrity and confidentiality
8	International transfers	No principle – separate provisions in Chapter V
9	(no equivalent)	Accountability

4.2 Privacy in smart grids

4.2.1 Challenges

A smart grid is a complex infrastructure based on a set of seven chief domains: bulk generation, energy distribution, power transmission, operation and control, market, service providers and customers. [NICS12] Each domain comprises several elements such as organisation, buildings, system resources and others. Of these, the backhaul communication and the Internet are critical for connecting different entities through an Advanced Metering Infrastructure (AMI), an interface for managing and interacting with smart meters and utility business systems. The privacy related issue is that for proper delivery of the AMI system, detailed ad precise information about the user’s electricity usage is required. Therefore, while the smart grid system offers many benefits, it has serious weaknesses from the level of privacy perspective as data is created, transferred and stored remotely and locally. In a smart grid environment, we need to address the following key questions when setting the policies on data privacy [SGP12]:

- Who owns the data of the customer?
- How is the access to and use of customer data regulated?
- Who guarantees privacy and security of customer data?
- Will sale or transfer of customer data be allowed? And under what terms and to whose benefit?
- In jurisdictions with retail choice, are measures needed to ensure competing electricity providers have access to customer data on the same terms as the incumbent utility?

4.2.2 Data handling

Smart grid is designed to enable utilities, customers and third-party providers to monitor and control energy use. Data collected by smart grid will provide many advantages to all the involved parties, including better decisions for energy-usage, deeper understanding of user demands and better energy distribution efficiency. This raises the concern of data handling and security applications. Here, we use a few examples to explain the procedure and guidelines of data handling for security.

NIST's NISTIR 7628 document provides general, policy-level guidance on data handling. [NISTIR10] For example, the guidance on retention recommends:

“Limit information retention. Data, and subsequently created information that reveals personal information or activities from and about a specific consumer location, should be retained only for as long as necessary to fulfil the purposes that have been communicated to the energy consumers.”

The guidance on aggregation recommends:

“Energy data and any resulting information, such as monthly charges for service, collected as a result of smart grid operations should be aggregated anonymised by removing personal information elements wherever possible to ensure that energy data from specific consumer locations is limited appropriately. “

The guidance on deletion recommends:

“When no longer necessary, consistent with data retention and destruction requirements, the data and information, in all forms, should be irreversibly destroyed.”

In this section, we also discuss data handling in terms of its application in smart grid [SCSG15].

Data minimisation: that is to say, how much data must be collected and how long data should be stored. Smart grid applications, e.g. demand-response analysis, require the collection and storage of fine-grained data. Any fine-grained data could be re-edited if some of it is no longer needed. This re-editing exercise may trigger privacy implications. One of the key factors when people consider safe data collection and retention policies is the ability of identifying electricity appliances via non-instructive load monitoring, which can be achieved by monitoring residential electricity consumption.

Data aggregation: privacy risks may be reduced by computing aggregates across people and deleting individual usage data. Unfortunately, the release of the aggregated data still has privacy implications. Evidence has shown that privacy increases as the size of the aggregate increases. The other issue is that aggregation does not protect an individual when all the individuals whose data is aggregated are similar.

Data access: one concern for real-time electricity consumption data is that it may facilitate burglaries. Latency may help mitigate this privacy threat. For example, consumption data may be released to the customers one week or one month later.

Anonymised data: simply removing identifying information, such as name or address, is not enough to anonymise different personal data. For example, location traces may still reveal home/work locations from the identities of individuals can be deduced. A linkage attack may be used to de-anonymise the data.

4.2.3 Privacy and data protection challenges for smart metering

Smart metering relates to the use of intelligent metering devices at customers and the standard process of reading, processing and supplying the consumption information to customers. Smart metering systems have the benefits of access to detailed energy use, accurate and timely billing, better power quality and breakdown management, and reducing metering readings and misuse and fraud. In spite of extra costs applied to smart metering systems, data protection and privacy assurance is one of the major concerns using smart metering systems. We need to ensure that secure data communication and protection of end-users data against unauthorised access or hacking.

A standard smart metering architecture has the following components [CSMD10]:

(1) Metering device with corresponding devices on the side of end-users, connected to smart home controllers for managing appliance use.

(2) Communication and data processing unit between the customer devices and the transactional systems of the utility suppliers.

(3) Central data management system which is located on the supplier's side and turn on/off the utility, to process data and to archive data, etc.

Two European directives are applicable to data processing in smart meters [SGED11]: (1) The European Data Protection Directive which governs the processing of personal data by data controllers and grants rights to individuals. (2) The European Privacy and Electronic Communications Directive, aiming to make it technology neutral. Under these directives, a set of requirements for data protection is identified. First, personal data processing is allowed only if specific legal purposes apply. Secondly, personal data collected for one purpose cannot be used in another application without permission. Thirdly, restrictions must be applied for the personal data to be transferred to other countries. Finally, strict obligation needs to be in place for ensuring adequate security.

Smart Energy Meters, a common form of smart grid technology, are digital meters that replace the old analog meters used at homes to record electrical usage. They cannot transfer any sensitive data such as customer name, e.g. ID number. The information that smart meters may transfer from the customer to the supplier includes: smart meter ID number, meter readings, information types, date and time, load profile. Before setting up proper strategies to handle the transmission data, we need to identify and understand important challenges of the privacy issues. Challenges in data protection include [ISIM13]:

(1) Challenges related to the trust of the parties engaged in the process.

The main trust relationships are built between the customers, the suppliers and the grid operators. Customers' trust is directly related to the privacy of the measured data and it must be clearly stated what party can access to the data for what purpose. The trust from the supplier or grid operator is mainly about the data correctness whilst ensuring the correct correspondence between the measurements and the bills. As described above, the adoption of smart metering changes the trust model to a mutual trust partner.

(2) Challenges related to the smart meter hardware.

Due to the economic requirements, smart meters cannot be equipped with high performance computers. Instead, fairly simple and compact devices with limited computational power are put into practice. Consequently, simple homomorphic encryptions such as symmetric cryptography will be implemented, which cannot handle integrity, distributed authentication and heavy public key data encryption. Unfortunately, homomorphic operations need more intelligent and complicated devices and hence violate the cost effectiveness.

(3) Challenges related to cryptographic protocols.

For private protocols based on homomorphic encryption, it is a common practice that a secret key is shared among several customers and the utility company. Key disclosure may trigger the risk of losing correct authentication. Other problems include the risk of forgery by users who are familiar with the system and the decryption technology. Possible solutions to these problems include the deployment of unusual key distribution mechanisms.

4.3 Security in smart grids

4.3.1 Smart grid information security

Smart grid refers to a network of sensors, monitors, devices and computers for data acquisition and analysis. Cyber-attacks may arise from one or more components of these physical elements. Smart grid security may have the concerns as confidentiality, integrity and availability. Confidentiality is to protect both consumers and operational data. Integrity is to make sure metering and billing is going well and the stability of the grid in terms of operation. Availability refers to the continuation of the power to be transmitted and received by customers.

To deal with the above challenges, it is necessary to address data handling of consumer data as well as control and automation readings and commands processed by intelligent decision-making systems. To secure data handling of these data, we have to understand: (1) The possibility of inferring relevant information from personal data. (2) Metering data must be securely accessible by several independent actors, e.g. DSO, service provider and the customer.

4.3.2 Cyber security

To achieve the three cyber security objectives availability, integrity and confidentiality, there is a large number of cyber-physical security requirements that can be applied to smart grids encompassing. The security issues and requirements concerning information and network systems. The physical equipment and environment protections as well as employee ad staff security policies. They are [CSSG12]:

- Attack detection and resilience operations. Smart grid has an open communication network over wide areas. Therefore, it is nearly impossible to protect every node in smart grid from network attacks. Consequently, the communication network needs to continuously profile, test and compare network traffic status in order to identify abnormal incidents. In addition, the network also needs to have the self-healing ability to maintain network operations in case of attacks.
- Identification, authentication and access control. Smart grid infrastructure has a massive number of electronic devices and users. Identification and authentication is to verify the identity of a device or user as a prerequisite for granting access to resources in smart grid to ensure the safety of the personnel and property.
- Secure and efficient communication protocols. Time-criticality and security in smart grid are two contradict objectives. Networks in smart grid cannot be kept secure all the time, physically-protected and high-bandwidth communication channels require proper trade-offs to balance communication efficiency and information security in the design of the smart grid architecture.

4.3.3 SGAM and cyber security

The SGAM framework aims to integrate several state of the art approaches in a European setting. The purpose of using SGAM includes mapping different smart grid use cases to a common architecture model, establishing a framework for analysing the implementations of a smart grid architecture, providing a common view and language for stakeholders and identifying standardisation **and interoperability gaps.**

SGAM has been used as a reference model in many EU smart grid projects, as a powerful tool for establishing a common language between experts and stakeholders in the smart grid. It facilitates the architecture development process **and** support the representation of smart grid use-cases and interoperability viewpoints for current and future energy grid implementations. In the EU FP7 project DISCERN [DISCERN16], for example, SGAM has been used to depict the present system architecture of involving DSOs by having them individually answer questions relating to each SGAM interoperability layer.

To link the security policy and standards to the SGAM model, we here give abbreviations of the SGAM model components:

SGAM Layer: B – Business; F – Function; I – Information; C – Communication; Phy – Component.

SGAM Domains: G – Generation; T – Transmission; D – Distribution; CP – Customer.

SGAM Zones: M – Market; E – Enterprise; O – Operation; S – Station; F – Field; P – Process.

The following table shows a generic mapping of the requirement standards to SGAM.

Table 8: Mapping of the requirement standards to SGAM

Standard	SGAM Layer	Domains	Zones
ISO/IEC 15408-1	n.a.	n.a.	n.a.
ISO/IEC 15408-2	F/I/C/Phy	G/T/D/DER/CP	P/F/S/O
ISO/IEC 15408-3	F/I/C/Phy	G/T/D/DER/CP	F/S/O
ISO/IEC 18045	n.a.	n.a.	n.a.
ISO/IEC19790	Phy/C	G/T/D/DER/CP	P/F/S
ISO/IEC27001	B/F/I	G/T/D/DER/CP	O/E/M
ISO/IEC27002	B/F/I	G/T/D/DER/CP	O/E/M/S/F
ISO/IEC 27019	B/F/I	G/T/D/DER	E/O/S/F
IEC 62443-2-4(CD)	F/I/C/Phy	T/D/DER/CP	E/O/S/F/P
IEC 62443-3-3(IS)	F/I/C/Phy	T/D/DER/CP	P/F/S/O/E

IEC 62443-4-2(WD)	F/I/C/Phy	D/DER/CP	P/F/S/O
IEEE 1686	Phy	G/T/D	F/P
IEEE C37.240	Phy/C	G/T/D/DER	F/P
IEC 62443-2-1	B/F/I	G/T/D/DER	O/S/F

The following table shows a mapping of the solution standards to SGAM

Table 9: Mapping of the solution standards to SGAM

Standard	SGAM Layer	Domains	Zones
ISO/IEC 15118-1 (FDIS)	F/I/C	T/D/DER/CP	M/E/O/S/F/P
IEC 62056-5-3 (IS)	F/I/C	T/D/DER/CP	O/S/F/P
IEC 62351-3 (TS)	I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-4 (TS)	I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-5 (TS)	I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-6 (TS)	I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-7 (TS)	I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-8 (TS)	F/I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-9 (TS)	F/I/C	G/T/D/DER/CP	E/O/S/F
IEC 62351-10 (TR)	B/F/I/C/Phy	G/T/D/DER/CP	M/E/O/S/F
IEC 62351-11 (WD)	F/I/C	G/T/D/DER/CP	E/O/S/F
IETF RFC 6960 OCSP	I/C	G/T/D/DER/CP	M/E/O/S/F
IETF RFC 7252	I/C	G/T/D/DER/CP	M/E/O/S/F/P
IETF I-D draft-weis-gdoi-iec62351-9	I/C	G/T/D/DER/CP	M/E/O/S/F/P
IETF RFC 7030 EST	I/C	G/T/D/DER/CP	M/E/O/S/F

For the selected standards shown above, we shall be able to provide an overview explain the generic goal of the standard as well as a status update in terms of the document state. We also can describe the gaps that relate to technical shortcomings or missing coverage of the dedicated requirements. For all these description, please refer to [SGIS14].

4.3.4 Additional security standards to be considered

Further security standards have been identified or recommended by experts, which address security in the target domain and could be relevant. These standards are listed here for possible use in the coming applications.

Table 10: Security standards

SGAM Layer	Standard	Comment
B/F/I	IEC 62443-2-1	Security for industrial automation and control systems – Network and system security.
F/I/C	ISA 100.11a	Industrial communication networks.
C	ISO 24759	Test requirements for cryptographic modules.
C	ISO 18367	Algorithm and security mechanism conformance testing.
C	ISO 17825	Testing methods for the mitigation of non-invasive attack classes against crypto modules.
B/F/I	ISO 27005	Information technology – Security techniques.
B/F/I	ISO 31000:2009	Risk management.
B/F/I	ISO 30104	Physical security attacks, mitigation techniques and security requirements.
B/F/I	NIST SP 800-39	Managing information security risk.

4.4 Measuring

Cyber security must be measured regarding its robustness, resiliency or reliability of the network under attacks. The number and impact (e.g. monetary, image, lives) of incidents can be counted. Detailed reports must be recorded and the degree of robustness must be controlled during the operation [ENISA12].

Need of European common framework: A standard framework is required to ensure a minimum level of agreement on security and resiliency requirements across EU, laying the foundation for a minimum set of auditable controls over EU. This allows National Regulatory Authorities (NRAs) to measure the security control.

Components of the framework: the following items shall be considered: (1) A set of standards and guidelines. (2) Certification schemes aiming products/devices and grid operators. (3) A certification authority as a Public-Private Partner (PPP). (4) Regulatory mechanisms for mandatory certifications and risks assessments. (5) A platform for knowledge sharing among DSOs -TSOs.

A set of standards and guidelines: We have such a list of standards and guidelines: (1) Common reference architecture. (2) Reference risk assessment methodology. (3) Methodology for assessing interdependence. (4) Incident handling reference strategy. (5) Technical requirements for products. (6) Organisational requirements for legal entities. (7) Standard requirements matching requirements for products with organisational requirements. (8) Standard requirements for security governance.

Regulatory mechanisms: (1) Requirements are stringent for system organisations. (2) Incompliance come with regulatory pressure (e.g. monetary files). (3) The European Directive 2008 114/EC include TSOs and DSOs. (4) Incompliance results should not reveal confidential information of the grid operator.

5 Conclusions

D1.2 provides a detailed overview of the overall reference architecture of the DOMINOES project developed using the SGAM Framework approach and the information from D1.1 *Local market reference architecture and business requirements*, namely, the stakeholders (end users most of them).

The logical view diagram that complements the design provides a description of each layer within the DOMINOES Reference Architecture. The proposed modules are also mapped against the identified uses case scenarios. The proposed architecture is flexible, scalable, and open.

Such description is essential for the development of the project and can also be explored in the future by the project's stakeholders. This reference architecture constitutes the starting point for the development of the platform and the implementation of the pilots.

References

[CEN11] Smart Grids. Accessed on 20/08/2018 https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

[CEN12] SGCG/M490/G_Smart Grid Set of Standards. Accessed on 20/08/2018 https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[CoAP52] RFC 7252 Constrained Application Protocol. Accessed on 20/08/2018 http://coap.technology/

[CSMD10] M.S.Jaganmohan, K. Manikandan, Easun Reyrolle Ltd, Challenges in Smart Meter Design. Accessed on 16/06/2018. https://pdfs.semanticscholar.org/972a/bb035dd32f4af53ea0269785f57b499c0573.pdf

[CSSG12] Cyber Security of the Smart Grids. Accessed on 15/06/2018. http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=1761

[DISCERN16] https://www.discern.eu/ Accessed on 21/08/2018

[DOM18] DOMINOES DELIVERABLE: D1.1 Local market reference architecture and business requirements.

[EDPS18] EUROPEAN DATA PROTECTION SUPERVISOR, Data Protection. Accessed on 30/07/2018. https://edps.europa.eu/data-protection/data-protection_en

[EG313] EG3 – Smart Grids Task Force, EG3 First Year Report: Options on handling Smart Grids Data. Accessed on 24/08/2018. https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group3_first_year_report.pdf

[ENISA12] https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations
Accessed on 15/06/2018.

[FREU18] Respect for fundamental rights in the European Union. Accessed on 16/06/2018. http://www.europarl.europa.eu/RegData/etudes/PERI/2017/600415/IPOL_PERI(2017)600415_EN.pdf

[GDPR18] https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf
Accessed on 16/06/2018.

[IEC50] International Electrotechnical Commission. Power Utility Automation (IEC 61850). Accessed on 20/08/2018 https://webstore.iec.ch/publication/6028

[IEC51] IEC TC57 WG15:IEC 62351 Security Standards for the Power System Information Infrastructure. Accessed on 20/08/2018 http://iectc57.ucaiug.org/wg15public/Public%20Documents/White%20Paper%20on%20Security%20Standards%20in%20IEC%20TC57.pdf

PUBLIC

[IEC68] International Electrotechnical Commission. Common Information Model (CIM) / Distribution Management (IEC 61968). Accessed on 20/08/2018
https://webstore.iec.ch/publication/27527

[IEC70] International Electrotechnical Commission. Common Information Model (CIM) / Energy Management. IEC 61970. Accessed on 20/08/2018
https://webstore.iec.ch/publication/61167

[IEE30] IEEE 2030.5-2018 Standard for Smart Energy Profile Application Protocol. Accessed on 20/08/2018
https://standards.ieee.org/findstds/standard/2030.5-2018.html

[ISIM13] Tomaz Zabkowski, Krzysztof Gajowniczek, Smart Metering And Data Privacy Issues. Accessed on 16/06/2018.
http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-266914f3-bbde-4035-87b3-8b1ed4fa83cb/c/ISIM_Vol_2_3__239-249.pdf

[MQTT14] http://mqtt.org/
Accessed on 20/08/2018

[NICS12] S. Zeadally, A. Pathan, C. Alcaraz, and M. Badra, “Towards Privacy Protection in Smart Grid”. Accessed on 30/07/2018.
https://www.nics.uma.es/pub/papers/1750.pdf

[NISTIR10] Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. Accessed on 16/06/2018.
https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

[OPC17] Open Platform Communiations (OPC), Classic Specification. Accessed on 20/08/2018
https://opcfoundation.org/about/opc-technologies/opc-classic/

[OAD17] Open Automated Demand Response (OpenADR). Accessed on 20/08/2018
http://www.openadr.org/

[SCSG15] Sanjay Goel and Yuan Hong, "Security Challenges in Smart Grid Implementation". Accessed on 16/06/2018.
https://pdfs.semanticscholar.org/c4f8/ad967bb11fa144b7cd1537a0e4f88e76ad87.pdf

[SGED11] Daniela Havlíková,"Smart Grids in the European data protection legal framework". Accessed on 15/06/2018
https://www.duo.uio.no/bitstream/handle/10852/22927/HAVLIKOVAx-xMaster.pdf?sequence=2

[SGIS14] SG-CG/M490/H_ Smart Grid Information Security. Accessed on 16/07/2018
ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

[SGP12] U.S. Department of energy Smart Grid Privacy Workshop Summary Report. Accessed on 16/06/2018.
https://www.energy.gov/sites/prod/files/2014/12/f19/SGPrivacyReport2012.pdf

Appendix A

The following table associates the planned project tasks with the reference architecture modules.

Table 1: Planned tasks

Project Tasks		Architecture
T2.2 – Design of a scalable local market infrastructure		
	2.2.1 – Information exchange and market interfaces	• Wholesale/Local Market Service
	2.2.2 – Overall market architecture design	• Wholesale/Local Market Service
	2.2.3 – Trading modules	• Wholesale/Local Market Service
	2.2.4 – Control modules	• Wholesale/Local Market Service
	2.2.5 – Settlement modules	• Wholesale/Local Market Service
	2.2.6 – Invoicing modules	• Wholesale/Local Market Service
	2.2.7 – Module integration and architecture testing	• Middleware DOMINOES
T2.4 - Stakeholder engagement, interfacing and interoperability		
	2.4.3 – Development of web interface for end-users	• DSO Portal • Market Manager/ Aggregator/Retailer Portal • Consumer/ Prosumer Web app
	2.4.4 – Development of mobile interface for end-users	• Consumer/ Prosumer Web app
	2.4.5 – Development of the backoffice tool	• Backoffice