Platone

PLATFORM FOR OPERATION OF DISTRIBUTION NETWORKS

Platone

PLATform for Operation of distribution NEtworks

D2.9 v1.0

Specification of the interoperability and standard communication protocols (v1)

Project name	Platone
Contractual delivery date:	31.12.2021
Actual delivery date:	22.12.2021
Main responsible:	Jonas Baude, RWTH Aachen University
Work package:	WP2 – Platform Implementation and Data Handling
Security:	P
Nature:	R
Version:	V1.0
Total number of pages:	28

Abstract

This deliverable defines the intra-platform interoperability mechanisms and standard communication protocols necessary for the implementation of the Platone Open Framework. In addition it reports on the specification for data interoperability, with a focus on security and privacy best practices. It also presents how these are implemented in the different platforms of the Platone Open Framework and in the Platone field trials and gives an outlook to foreseen features in the next releases.

Keyword list

Platone Open Framework, Data Interoperability, Security Aspects, Privacy Considerations

Executive Summary

"Innovation for the customers, innovation for the grid" is the vision of project Platone - Platform for Operation of distribution Networks. Within the H2020 programme "A single, smart European electricity grid", Platone addresses the topic "Flexibility and retail market options for the distribution grid". Modern power grids are moving away from centralised, infrastructure-heavy transmission system operators (TSOs) towards distribution system operators (DSOs) that are flexible and more capable of managing diverse renewable energy sources. DSOs require new ways of managing the increased number of producers, end users and more volatile power distribution systems of the future. Platone is using blockchain technology to build the Platone Open Framework to meet the needs of modern DSO power systems, including data management. The Platone Open Framework aims to create an open, flexible and secure system that enables distribution grid flexibility/congestion management mechanisms, through innovative energy market models involving all the possible actors at many levels (DSOs, TSOs, customers, aggregators). It is an open source framework based on blockchain technology that enables a secure and shared data management system, allows standard and flexible integration of external solutions (e.g. legacy solutions), and is open to integration of external services through standardized open application program interfaces (APIs). It is built with existing regulations in mind and will allow small power producers to be easily certified so that they can sell excess energy back to the grid. The Platone Open Framework will also incorporate an open-market system to link with traditional TSOs. The Platone Open Framework will be tested in three European field trials and within the Canadian Distributed Energy Management Initiative (DEMI).

The Platone platform solution consists of a layered architecture named Platone Open Framework. This deliverable focuses on the selected communication protocols and data models for integrating the different platform components within the framework and with external systems. Relevant data models are initially based on the IEC 61850 and the CIM-61968-9 standards and will be extended throughout the project based on the outcomes of the field trial executions. The underlying communication protocols for intra-platform communication are MQTT and Kafka for asynchronous communication and RESTful APIs for synchronous communication. For communication between different components of the framework, both kinds of the communication channels are secured with underlying transport layer security (TLS). Furthermore, several design principles are depicted with respect to security and privacy aspects. Therefore, two components of the framework - the shared customer database and the DSO data server - are presented in more detail as they are designed to separate DSO internal systems from the framework.

This document forms the first (v1) of two reports on the intra-platform communication within the Platone Open Framework. It will be extended based on the next releases of the individual components and the progressing integrations and validations in the context of the Platone trial sites. These outcomes will be reported in D2.10 (v2).

Authors and Reviewers

Main responsible		
Partner	**Name**	**E-mail**
RWTH		
	Jonas Baude	
Author(s)/contributor(s)		
Partner	**Name**	
ENG		
	Ferdinando Bosco	ferdinando.bosco@eng.it
RWTH		
	Jonas Baude	jonas.baude@eonerc.rwth-aachen.de
Reviewer(s)		
Partner	**Name**	
NTUA		
	Panagiotis Pediaditis	
AVAC		
	Navreet Dult Benjamin Petters	
Approver(s)		
Partner	**Name**	
RWTH		
	Padraic McKeever	

Table of Contents

1 Introduction

The project "PLATform for Operation of distribution Networks – Platone" aims to develop an architecture for testing and implementing a data acquisition system based on a two-layer Blockchain approach: an "Access Layer" to connect customers to the Distribution System Operator (DSO) and a "Service Layer" to link customers and DSO to the Flexibility Market environment (Market Place, Aggregators, …). The two layers are linked by a Shared Customer Database, containing all the data certified by Blockchain and made available to all the relevant stakeholders of the two layers. This Platone Open Framework architecture allows a greater stakeholder involvement and enables an efficient and smart network management. The tools used for this purpose will be based on platforms able to receive data from different sources, such as weather forecasting systems or distributed smart devices spread all over the urban area. These platforms, by talking to each other and exchanging data, will allow collecting and elaborating information useful for DSOs, transmission system operators (TSOs), Market, customers and aggregators. In particular, the DSOs will invest in a standard, open, non-discriminatory, blockchain-based, economic dispute settlement infrastructure, to give to both the customers and to the aggregator the possibility to more easily become flexibility market players. This solution will allow the DSO to acquire a new role as a market enabler for end users and a smarter observer of the distribution network. By defining this innovative two-layer architecture, Platone strongly contributes to remove technical and economic barriers to the achievement of a carbon-free society by 2050 [1], creating the ecosystem for new market mechanisms for a rapid roll out among DSOs and for a large involvement of customers in the active management of grids and in the flexibility markets. The Platone platform will be tested in three European trials (Greece, Germany and Italy) and within the Distributed Energy Management Initiative (DEMI) in Canada. The Platone consortium aims to go for a commercial exploitation of the results after the project is finished. Within the H2020 programme "A single, smart European electricity grid" Platone addresses the topic "Flexibility and retail market options for the distribution grid".

The Platone platform solution consists of a layered architecture named Platone Open Framework. It mainly consists of the Blockchain Access Layer, handling data certification and flexibility activation based on smart contracts, the Platone Market Platform allowing for flexibility requests from TSOs and DSOs in a large geographical area and the Platone DSO Technical Platform that provides DSOs with a reference way to deploy auxiliary grid services. The reference architecture of the Open Framework is provided in Deliverable D2.1 [2].

In order to make all these components work smoothly together, the interoperability and security between the different platform components needs to be aligned. This deliverable focuses on the current design principles of the different platform components with respect to data models, communication protocols and security aspects.

1.1 Task 2.4

Task 2.4 covers the intra-platform interoperability and standard communication protocols of the Platone Open Framework. This first version of this document focuses on the intra-platform communication between the three core components of the Platone Open Framework.

1.2 Objectives of the Work Reported in this Deliverable

This first version of the deliverable provides the intra-platform communication between the three core components of the Platone Open Framework (Blockchain Access Layer, DSO Technical Platform, and Market Platform) and further external systems. An updated version of this deliverable will be made in M48.

The main goal of this report is to provide an overview of the intra-platform communication in the Platone Open Framework from different points of view, in order to allow all stakeholders involved to understand the characteristics and consider possible integrations. It also presents how security and privacy aspects are addressed in the intermediate implementations of the platform components.

1.3 Outline of the Deliverable

Chapter 2 presents the relevant data formats and standards that are relevant for the first deployment phase of the Platone Open Framework in the field trials and also addresses the internal representation of the data within the platforms.

Chapter 3 presents the components of the Platone Open Framework and the respective communication protocols. It also includes a section about the integration with external systems.

Chapter 4 addresses security aspects that were considered during the design of the platform components and during the deployment in the field trials.

Chapter 5 focuses on the privacy consideration of data within the different platform components and how they are addressed.

Finally, Chapter 6 discusses conclusions of the deliverable.

1.4 How to Read this Document

This document reports the intra-platform interoperability and standard communication protocols of the Platone Open Framework with a strict focus on Platone Platforms implemented within WP2. Other external systems, implemented within other WPs (WP3, WP4 and WP5) are briefly described. A greater level of detail will be included in the deliverables of the respective WPs. Use cases and scenarios, used for defining the functional and non-functional requirements, are available in D1.1 [3] , D4.1 [4] and D5.2 [5]. A more coherent overview of the Platone Open Framework is provided in the deliverable on Platform requirements and reference architecture, D2.1 [2], and in the deliverables of the reference implementations of the platform components in the field trials, D2.3 [6], D2.6 [7], D2.11 [8] and in the Deliverable on the Framework integration D2.14 [9].

2 Data Interoperability

This section provides an overview of different data formats that are used in the Platone field trials and need to be integrated into the different Platforms of the Platone Open Framework. The first subsection presents relevant standardized or proprietary data formats the Platone Open Framework receives from devices or external systems. The second subsection presents relevant ontologies that are considered for semantic representation of data within the Platone framework.

2.1 Data Formats relevant for the field trials

This subsection presents data formats and related standards that are used in the first release and integration phase of the Platone Open Framework in the field trials.

2.1.1 CIM-61968-9 meter readings

The two common IEC 61968 and IEC 61970 series of standards are both based on the Common Information Model (CIM). The CIM standard family is relevant in the field of system interfaces and data models for network management. Furthermore, it plays an important role for the integration of applications into the ICT system landscape of system operators [10].

CIM aims at minimizing both efforts and costs for the integration of applications in and with energy management systems (EMS). Furthermore, it protects investment into systems by providing standardization and ensuring effective operation thereof. In this context, the CIM is to be understood as an integration framework that enables seamless integration on the vertical value chain by defining and standardizing both different interfaces but a single data model for EMS and for distribution network management systems (DMS).


```xml
<mr:MeterReadings xmlns:mr="http://iec.ch/TC57/2011/MeterReadings#">
   <mr:MeterReading>
      <mr:Meter>
         <mr:Names>
            <mr:name>11111111</mr:name>
            <mr:NameType>
               <mr:name>EndpointID 110</mr:name>
               <mr:NameTypeAuthority>
                  <mr:name>NAME</mr:name>
               </mr:NameTypeAuthority>
            </mr:NameType>
         </mr:Names>
      </mr:Meter>
      <mr:Readings>
         <mr:timeStamp>2019-09-13T15:30:00+03:00</mr:timeStamp>
         <mr:value>11.04</mr:value>
         <mr:ReadingType ref="0.26.0.0.1.1.12.0.0.0.0.0.0.0.0.224.3.72.0"/>
      </mr:Readings>
      <mr:Readings>
         <mr:timeStamp>2019-09-13T15:30:00+03:00</mr:timeStamp>
         <mr:value>3.45</mr:value>
         <mr:ReadingType ref="0.26.0.0.1.1.12.0.0.0.0.0.0.0.0.224.3.73.0"/>
      </mr:Readings>
      <mr:UsagePoint>
         <mr:mRID>111111</mr:mRID>
      </mr:UsagePoint>
   </mr:MeterReading>
</mr:MeterReadings>
```


Figure 1 Meter Readings Data Model

The IEC 61968 distribution management standard is the first part in a series of standards that define interfaces for the major elements of an interface architecture for Distribution Management Systems. It identifies and establishes requirements for standard interfaces based on an Interface reference model. It defines function blocks and XML-based messages and associated use cases. In particular, Part 9 of

IEC 61968-9 [11] focuses on interfaces for meter reading and control. Besides its intended use in electrical distribution grids, it can also be applied to non-electrical metering applications, e.g. gas or water metering. Its core purpose is to standardize the integration of metering systems and meter data management systems with further operator systems or business functions. Therefore, IEC 61968-9 defines the standard models required data formats that are expected to cover the capabilities of common metering infrastructure as well as advanced features such as dynamic pricing, or DER signalling. It is noteworthy that the standard does not define specific communication protocols over which these data are exchanged.

Figure 1 shows an example of IEC 61968-9 CIM meter readings data in XML format as they are used in work package (WP) 4 to transfer aggregated metering data sets from automated meter reading systems into the Blockchain Access Layer of the Platone Open Framework.

2.1.2 IEC 61850

Initially, the international standard IEC 61850 was defined with protection and substation automation in mind. But today, it also plays an important role outside substation context for information exchange in electrical power supply with decentralized generation.

Substations are important nodes in these networks. In these, the load flow is controlled and monitored and network control points can access the power network. In addition, the majority of the existing protective devices for the safe operation of the power grid are installed there. In view of these functions, it is hardly surprising that distributed systems for the automation of substations generate and distribute a wide range of information and data volumes (measured values and status information, switching commands and parameters). The information model and the exchange of information are the necessary basis for distributed control technology with a large number of intelligent devices.

In contrast to IEC 61968-9, the IEC 61850 defines a communication layer and data models for various use cases. However, the data model layer is clearly separated from the communication layers into separate parts of the standard, allowing for simplified and independent extension of the data models or adoption of new communication technologies.

The main objective of the IEC 61850 series of standards is communication interoperability of instrumentation and control equipment. That means the possibility that two or more intelligent electronic devices, either from a single source or several manufacturers, can implement the IEC 61850 series of standards and can interpret and use this available information unambiguously, in order to implement the functionality required by the application.

In the scope of the Platone Open Framework, the standard is of special interest due to the integration of data from field devices such as Phasor Measurement Units (PMUs) into the platform. The separation between communication layer and data modelling of the standard allows for a good separation of the data from the underlying transport mechanisms and hence the propagation of data into the platform.

2.1.3 Proprietary Data Models

In the first iteration of releases and field trial integrations, the Platone Open Framework is not entirely based on standardized data models. In such cases, data is currently exchanged in proprietary data formats. For instance, the Low-Cost Phasor Measurement Unit (LOCO PMU) is capable of communicating via IEC 61850 if integrated into substation automation systems. However, in the Platone use cases it is integrated into the Platone Blockchain Access Layer by means of MQTT as an IoT Sensor network, sending data in a proprietary data format, an example of which is shown in Figure 2.

```
{
    "device": "pmu1",
    "timestamp": "2020-05-20T10:27:57.980802+00:00",
    "readings": [
        {
            "component": "BUS1",
            "measurand": "voltmagnitude",
            "phase": "A",
            "data": 11
        },
        {
            "component": "BUS2",
            "measurand": "voltmagnitude",
            "phase": "A",
            "data": 22
        }
    ]
}
```


Figure 2 Example for PMU Reading Data Model

2.2 Internal Data Representation in the Platone Open Framework

2.2.1 SAREF and SAREF4ENER

The SAREF (Smart Appliance REFerence) ontology [12] was initially created to address the issue of fragmentation and the need for interoperability in the smart appliances and Internet of Things (IoT) industry. It was mainly targeting energy efficiency use cases based on smart appliances integrated into local energy management systems.

SAREF can be considered an interoperability enabler as it gives a common language for devices while not defining particular communication protocols. Instead, it targets to provide a common data model for mapping information coming from various existing protocols. This reduces the number of required mappings to one mapping with SAREF per data model, instead of one mapping with each other data model per data model.

SAREF was designed to be extensible and several main extensions have been released up to now, including SAREF4ENER for energy domain, SAREF4BLDG for Smart Buildings, SAREF4ENVI for environment. In total there are ten extensions including Smart Cities, Agriculture and Industries.

SAREF focuses on the concept of device, defined as “a tangible object designed to accomplish a particular task in households, common public buildings or offices. In order to accomplish this task, the device performs one or more functions” [12]. The role of SAREF is then to provide a standard way to describe devices and their characteristics.

The SAREF ontology is written in Web Ontology Language (OWL) [13], and its instantiations use the Turtle syntax [14]. An application example would be describing different devices managed in a home gateway. Examples of instantiations and use cases can be found in ETSI TR 403 111 [15].

SAREF4ENER is an extension of SAREF targeting the interoperability among a variety of proprietary solutions in the smart home domain. The SAREF4ENER standard was created by an ETSI collaboration with the industry associations Energy@Home and EEBus to align their data models in order to facilitate the interoperability among various proprietary solutions developed by different consortia in the smart home domain. By using SAREF4ENER, smart appliances from manufacturers that support either of the aforementioned data models can easily communicate with one another. The UCs that have been considered in the development of SAREF4ENER are mainly about the demand response scenarios, in which the flexibility of the smart grid in the management of the smart home devices is focused on customer energy manager.

2.2.2 SARGON

SARGON, the SmArt eneRGy dOmain oNtology, is another extension of SAREF that cross-cuts domain-specific information representing the smart energy domain and includes building and electrical grid automation together [16]. Therefore, SARGON is based on CIM and the IEC 61850 data models to derive basic components and data models in accordance with the standard. The five following use cases have been considered in the design phase of SARGON.

1. *Automation of medium voltage distribution grids:* As described previously, IEC 61850 provides a commonly adopted reference for automation of distribution grids. The first version of SARGON reformulates a subset of the data structures related to AC/DC hybrid grids according to an ontology description.
2. *PMU interaction and data visualisation:* Similar to the Platone use cases, SARGON demonstrates the integration of a PMU data format for data visualization by defining the PMU as a subtype of a metering device in the ontology.
3. *Building automation and monitoring*: This use case addresses the optimization of energy demand in buildings and is not considered relevant in the context of Platone.
4. *Energy management with residential/non-residential involvement:* This use cases covers modern building energy systems, especially in residential/non-residential buildings, and is not considered relevant in the context of Platone.
5. *Energy management in building/districts level:* This use case considers the control functionalities as well as the data models (e.g. for measurements) that are relevant for the interaction between the energy management of buildings or districts and their electrical automation.

Several of the SARGON extensions to SAREF are considered relevant for the further development of the Platone Open Framework. In particular, the efforts on the extensions to SAREF for integration devices such as PMUs and converters, the consideration of CIM and IEC 61850 data models and additional ontologies for services in smart grids such as controlling, monitoring and protection. This allows to reduce the number of internal proprietary data formats. Hence, it is foreseen to evaluate SARGON on a subset of data models during the second development phase of the Platone Open Framework. While extensions of SARGON with entire data models from other standards would be out of scope for Platone, the tests in Platone Framework can still support the evolution of SARGON and potential extension would be contributed upstream. The results will be reported in the second version of this report D2.10, expect at the end of the project.

3 Platone Open Framework Design Overview

Platone Open Framework is an open source and modular framework based on blockchain technology that enables a secure and shared data management system, allows standard and flexible integration of external solutions (e.g., legacy solutions), and is open to integration of external services through standardized open application program interfaces (APIs) [2].

The framework's main characteristics rely heavily on the concepts of interoperability, adaptability, and flexibility and for these reasons it includes by design several interoperable and standardised mechanisms for the integration.

More in detail the framework consists of three main components, each of these can be used individually, or integrated with the others.

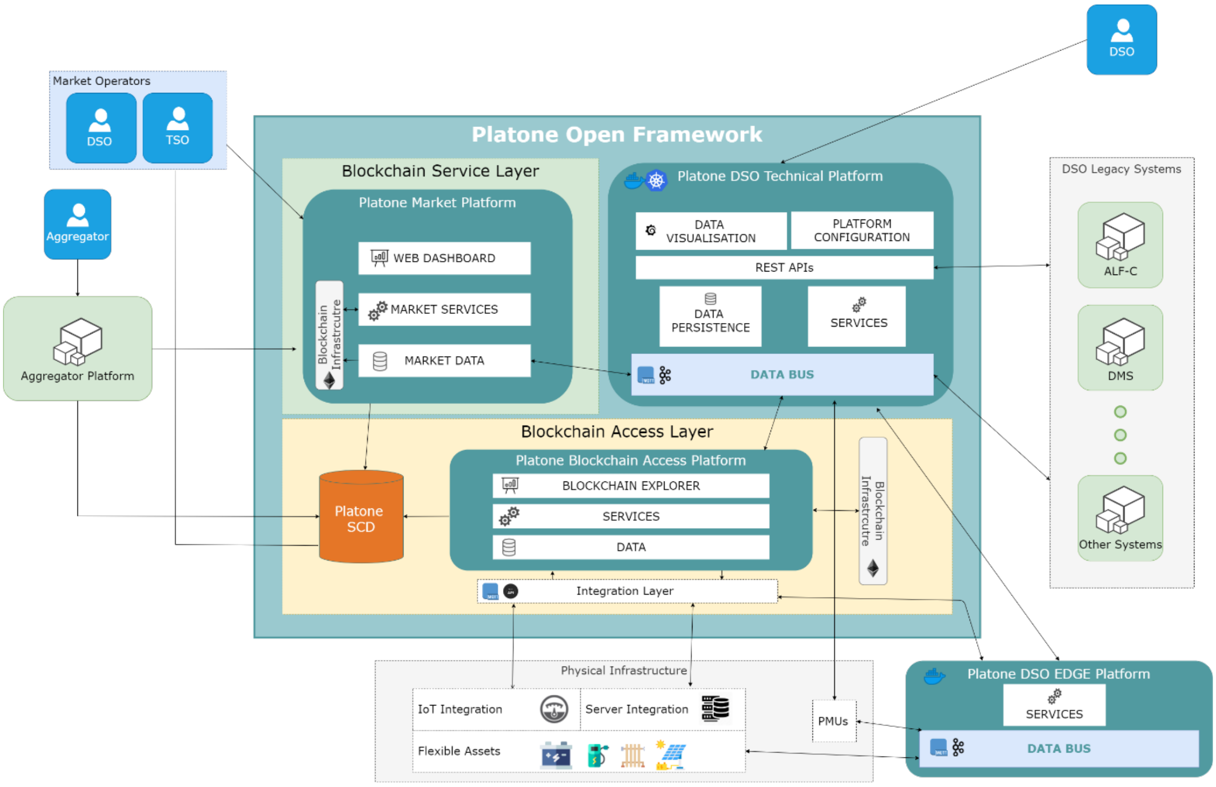

Figure 3 Platone Open Framework

Platone Market Platform, which allows the support of wide geographical area flexibility requests from TSOs and local flexibility requests from DSOs. These are matched with offers coming from aggregators, resolving conflicts according to pre-defined rules of dispatching priorities. All the market operations are registered and certified within the blockchain service layer, ensuring a transparency, security and trustworthiness among all the market participants.

Blockchain Access Layer, which adds a further level of security and trustworthiness to the framework. It is an extension of the physical infrastructure and performs multiple tasks, among which are data certification and automated flexibility execution through Smart Contracts. It includes the Blockchain Access Platform and the Shared Customer Database.

Platone DSO Technical Platform, which allows DSOs to manage the distribution grid in a secure, efficient, and stable manner. It is based on an open-source extensible microservices platform and allows to deploy, as Docker containers, specific services for the DSOs and execute them on Kubernetes. The Data Bus layer, included on the DSO Technical Platform, allows integration both of other components of the Platone framework and of external components (e.g. DSO Management System) with a direct connection to the classical supervisory control and data acquisition (SCADA) system adopted by the DSO and served by standard communication protocols.

In the next chapters, a more detailed description on the interoperability and standardisation of the different components is provided.

3.1 Blockchain Access Layer

Platone Blockchain Access Layer (BAL) is the component in charge of enabling a standard, secure, and easy integration of energy data coming from the physical infrastructure and grant the access to this data to DSOs and other energy stakeholders [8].

More in detail, it implements a data integration interface for collecting energy measurements coming from smart meters (IoT devices), data servers (e.g., DSO Data Server in the Greek field trial) and PMUs (Phasor Measurement Unit), supporting standardised data models (at the moment the CIM IEC 61968-9) and certifying this data thanks to blockchain technology and smart contracts, **ensuring data integrity, and avoiding data tampering**.

The energy data collected, harmonized, and certified are available for all the energy stakeholders involved as well as external platforms and services (e.g. the Platone DSO Technical Platform), who need to use this data, within the Platone Shared Customer Database.

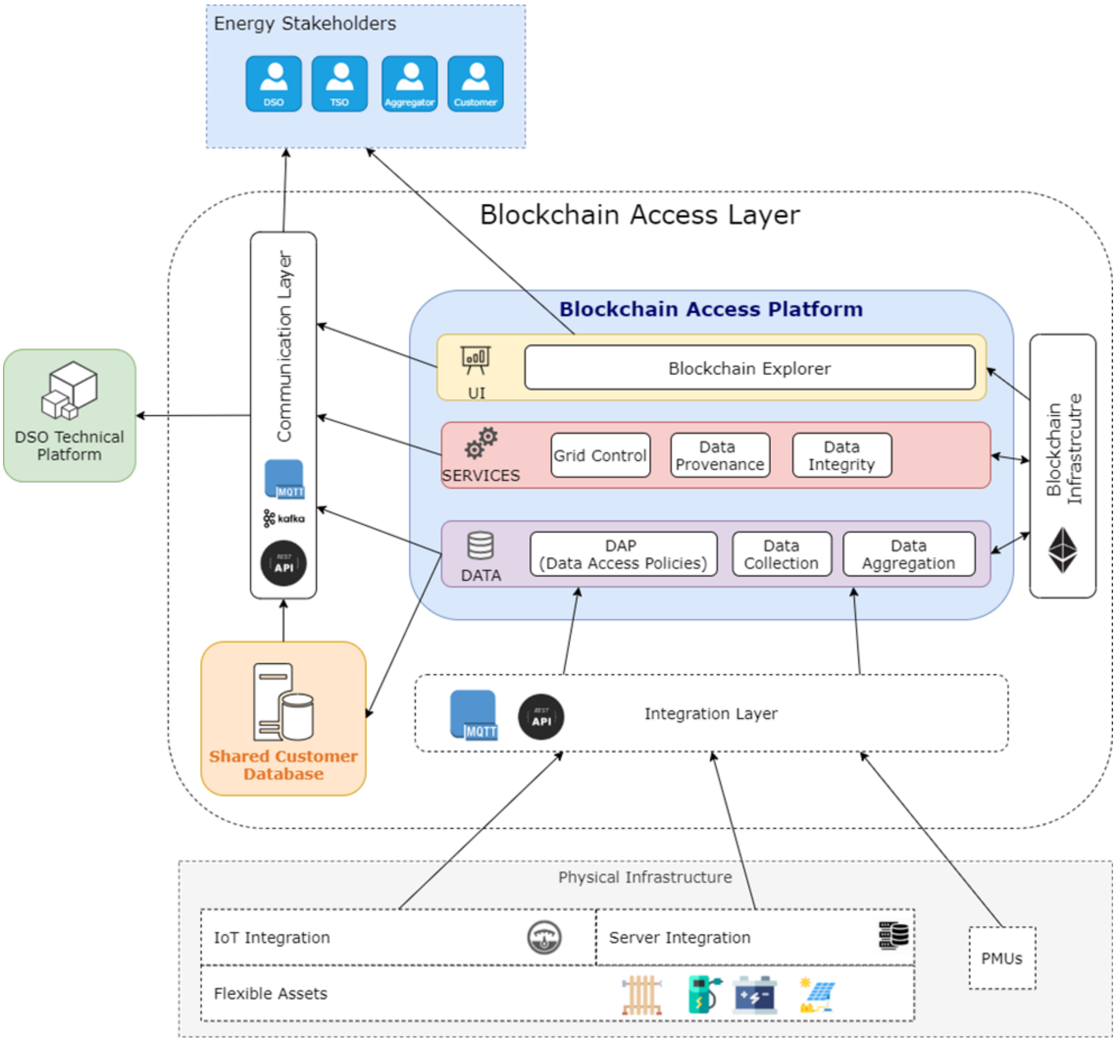

Figure 4: Blockchain Access Layer Architecture

BAL is probably the core component focussed on data interoperability, since it is the main responsible for collecting and integrating data from smart devices and external data sources and managing these data in a secure manner, as well as providing access to possible external actors.

The SCD that is responsible for storing and providing the data externally, but there are two important layers that provide the necessary interoperability services and standard protocols: the **Integration**

Layer for the data collection and integration and the **Communication Layer** for the data provisioning and the integration of external users and/or platforms.

The integration layer implements the Message Queue Telemetry Transport (MQTT) [24], an OASIS standard messaging protocol for integrating Internet of Things (IoT) devices ensuring high performance, minimal network bandwidth and small code footprint.

The first version of BAL uses the Mosquitto MQTT Message broker [25]. The MQTT broker can receive messages from different sources using a tunnel-encrypted channel which supports both certificates and authentication mode, in this way it guarantees the security and ownership of the data.

In the next version of the BAL, expected for M38, October 2022, the integration layer will be extended with other communication mechanisms and protocols (e.g. REST APIs).

The Communication Layer provides two different communication mechanisms: synchronous and asynchronous.

This architectural component dedicated to communication mechanisms, provides a greater flexibility to the BAL, which can cover different solution and integrate different external systems and users.

More in detail, the synchronous communication is implemented in the API Gateway via REST APIs. The API gateway is the entry point for every HTTP request that is being launched by the external systems.

The API gateway is developed using open-source framework Express.js [26].

The asynchronous communication is implemented in the Message Broker. It acts as a middleware for various services (e.g., different external systems). They can be used to reduce loads and delivery times by web application servers since tasks, which would normally take quite a bit of time to process, can be delegated to a third party whose only job is to perform them.

The first version of the BAL provides two different brokers: Mosquitto MQTT broker for providing high performance data streams and Apache Kafka [27], better suited for integrating external services.

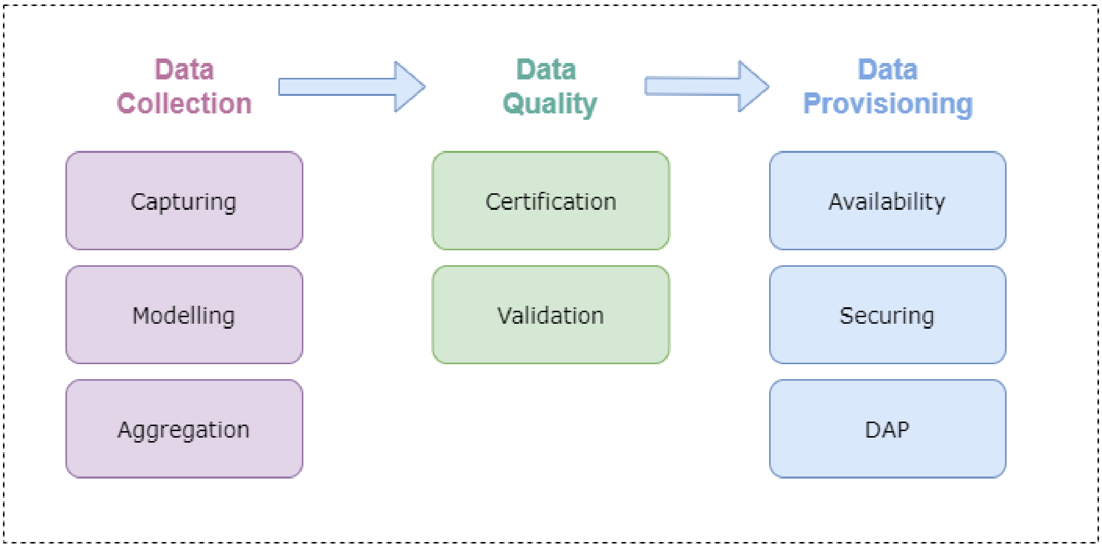

Figure 5 BAL Data Management Process

In the data collection phase, the data is captured in a secure way, using certification mechanisms and MQTT under TLS [28], also ensuring the data ownership and the data privacy. Then the data are linked to a standardised data model, aggregated and/or harmonised if necessary and finally stored in the SCD.

In the data quality phase, the blockchain technology performs the validation and the certification of all the data stored in the SCD using Smart Contracts [29] and hashing functions.

The data provisioning phase includes the availability of the data to external stakeholders, implementing specific data access policies and secure authorization/authentication mechanisms, exploiting the multiple possibilities offered by BAL for the integration of users and external platforms (REST APIs, MQTT and Apache Kafka, using certificates and underlying TLS connections).

3.2 Market Platform

The Platone Market Platform is one of the core components of the Platone Open Framework. It is a blockchain-based platform that enables the management of the flexibility market, involving any possible stakeholders (TSOs, DSOs, Aggregators, Customers) [6].

All the market operations are registered and certified within the blockchain service layer, ensuring a higher level of transparency, security and trustworthiness among all the market players.

Furthermore, the Platone Market Platform enables an innovative incentivisation mechanism for customer engagement based on blockchain technology, smart contracts, and tokenisation.

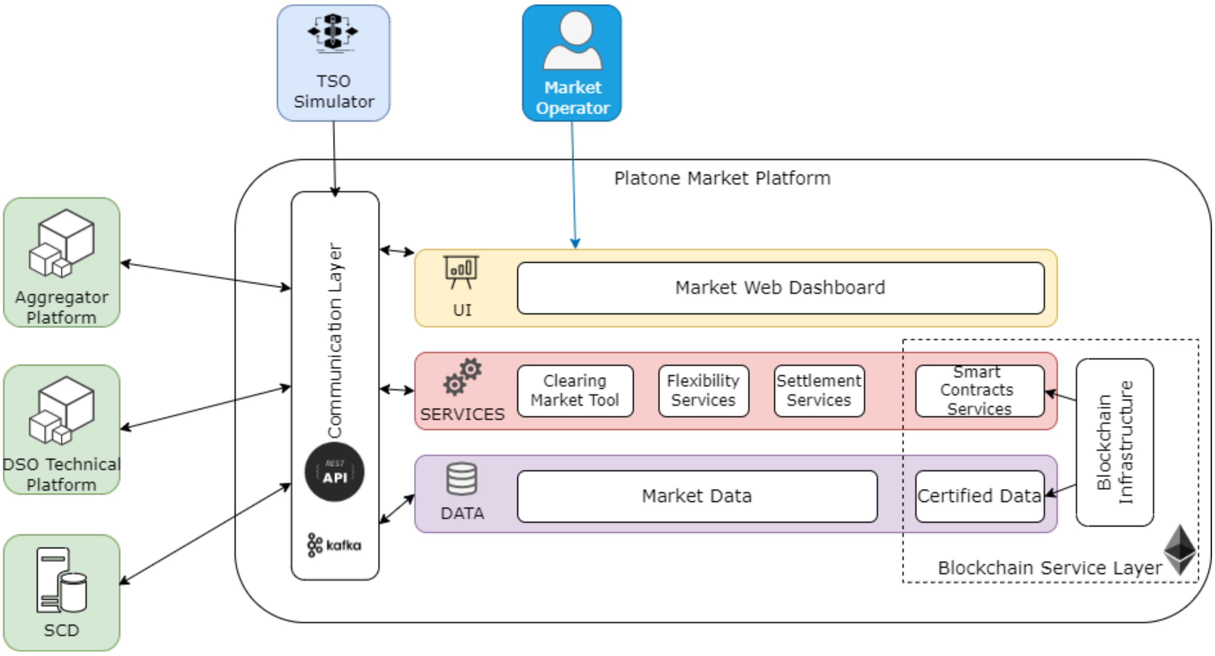

Figure 6: Market Platform Architecture

From the interoperability and standardisation point of view, the Market Platform implements in its Communication Layer an API Gateway (based on Express.js) and a Message Broker (based on Apache Kafka) for the integration of external services and platforms.

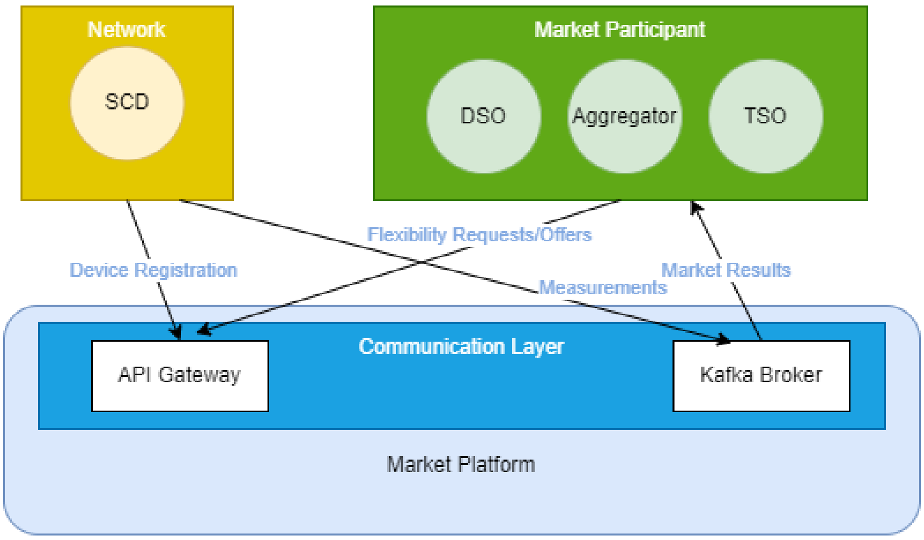

Figure 7: Market Platform Communication mechanisms

More in detail, the Market Platform uses (see Figure 7):

- the API Gateway:

  - For collecting flexibility offers and requests coming from DSOs, TSOs and Aggregators defining a specific data model that allows matching flexibilities with high granularity.
  - For receiving the information about the network grid and in particular the devices' information, via the SCD.
- the Message Broker:
  - For providing the results of the Market to all the Market Participants using a publish/subscribe mechanism.
  - For periodically collecting the measurements and performing the settlement and the validation.

From a security point of view, all the REST APIs exposed on the API Gateway are protected under TLS connection and Oauth2.0 authentication, while for the Apache Kafka subscriptions each external platform must authenticate itself using Two-Way authentication mechanism, SSL keys and certificates [30].

3.3 DSO Technical Platform

The DSO Technical Platform is a component of the Platone Open Framework designed to allow DSOs to manage the distribution grid in a secure, efficient and stable manner. It is based on an open-source extensible microservices platform and allows to deploy, as Docker containers, specific services for the DSOs and execute them on Kubernetes. The Data Bus layer, included on the DSO Technical Platform, allows integration both of other components of the Platone framework and of external components (e.g. DSO Management System) with a direct connection to the classical supervisory control and data acquisition (SCADA) system adopted by the DSO and served by standard communication protocols. The platform design builds on previous work done in the Horizon 2020 project *SOGNO* [31] and relies massively on a micro-service architecture.

The presented platform architecture aims at facilitating the transition to modular, micro-services based control centre software solution for distribution system operators. This allows for faster adjustment and independent development of components. The goal is to provide system operators and automation software developers with an open source framework that exposes open APIs to plug in new automation functions and supports industry standards such as CIM IEC61970 and IEC61850.

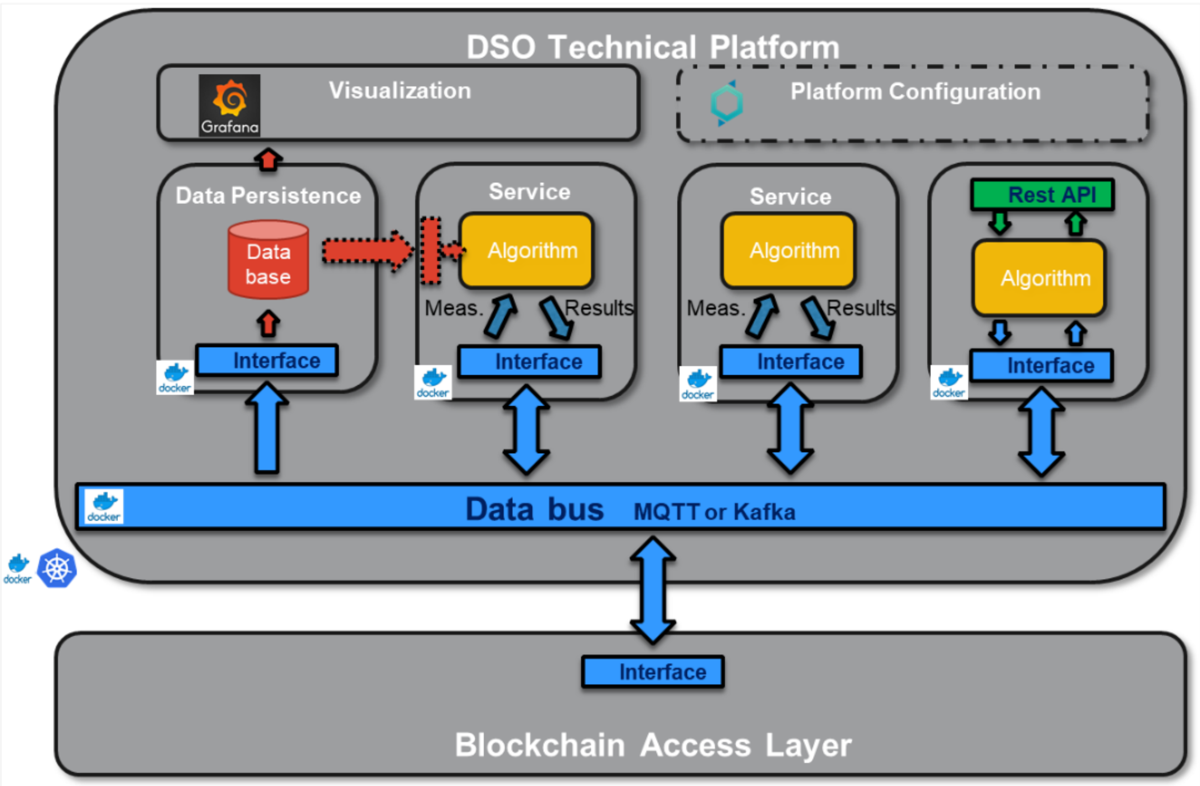

Figure 8 Platone DSO Technical Platform Architecture

To address requirements such as high availability, scalability and modularity from the very beginning, the DSO Technical Platform is designed for deployment on kubernetes [32] clusters. Kubernetes, also known as K8s, is an open-source system for automation deployment, scaling and management of containerized applications. As all micro-services of the platform are per requirement containerized in Docker [33] containers, they can easily be deployed on a kubernetes cluster. Kubernetes also simplifies different deployment approaches: from edge- and public-cloud to on-premises installation. However, the on-premises installation is considered the most relevant for a control centre platform. In order to minimize initial hurdles, Platone provides detailed installation manuals for a local installation based on the lightweight kubernetes distribution k3s [34].

Figure 8 illustrates the architecture of the DSO Technical Platform. The databus is one of its core components and is implemented by means of a message broker to which all services can publish and / or subscribe in order to exchange data with other services, with field devices, or with external systems. Field devices or external systems can be made available in the data bus either directly or through the Platone Blockchain Access Layer [8].

3.4 External Systems

Besides the integration of the core platform components of the Platone Open Framework (cf. D2.14 [9]) the framework also allows the integration of external systems. This section depicts examples of the ALF-C and the DSO data server integrations from the WP4 and WP5 field trials.

3.4.1 Avacon Local Flex Controller (ALF-C)

The ALF-C is the main component developed, implemented and tested in the German field trial of WP5. The platform is integrated into the Platone framework and acts as an own SCADA/ADMS of the local low voltage (LV) grid. The controller optimizes the synchronization of consumption and generation inside the field test LV grid and provides flexibility on external request such as from the Market Platforms or directly from the DSO or TSO in frame of mechanisms that maintain safe and reliable operation of the distribution grid. The following section gives a detailed description of ALF-C functions.

The ALF-C implementation is based on Microsoft Azure Functions and Function Apps. It integrates some of the assets of the field trial such as the large-scaled battery energy storage system and domestic storages, operated by households in combination with a roof top photovoltaic system. In addition, it is combined with the Platone Open Framework to integrate the PMU at substation level via the Blockchain Access Layer and to utilize an external optimization algorithm that is provided as a service by the DSO technical platform.

In order to integrate an optimization service which is not part of its core business logic, the ALF-C uses REST API calls to the service running within the DSO Technical platform. PMU data coming from the PMU devices will be integrated and certified into the Platone BAL and provided to the Platone DSOTP to be used for data visualisation.

3.4.2 DSO Data Server

The DSO Data Server is a database that contains DSO data in the Greek Demo environment, i.e. master data and automated meter reading (AMR) metrics for MV and LV customers. It is designed as, i.e. master data and automated meter reading (AMR) metrics for MV and LV customers. It is designed as a containerized application that unifies data from different telemetering centres offline into a uniform internal database. A dedicated API allows querying the database and gather reading data occasionally or periodically. The data is then published via MQTT, e.g. scheduled every 15 minutes. The API side of the DSO Data Server also transforms the data into an xml file which a data model, format, and structure according to the CIM 61968-9 standard for meter reading and control [11].

As shown in Figure 9, in this first integration within the Greek field trial architecture, metering data coming from the DSO Data server will be integrated and certified into the Platone BAL and provided to the Platone DSOTP to be used for data visualisation and by State Estimation Tool developed within WP4. The MQTT Broker of the BAL receives metering data from DSO Data Server, every 15 minutes, in CIM standard model, in authenticated way and under TLS connection; The BAL stores data into SCD and certify aggregated data into BAP and adds a certification hash to the data prior to storing it in the SCD. In parallel, the BAL provides the metering data to DSOTP via MQTT on a dedicated topic which is forwarded into the internal databus of the DSOTP. Within DSOTP, Metering data is stored in a timeseries database and visualized in customizable dashboards and is available to all services running on the DSO Technical Platform, e.g. the state estimation service that is of special interest in the WP4 field trial.

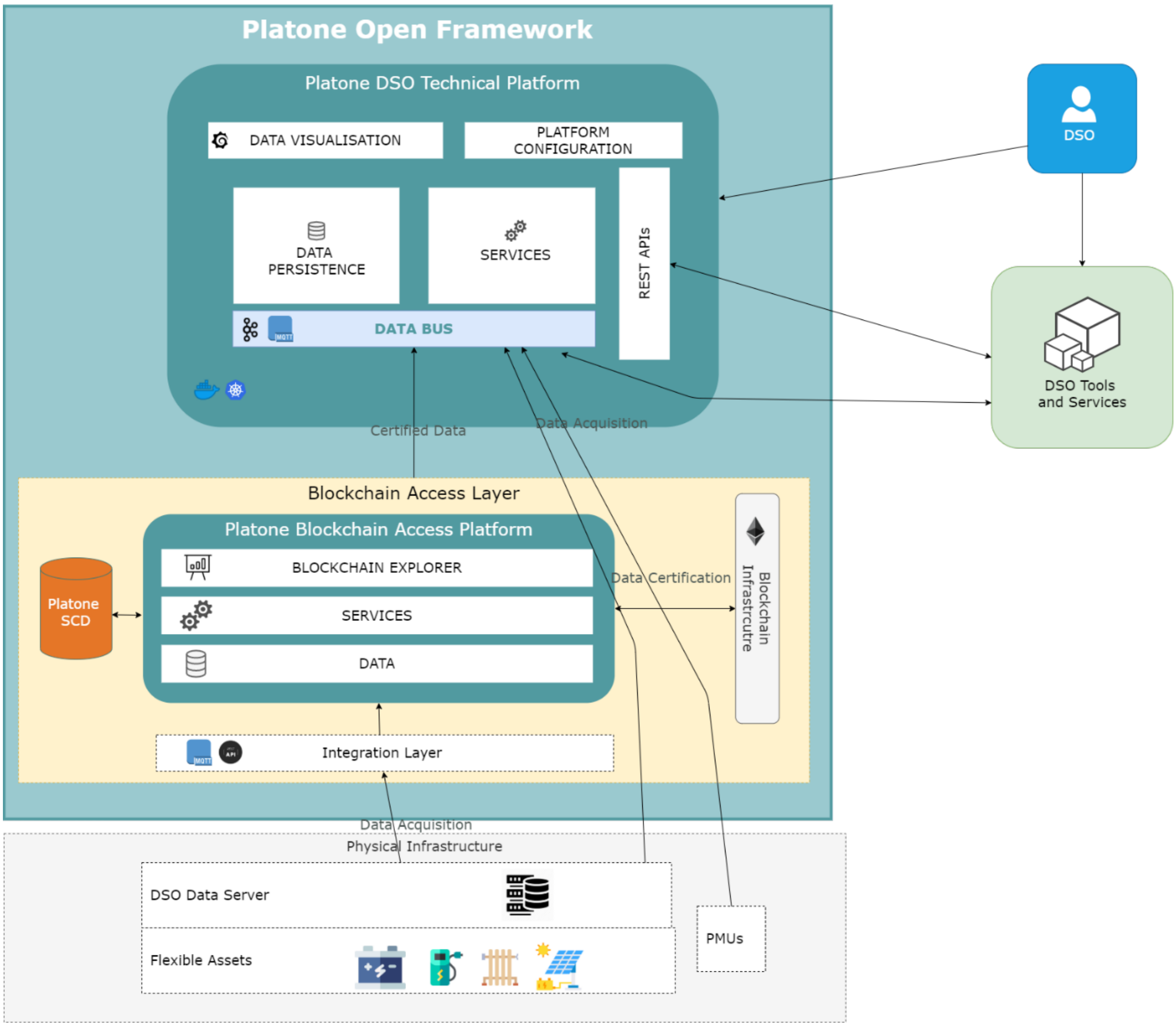

Figure 9: Greek Demo Implementation of the Platone Open Framework

4 Secure Intra-Platform Communication

This section provides on overview of security design principles and best practices that were considered in the first release cycle and integration phase of the Platone Open Framework. Additionally, an outlook to foreseen extension for the next release phase is provided.

4.1 Design Principles

For communication within the Platone Open Framework we distinguish between synchronous communication interfaces and asynchronous communications interfaces. Synchronous communication is used for instance for configuring services running on one of the platforms or for querying specific data sets and is implemented by means of REST APIs. Asynchronous communication is for instance used for event-based or streaming-data mechanisms and implemented by means of a message broker. In the first release of the Framework, MQTT and Apache Kafka are used as internal message brokers in the different Platone platforms.

Intra-Platform Communication within the Platone Open Framework is also based on these three different communications mechanisms. However, special security considerations are necessary because the three platforms are not necessarily operated within the same internal network but may, for example, be partially hosted on-premises and integrated with other parts that are hosted on public cloud infrastructure. Hence, all these interfaces are secured by TLS on the underlying transport protocol together with user authentication. Table 1 depicts all internal and external communication protocols.

Table 1 Communication Protocol Matrix

Platform	**Internal**	**External**	**Authentication Mechanism**	**Foreseen for next release**
Blockchain Access Layer	MQTT Kafka	MQTTS Kafka TLS	Basic Authentication	HTTPS
DSO Technical Platform	MQTT HTTP	MQTTS HTTPS	OAuth2, Basic Authentication	Kafka, Client-Cert. Authentication
Platone Market Platform	Kafka HTTP	Kafka TLS HTTPS	Oauth2, Client-Cert. Authentication	-

While the message broker or event bus implementations are based on well-established open-source implementations such as RabbitMQ or Apache Kafka, they usually bring native support for TLS and sufficient authentication mechanisms. In contrast, the REST API interfaces are custom implementations e.g. for platform components or services. To achieve the same level of security without replicating the effort for each service, the TLS support and the authentications mechanisms are offloaded to an API gateway component. That serves as entry point for external REST API requests via HTTPS and handles the TLS termination and the authentication of the request. Within the respective platform, successfully authenticated requests are then forwarded to the responsible services via plain HTTP as illustrated in Figure 10.

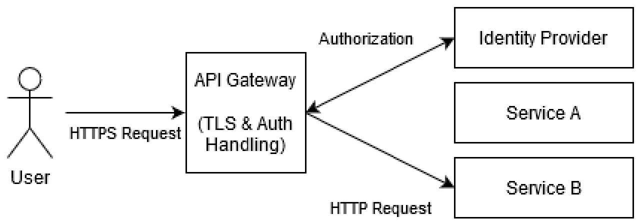

Figure 10 TLS offload and Authentication in API Gateway

4.2 Best-practices from Field Trials

Besides the security design principles that were discussed in the previous section, the integration and deployment phase of the Platone Open Framework in the different field trial sites provided additional insight into security best-practices. Furthermore, the Greek and German field trials allow for a verification of different deployment scenarios. In the context of the Greek field trial, the Blockchain Access Layer and the DSO Technical Platform are deployed entirely on-premises whereas in the German field trial context, the BAL and the DSOTP are deployed on a public cloud infrastructure.

Besides verification of the different deployment scenarios, the field trial deployments revealed additional security requirements coming from the participating DSOs' ICT departments. For instance, the deployment of the DSO Technical Platform on a Kubernetes Cluster managed by the operator required higher security configurations than anticipated. These findings will be integrated into the code base for the next release cycle and reported in the related Deliverables.

4.3 Outlook for next Release Phases

As this report is based on the first release cycle of the Platone Open Framework, additional security features are foreseen for the next releases. These include a more unified approach to Identity Management (IDM) and Access control between the different Platforms. In addition, the Client-Certificate Authentication Mechanism as already implemented in the Market Platform is considered for additional security, e.g. on field devices such as the PMU.

5 Privacy Considerations within the Platone Open Framework

This section presents how privacy considerations are addressed in the design of the Platone Open Framework, in particular how two components of the Platone Open Framework are designed to communicate with DSO internal systems or external devices.

Demand Side Flexibility is strongly dependent on the data management and exchange. The access and sharing of correct data should be ensured in a secure and trusted way and play a crucial role for the business model of relevant market parties. The Platone Open Framework handles only technical data, it does not handle any customer-related personal data.

System operators need to have a proper legal framework to make use of flexibility resources data to manage the distribution and transmission grid. Current national implementation of the privacy protection regulation (GDPR) [17] and also future stricter e-Privacy regulation [18] on data collection must be taken into account. Although the recently agreed CEP [19] clearly states that smart meter data also enables DSOs to have better visibility of their networks and consequently reduce their operation and maintenance costs.

5.1 Shared Customer Database

Demand side flexibility is crucial for allowing final customers to become active in the market but also to system operators to make best use of flexibility in order to ensure efficient system operation on a regional level [20].

The main challenges for managing the demand side flexibility are:

- Enable access and use of flexibility to all the market parties.
- Ensure standardisation and interoperability among all the IT systems (customers, aggregators, operators, etc.). [21]
- Provide flexibility data in a secure and trusted way.

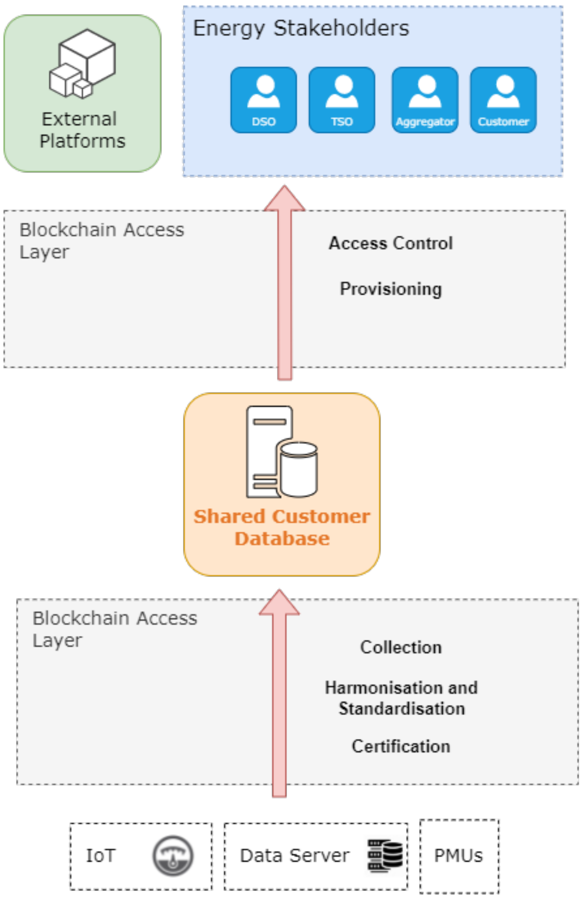

Figure 11: SCD Data Management

In this context, the Platone Blockchain Access Layer is able to enable a secure and shared data management, allows standard and flexible integration of external solutions and is open to the integration of external devices through standardized and interoperable interfaces and protocols. More details on the Blockchain Access Layer are provided in D2.11 [8] and in the Section 3.1. The scope of this chapter is to describe more in detail the Shared Customer Database, which is part of the Blockchain Access Layer, and how this component implements the data access management.

The Shared Customer Database (SCD) is the component that aims to ensure secure storage and availability of the data, respecting data standards modelling, data access policies, as well as data privacy. All the data collected, harmonized, and certified (through blockchain technology) are available for all the energy stakeholders involved as well as external platforms and services who need to use this data. Furthermore, the Platone Shared Customer Database includes rules and mechanisms for defining a Data Access Policy as well as security mechanisms for ensuring data protection and data privacy.

The SCD, as it is designed and developed, fits very well with the concept of the Flexibility Resources Register, which represents a high priority tool in the hands of both TSOs and DSOs for the effective management of all the flexibility resources, according to the report on the "Roadmap on the Evolution of the Regulatory Framework for Distributed Flexibility" performed by ENTSO-E and the European Associations representing DSOs [22].

From a technical perspective, given the large amount of data and high frequency provisioning within a smart grid, we decided to approach the technical implementation using Apache Cassandra [23] database that ensures scalability and high availability without compromising performance.

The Shared Customer Database was released in its first version and deployed in all the field trials (Italian, Greek and German) in the respective DSO environment, which is in charge to manage the SCD instance and all the data stored on it.

All the data collected and stored are:

- already anonymized before being passed to the SCD,
- uniquely traceable,
- tamper-proof (thanks to the blockchain technology application).

5.2 DSO Data Server

The DSO Data Server is a database that contains DSO data in the Greek DSO environment, i.e. master data and automated meter reading (AMR) metrics for MV and LV customers. It is designed as a containerized application that unifies data from different telemetering centres offline into a uniformed internal database. A dedicated API allows querying the database and gather reading data occasionally or periodically. The data is then published via MQTT, e.g. scheduled every 15 minutes. The API side of the DSO Data Server also transforms the data into an xml file which a data model, format, and structure according to the CIM 61968-9 Standard for Meter and Control. Introducing the DSO Data Server as a layer of indirection between the metering systems and externally hosted systems such as the Blockchain Access Layer allows for a fine-grained control to the accessed data without the need to expose the internal metering systems to the external platforms.

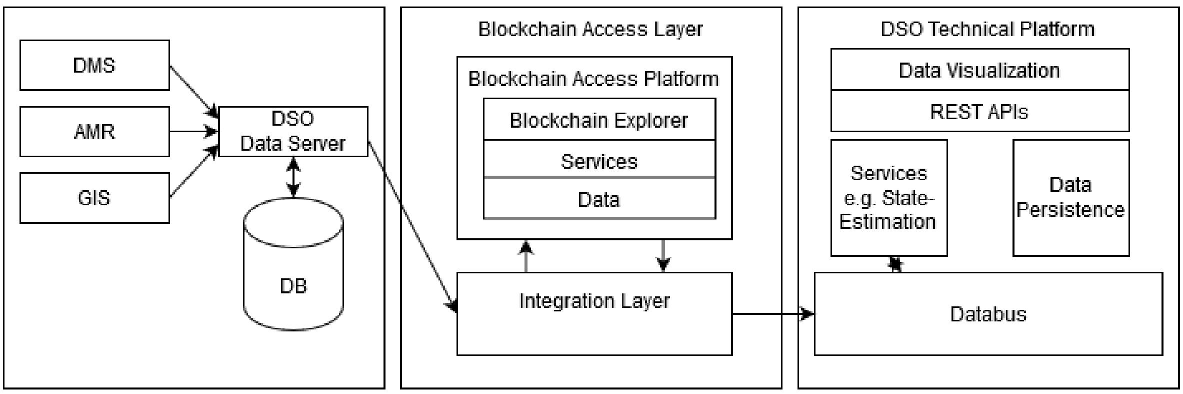

Figure 12 DSO Data Server between DSO systems in the Greek Demo and Platone Open Framework

6 Conclusion

The work done at this stage, allowed us to present a first overview of the intra-platform communication of the Platone Open Framework from different points of view, in order to allow all stakeholders involved to understand the characteristics and consider possible integrations. The most relevant standards for the Platone Open Framework at this stage are IEC 61850 and the CIM-61968-9 standards. Furthermore, the need for further harmonization of internal data models became apparent. The SARGON ontology was identified as a possible solution and will be evaluated during the further development and integration phases of the open framework. Results will be included in the second version of this report, D 2.10. Data privacy was considered from the beginning of the design phase and different measures for ensuring privacy at different layers of the framework were presented in this document.

The communication channels for the intra-platform communication are protected following well-established industry standards for cyber security. However, these will be monitored and adjusted throughout the remainder of the project and be presented in the final version of this report. Foreseen future releases will include more unified approaches for identity management and access control between the different Platforms. In addition, security measures such as the client-certificate authentication mechanism which are already successfully tested in some parts of the framework will be included in the remaining components as well.

All updates to the communication protocols and data models will also be included as public open-source in the git repositories of the respective Platone Open Framework components by end of the second (month 40) and third release phase (month 48). Potential extensions to other open-source projects, e.g. SARGON or SOGNO will also be merged upstream to the original projects to support the evolution of open source solutions.

7 List of Tables

8 List of Figures

9 List of References

[1] European Commission, "2050 long-term strategy", [Online]. Available: https://ec.europa.eu/clima/policies/strategies/2050_en

[2] Platone "D2.1 Platone Platform requirements and reference architecture (v1)" [Online]. Available: https://platone-h2020.eu/data/deliverables/864300_M12_D2.1.pdf

[3] Platone "D1.1 v1.0 General functional requirements and specifications of joint activities in the demonstrators" [Online]. Available: https://platoneh2020.eu/data/deliverables/864300_M12_D1.1.pdf

[4] Platone "D4.1 Report on the definitions of KPIs and UCs" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M12_D4.1.pdf

[5] Platone "D5.2 Detailed use case descriptions" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M12_D5.2.pdf

[6] Platone "D2.3 PlatOne Market platform (v1)" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M18_D2.3.pdf

[7] Platone "D2.6 PlatOne DSO Technical Platform (v1)" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M18_D2.6.pdf

[8] Platone "D2.11 PlatOne BlockChain Customer Access Layer (v1)" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M18_D2.11.pdf

[9] Platone "D2.14 PlatOne Integrated Framework Prototype (v1)" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M20_D2.14.pdf

[10] Uslar, M., Specht, M., Rohjans, S., Trefke, J., Gonzalez, J.M.V., The Common Information Model CIM: IEC 61968/61970 and 62325 –A practical introduction to the CIM (Power Systems), Springer, 2012.

[11] IEC 61968-9 : "Application integration at electric utilities - System interfaces for distribution management - Part 9: Interfaces for meter reading and control", 2013

[12] "SAREF ontology" [Online]. Available: http://ontology.tno.nl/saref

[13] "Web Ontology Language (OWL)" [Online]. Available: https://www.w3.org/OWL/

[14] W3C "RDF 1.1 Turtle" [Online]. Available: https://www.w3.org/TR/turtle

[15] ETSI TR 403 111: "SmartM2M; Smart Appliances Extension to SAREF; SAREF Extension Investigation".

[16] Haghgoo, Maliheh, et al. "SARGON–Smart energy domain ontology." *IET Smart Cities* 2.4 (2020): 191-198.

[17] GDPR "General Data Protection Regulation (GDPR) Compliance Guidelines" [Online]. Available: https://gdpr.eu/

[18] Wikipedia "ePrivacy Regulation" [Online]. Available: https://en.wikipedia.org/wiki/EPrivacy_Regulation

[19] FSR EUI "The Clean Energy for all Europeans Package - Florence School of Regulation" [Online]. Available: https://fsr.eui.eu/the-clean-energy-for-all-europeans-package/

[20] European Commission "Final Report: Demand Side Flexibility – Perceived barriers and proposed recommendations" [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/eg3_final_report_demand_side_flexiblity_2019.04.15.pdf

[21] European Commission "Study on ensuring interoperability for enabling Demand Side Flexibility" [Online]. Available: https://publications.europa.eu/resource/cellar/a61d67de-9ecd-11e9-9d01-01aa75ed71a1.0001.01/DOC_1

[22] E.DSO "Roadmap on the Evolution of the Regulatory Framework for Distributed Flexibility" [Online]. Available: https://www.edsoforsmartgrids.eu/wp-content/uploads/210722_TSO-DSO-Task-Force-on-Distributed-Flexibility_proofread-FINAL-2.pdf

[23] Apache "Apache Cassandra | Apache Cassandra Documentation" [Online]. Available: https://cassandra.apache.org/_/index.html

[24] OASIS "MQTT - The Standard for IoT Messaging" [Online]. Available: https://mqtt.org/

[25] Eclipse Foundation "Eclipse Mosquitto" [Online]. Available: https://mosquitto.org/

[26] OpenJS Foundation "Express - Node.js web application framework" [Online]. Available: https://expressjs.com/

[27] Apache Software Foundation "Apache Kafka" [Online]. Available: https://kafka.apache.org/

[28] Internet Society "What is TLS & How Does it Work? | ISOC Internet Society" [Online]. Available: https://www.internetsociety.org/deploy360/tls/basics/

[29] ethereum.org "Introduction to smart contracts | ethereum.org" [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/

[30] Confluent "Configure Confluent Platform to use TLS/SSL encryption and authentication | Confluent Documentation" [Online]. Available: https://docs.confluent.io/platform/current/kafka/authentication_ssl.html

[31] Linux Foundation Energy "SOGNO - LF Energy" [Online]. Available: https://www.lfenergy.org/projects/sogno/

[32] Linux Foundation "Kubernetes" [Online]. Available: https://kubernetes.io/

[33] Docker Inc., "Empowering App Development for Developers | Docker" [Online]. Available: https://www.docker.com/

[34] Linux Foundation "K3s: Lightweight Kubernetes" [Online]. Available: https://k3s.io/

[35] Platone "D4.2 v1.0State estimation tool" [Online]. Available: https://www.platone-h2020.eu/data/deliverables/864300_M15_D4.21.pdf

10 List of Abbreviations

Abbreviation	Term
ADMS	Advanced Distribution Management System
ALF-C	Avacon Local Flexibility Controller
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
API	Application Programming Interface
BAL	Blockchain Access Layer
BAP	Blockchain Access Platform
CIM	Common Information Model
DB	Database
DMS	Distribution Management System
DSO	Distribution System Operator
DSOTP	DSO Technical Platform
EMS	Energy Management System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IDM	Identity Management
IEC	International Electrotechnical Commission
IoT	Internet of Things
JSON	JavaScript Object Notation
MQTT	Message Queuing Telemetry Transport
PMU	Phasor Measurement Unit
REST	Representational State Transfer
SAREF	Smart Appliance REFerence
SARGON	SmArt eneRGy dOmain oNtology,
SCADA	Supervisory Control and Data Acquisition
SCD	Shared Customer Database
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
WP	Work Package
XML	Extensible Markup Language