IOF2020 REFERENCE ARCHITECTURE FOR INTEROPERABILITY, REPLICABILITY AND REUSE

Based on *D3.3 Opportunities and Barriers in the present regulatory situation for system development* available on https://www.iof2020.eu/deliverables/d3.3-opportunities-and-barriers-in-the-present-regulatory-situation-for-system-development-v1.2.pdf

WP 3

IoF2020 has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 731884. Visit iof2020.eu for more information about the project.

Extended summary

IoF2020 has analysed how IoT and related technologies can be applied to the domain of Agrifood, with a view to creating interoperable and portable solutions. The final aim is allowing for the building of an IoT ecosystem around the IoF2020 project and ultimately around Smart Farming in Europe.

This overview identifies relevant technologies and standards in several IT architectural layers, analyses gaps and adoption barriers and describes how they are adopted in the use cases and trials within the IoF2020 project.

The technologies and associated standards considered by this document address different layers that have to be tackled when deploying a Smart Food and Farming solution, as depicted by the figure below. To this aim the main layers that have been identified are:

- *Physical Device Layer*. This layer is composed by different IoT devices and agricultural machinery deployed in the field.
- *Connectivity Layer*. This layer enables the bidirectional transmission of data produced by devices or machinery.
- *IoT Service Layer*. It exposes the raw data generated from IoT Devices and, possibly, actuation commands through different application-level transport protocols.
- *Mediation Layer.* It transforms the raw data coming from devices or other external services, into curated, harmonized and possibly aggregated data.
- *Information Management Layer*. This layer serves mainly as a data hub, which enables the publication, consumption, subscription and processing of all the information relevant to a food and farming solution.
- *Application Layer.* In this layer reside all the different applications such as those related to decision support (DSS), farm management (FMIS), dashboards or enterprise resource planning (ERPs).
- A cross-cutting layer on *Security and Privacy* aimed at guaranteeing secure access to information and devices, while respecting the privacy of consumers, farmers and exploitations.

In addition, other external entities play a relevant role, namely:

- *Open Data providers and Public Geo-Services*. For instance, public databases offering data in the agricultural domain, geo-services publishing weather or spatial data or even satellite data/image platforms.
- *Harmonized information models.* They define the structure and representation of the information to be managed, with a view to enabling interoperability and portability of solutions in a wider ecosystem.

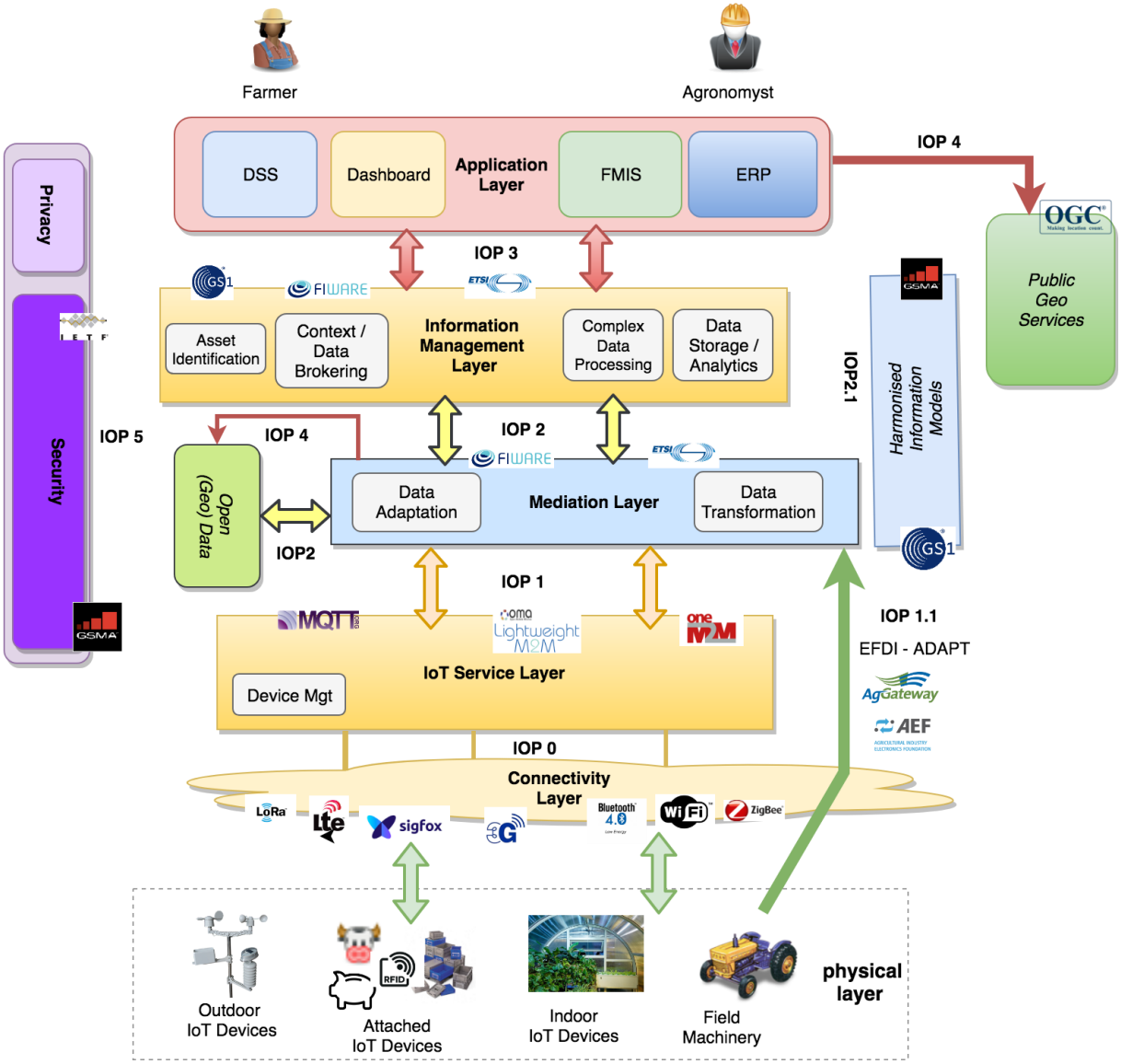

Figure 1: Overview of IoF2020 interoperability points and their relationship to standards

The interoperability points identified in the referred figure are described in the following text.

Interoperability Point 0: IoT Connectivity Layer

The IoT Connectivity Layer enables communication between IoT devices or agricultural machines (physical device layer) and data gathering platforms. It enables transmission of data from devices (uplink), and reception of actuation commands or task plans by device (downlink). There are three different enabling technologies:

- Short range communications are based on well-established standards for wireless indoor communications based on local area networks, where WiFi and Bluetooth are the most significant ones. There are also solutions for outdoor facilities as ZigBee (IEEE 802.15.4). There

are challenges related to device battery life, network coverage and operation costs. ZigBee is being used in a solution based on wireless sensor networks for precision agriculture. Trial 4 is planning to use ZigBee to monitor vegetable growth and manage resources.

- Cellular networks allow data transmission at high speed, long range, with high reliability and great degree of autonomy. These include cellular and telco-operated networks exploiting 3G, 4G and 5G technologies. The main challenge is universal coverage, battery lifetime and device costs. Rural areas still have low connectivity and usually considerable extension.
- Low Power Wide Area (LPWA) wireless technology complements existing cellular mobile network and short-range technologies, with lower costs and better consumption characteristics. LPWA networks are well suited for smart farming as they provide long range communications and a low-cost proposition for devices, together with long battery life. SigFox employs a proprietary technology that enables communication using the Industrial, Scientific and Medical (ISM) radio band. LoRa is intended for wireless battery-operated things on a regional, national or global network. LoRaWAN targets key requirements of IoT such as secure bidirectional communication, mobility and localization services. NB-IoT enables a wide range of devices and services to be connected using cellular telecommunication bands and focuses specifically on indoor coverage, low cost, reliability, long battery life, and enabling many connected devices. LTE-M combines several radio access network and core network features to optimize LTE networks for IoT needs and support of new category of LTE devices. SigFox is planned to be used at least in trials 2, 3 and 4, while LoRa is planned to be used in trials 1, 2, 3 and 5. All trials want to potentially explore using NB-IoT and LTE-M, provided there is network coverage in the field areas.

Interoperability Point 1: IoT Service Layer

The IoT Service Layer exposes the raw data generated from IoT devices through different applications level transport protocols based on different paradigms. It also offers interfaces that allow communicating with devices for management or actuation purposes. The most relevant technologies enabling this interoperability point are:

- MQTT is a lightweight event and message-oriented protocol allowing devices to asynchronously communicate efficiently across contained networks to remote systems. It is a publish/subscribe messaging protocol capable of delivering messages from one publisher to multiple subscribers through a topic. There are multiple MQTT opens source implementations and client libraries and it has been successfully implemented in the smart farming domain.
- MQTT-SN can be considered a version of MQTT further adapted to wireless communication and optimized for the implementation on low-cost, battery-operated devices with limited

processing and storage resources. There are different open source implementations of MQTT-SN.

- LWM2M defines an application layer communication protocol between LWM2M sensors and LWM2M clients. It makes uses of a light and compact protocol and an efficient resource data model. It is frequently used with CoAP, which is a specialized web transfer protocol for use with constrained nodes and constrained networks in the IoT, particularly designed for machine-to-machine applications. The OMA LWM2M protocol, which enables remote management of M2M devices, has a modern architectural REST-based architecture and is highly extensible.
- ONEM2M is a horizontal IoT/M2M middleware platform providing common functions, i.e. abstract and common APIs, for different vertical service domains. There are commercial and open source implementations of this technology.

The main adoption barrier in this interoperability point is the existence of diverse standards, which are endorsed by different entities. Use cases face the challenge of selecting a technology linked to specific components, which may be replaced or become outdated. There is a promising initiative called Web of Things, aiming to expose IoT devices as web resources, regardless of IoT protocols, leveraging the possibilities offered by Open Linked Data. Although there is no final specification yet, this technology should be followed and explored.

Interoperability Point 1.1: Agricultural Machinery Comms Layer

This layer sits between the agricultural machinery (tractors, implements, etc.) and the Mediation Layer, and allows to publish relevant data generated from machinery to the cloud. The most relevant standards are:

- ISOBUS (ISO—11783) governs electronics and data exchange between different farm machines (e.g. tractor – farm implement) and has been the de-facto standard for decades between tractors and has been implemented by different manufacturers. A local communication bus-system based on CAN bus connects the tractor and various components implemented. Data interchange and process flow are also defined in parts of this standard, namely using ISO-XML and EFDI.
- The ADAPT framework is comprised of an Agricultural Application Data Model, a common API (Application Programming Interface), and a combination of open source and proprietary data conversion plugins. Participating FMIS (Farm Management Information System) companies are responsible for completing their own implementation of mapping the Agricultural Application Data Model to their FMIS data model.

Interoperability Points 2, 3 and 4: Mediation and Information Management Layer

The aim of the mediation and the information management layers is to offer the right information to the right application at the right time. These layers are responsible for transforming raw data into information relevant and ready to be consumed by applications, so that smart behaviours are exhibited, enabling the optimization of Agrifood processes.

The Mediation Layer, situated between the IoT Service Layer and the Information Management Layer (Interoperability Point 2), is responsible for gathering the raw data coming from devices or other external services, and curate, harmonize and possibly aggregate it, so that it can be published as context information, or supplied to upstream data processing algorithms or analytics. In addition, this layer is also capable of sending actuation commands to the IoT Service Layer. Finally, the Mediation Layer may also be capable of gathering data from other data sources such as agricultural machinery or public geo-services (interoperability point 4).

The Information Management Layer, situated between the Mediation Layer and the Application Layer, serves mainly as data hub to enable publication, consumption and subscription of all information relevant to an application (interoperability point 3).

- FIWARE NGSI is an instantiation of the OMA NGSI-9 and NGSI-10 abstract interfaces for context information management. FIWARE NGSIv2 is based on HTTP/REST and JavaScript Object Notation (JSON), following the usual, de-facto industry standards. NGSI supports a powerful, yet simple, well-known approach to represent context information, with a meta-model based on entities, attributes and metadata. The most popular implementation of FIWARE NGSI is the Orion Context Broker, which uses MongoDB as underlying data source.
- NGSI-LD is an evolution of the OMA NGSI information model, to better support linked data, property graphs and semantics. This work is being conducted under the ETSI ISG CIM initiative.
- WFS is an interface specified by the Open GIS Consortium to allow exchange of geographic data across the Web. It defines the rules for requesting and retrieving geographic information using HTTP. The interface describes the data manipulation operations on geographic features. XML-based Geographic Markup Language is used to exchange information.
- WMS is a specification outlining communication mechanisms allowing disjoint software products to request and provide preassembled map imagery to a requesting client. Using WMS, a request is responded with a readymade map which can be displayed, and not raw data.

The main adoption barrier in the Mediation and Information Management Layers is the proliferation of proprietary APIs, vocabulary and incompatible data models.

Interoperability Point 2.1: Harmonised Information Models

Interoperability in the Agrifood sector is not only a matter of hamonised APIs (such as NGSI-LD or WFS), but also harmonised domain-specific data models, capable of modelling the different concepts that are relevant and which intervene in the different applications.

- CLP.26-IoT Big Data Harmonized Data Model, published by GSMA IoT programme, is a normative document describing some harmonised data entities used in different IoT domains as agriculture, environment, and smart city. The definition of different entity types is based on JSON and the FIWARE NGSIv2 information model, while reusing some parts of schema.org.
- ADAPT Framework, developed by AG-Gateway, includes three core elements: the ADAPT data model (ADM), a plugin manager and a set of plugins. The ADAPT framework involves the development of a proprietary plugin, which maps the own system's model into the ADM model and serializes the information into a container to share it. The receiver deserializes the container using its own plugin and extracting relevant information for its system.
- GS1 Core Business Vocabulary is the data standard used within Electronic Product Code Information Service (EPCIS), which is a GS1 standard interface for capturing and sharing event data independent of any data carrier. The Core Business Vocabulary defines elements and their values e.g. for business step identifiers, disposition identifiers, business transactions and respective types, and source/destination identifiers and types.
- GS1 enables unique asset identification through different standards.
    - GEPIR (Global Electronic Party Information Registry) is a unique, internet-based service that gives access to basic contact information for companies that are members of GS1. These member companies use GS1's globally unique numbering system to identify their products, physical locations, or shipments.
    - Global Location Number (GLN) can be used by companies to identify their locations, giving them complete flexibility to identify any type or level of location required.
    - Global Trade Item Number (GTIN) can be used by a company to uniquely identify all of its trade items. GS1 defines trade items as products or services that are priced, ordered or invoiced at any point in the supply chain.
    - GS1 has two GS1 Keys for asset identification. The Global Returnable Asset Identifier (GRAI) is especially suitable for the management of reusable transport items, transport equipment, and tools and can identify these returnable assets by type and if needed also individually for tracking and sorting purposes. The Global Individual Asset Identifier (GIAI) can be applied on any asset to uniquely identify and manage that asset. This could be e.g. a computer, desk, vehicle, piece of transport equipment, or spare part.

- The Electronic Product Code™ (EPC) is syntax for unique identifiers assigned to physical objects, unit loads, locations, or other identifiable entity playing a role in business operations. EPCs have multiple representations, including binary forms suitable for use on Radio Frequency Identification (RFID) tags, and text forms suitable for data sharing among enterprise information systems. GS1's EPC Tag Data Standard (TDS) specifies the data format of the EPC, and provides encodings for numbering schemes -- including the GS1 keys -- within an EPC.

Interoperability Point 5: Security and Privacy

The digitalization of the Agrifood industry to enhance the farming process implies that data is being generated and exchanged throughout the production process. Such increasing exchange of data is a major challenge for the sector, and poses questions about privacy, data protection, intellectual property, data attribution (ownership), relationships of trust/power, storage, conservation, usability and security.

An IoF2020 solution should be able to properly react to data privacy and security violations with defined procedures and should incorporate capabilities in order to secure the platform which is going to support the farming services, by providing support for confidentiality, integrity, authentication, authorization, immutability, trust and non-repudiation, when needed. IoF2020 has defined a set of IoT Security Guidelines, which are recommended to be followed when implementing the use cases and trials.

Some relevant initiatives include:

- The EU General Data Protection Regulation (GDPR) was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.
- A coalition of associations from the EU agri-food chain launched a joint EU Code of Conduct on agricultural data sharing. The Code promotes the benefits of sharing data and enables agri-business models, including agri-cooperatives and other agri-businesses, to swiftly move into an era of digitally enhanced farming. The Code sheds greater light on contractual relations and provides guidance on the use of agricultural data, particularly the rights to access and use the data.
- GSMA IoT Security Guidelines provide an approach to end-to-end security, including 85 detailed recommendations for secure design, development and deployment of IoT services. These guidelines promote best practices for the secure design, development and deployment of IoT services, and provide a mechanism to evaluate security measures.
- oneM2M develops technical specifications and standards which address the need for a common M2M Service Layer in IoT. oneM2M has issued two relevant technical specifications in this topic, namely TS-0003-V2.12.1 Security Solutions and TR-0008-V2.0.1 Security.