DAPHNE

Data-as-a-service platform for healthy lifestyle and preventive medicine

610440

D8.4 Standardization Report

Lead Author: Roni Ram

With contributions from: Susan van Wissen (Evalan), Tijmen Gelijsteen (Evalan)

Reviewer: Ángel Palomares Pérez (ATOS)

Deliverable nature:	R
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	30/10/2015
Actual delivery date:	
Version:	1.0
Total number of pages:	19
Keywords:	Interoperability, data cloud, open middleware, standards

Abstract

The present report is the second version of the standardization report. Based on the final architecture of DAPHNE platform, it identifies the main components in the solution that should support standards. Moreover, it defines for these components the relevant standards and terminology systems that relate to data format, messaging exchange, communication, security and interoperability. The decision process regarding the final standards that will be supported is described following the different considerations that were taken into account. The roadmap for the implementation process of the selected standards is specified.

Executive summary

This standardization report describes the decision of the final standards that will be supported by DAPHNE platform. Although the first standardization report, which was created at the end of the first year, recommends on the standards to support, some changes had to be made based on the final architecture of DAPHNE. According to this architecture, the Data Cloud plays a central role while almost all the different layers (aggregator, decision-making and application layers) interact with it. As a result, standards are crucial for the Data Cloud; it stores and provides data to DAPHNE components and it may be used in the future by other healthcare and research systems. For all the other DAPHNE components that interact only among themselves, standards are not needed.

An additional layer that was also identified in the first standardization report as a channel to external systems is the aggregation layer. The Aggregator is the component that interacts with DAPHNE sensor and movement devices. However, to collect measurement data from additional 3rd party sensors the Open Middleware is being used. The Open Middleware which is the core component of the Aggregator was designed to support the Continua standard and as a result any Continua certified device can be connected to DAPHNE platform and upload data to DAPHNE Data Cloud.

The security controls that should be implemented for DAPHNE platform are driven by following a standardized approach. Since privacy and security are crucial for a system like DAPHNE, serving patients and managed by medical institutions, the relevant standards for the above components are detailed.

The main aim of this version of the report is to describe the standards chosen for DAPHNE platform and to provide the first insights regarding the implementation efforts. As the first milestone for DAPHNE prototype is approaching (M24) there is a significant progress and most of the standards are already supported. The final version of the prototype which is planned for M30 will support the rest of the standards.

The standardization report gives an overview in section 2 of the main DAPHNE components that should support standards based on the final DAPHNE architecture. Then, section 3 details the most relevant standards for DAPHNE Data Cloud and the standards that should be supported are described with focus on standards for communication, data, messaging, interoperability and security. A detailed analysis of the standards that are relevant and supported by the Open Middleware, the core of the DAPHNE Aggregator component, is presented in section 4. Finally, in section 5 there is a summary of the supported standards with the roadmap for implementation.

Document Information

IST Project Number	610440	**Acronym**	DAPHNE
Full Title	Data-as-a-service platform for healthy lifestyle and preventive medicine		
Project URL	http://www.daphne-fp7.eu/		
Document URL			
EU Project Officer	Mr. Benoit Abeloos		

Deliverable	**Number**	D8.4	**Title**	Standardization Report v2
Work Package	**Number**	WP8	**Title**	Exploitation and standardization

Date of Delivery	**Contractual**	M24	**Actual**	M24
Status	version 0.1		final ■	
Nature	prototype □ report ■ demonstrator □ other □			
Dissemination level	public ■ restricted □			

Authors (Partner)				
Responsible Author	**Name**	Roni Ram	**E-mail**	roni@il.ibm.com
	Partner	IBM	**Phone**	roniram1 (skype)

Abstract (for dissemination)	The present report is the second version of the standardization report. Based on the final architecture of DAPHNE platform, it identifies the main components in the solution that should support standards. Moreover, it defines for these components the relevant standards and terminology systems that relate to data format, messaging exchange, communication, security and interoperability. The decision process regarding the final standards that will be supported is described following the different considerations that were taken into account. The roadmap for the implementation process of the selected standards is specified.
Keywords	Interoperability, data cloud, open middleware, standards

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
13/09/2015	V0.1	Roni Ram (IBM)	First draft
16/09/2015	V0.2	Roni Ram (IBM)	Remove the section about security
17/09/2015	V0.3	Ángel Palomares Pérez (ATOS)	Internal review
20/10/2015	V1.0	Roni Ram (IBM)	Final version

Table of Contents

List of figures

Abbreviations

BLE: Bluetooth Low Energy

CDG: Continua Design Guidelines

IAM: Identity and Access Manager

PHI: Protected Health Information

PHR: Personal Health data Repository

PIHub: Pseudo Identifier HUB

TLS: Transport Layer Security

Definitions

Interoperability: The ability to work together from different systems, technologies and organisations. For this, usually it is necessary that common norms and standards are observed.

DAPHNE Data Cloud: The storage of user data in the cloud which includes the Public Personal Health Record (PHR) and the self-tracking health data repositories.

Open Middleware: The core component of DAPHNE Aggregator that is used to collect measurement data from sensor of third parties and to upload this measurement data to the DAPHNE Data Cloud.

1 Introduction

The main goal of the DAPHNE platform is to develop a state-of-the-art breakthrough ICT platform for reducing sedentariness and unhealthy habits, based on data-as-a-service and personalized services. To achieve the interoperability that is needed among all the devices, services, systems, models and technologies, it is necessary that common norms and standards are observed.

Interoperability, as defined by IEEE, is the ability of two or more systems or components to exchange information and to use the information that has been exchanged. It distinguishes between two types of interoperability: syntactic and semantic interoperability. Syntactic interoperability is the ability of two or more systems to communicate and exchange data. Specified data formats, communication protocols and the like are fundamental. In general, XML or SQL standards provide syntactic interoperability. Syntactical interoperability is required for any attempts of further interoperability. Semantic interoperability is the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of both systems. To achieve semantic interoperability, both sides must defer to a common information exchange reference model. The content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood.

A high degree of compatibility of the DAPHNE platform with common standards will help to guarantee sustainability and business impact. The standardization plan is driven by T8.2 which plans, organizes and coordinates the standardization activities to maximize widely adoption of DAPHNE results.

Standardization is a process driven by planning, identifying, executing and creating opportunities. The standardization work within the DAPHNE project is divided to three phases which are reported in three different deliverables; D8.2, D8.4 and D8.6 respectively.

The first phase of the standardization work was focused on research [2]. It aimed to explore the state of the art standards that may be related to DAPHNE platform and to recommend on the standards that should be supported by the platform.

The current standardization report (v2) which reflects the second phase, aims to report on the selected standards and on the execution process within the different DAPHNE components to support these standards. Since the decision on the standards depends not only on the available standards but also on what can actually be standardized, the selected standards may differ from those that were recommended at the first phase.

The third version of the standardization report will report on the lessons learnt and recommend on further activities to promote and contribute to relevant standardization development bodies and initiatives.

1.1 Scope

This document is the second version of the standardization report which is delivered at the end of the second year of the project. The third version (D8.6) is planned to be delivered at the end of the third year of the project. The present report revisits the standards that were recommended in the first report and adopts the relevant standards to the final design of DAPHNE platform. While deciding on the standards to support, proprietary interfaces are considered as well. Topics as development time, resources to invest, expected impact, etc are considered and based on that, the supported standards for the DAPHNE platform are selected and the main insights regarding their execution are reported.

1.2 Expiration

The standardization report is split in 3 versions as specified in the DOW [1]. Each version updates, extends and elaborates on the former document based on the current state of the project in terms of relevant requirements, architecture, implementation and execution of the pilots.

2 DAPHNE platform

The architecture of DAPHNE platform is specified in D2.7 [3]. It is described by two different functional blocks diagrams: (1) for installation A (wellbeing users) as described in Figure 1 and (2) for installation B (patients) as described in Figure 2.

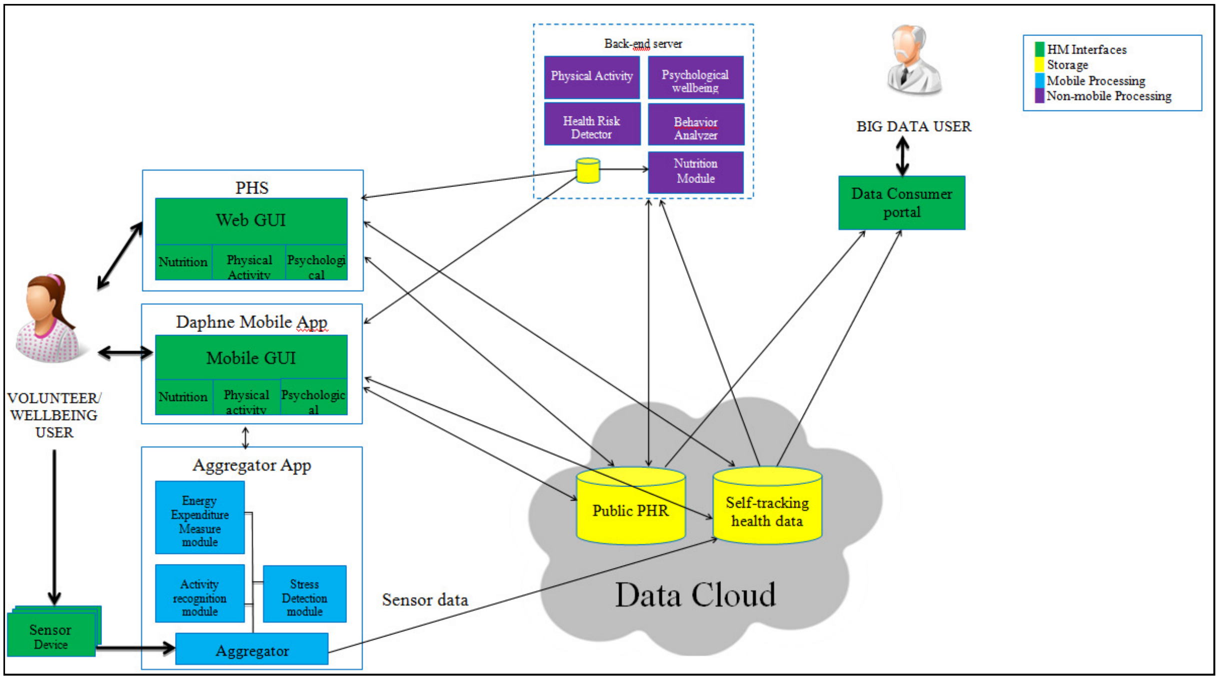

Figure 1 DAPHNE functional blocks diagram for Installation A (wellbeing users)

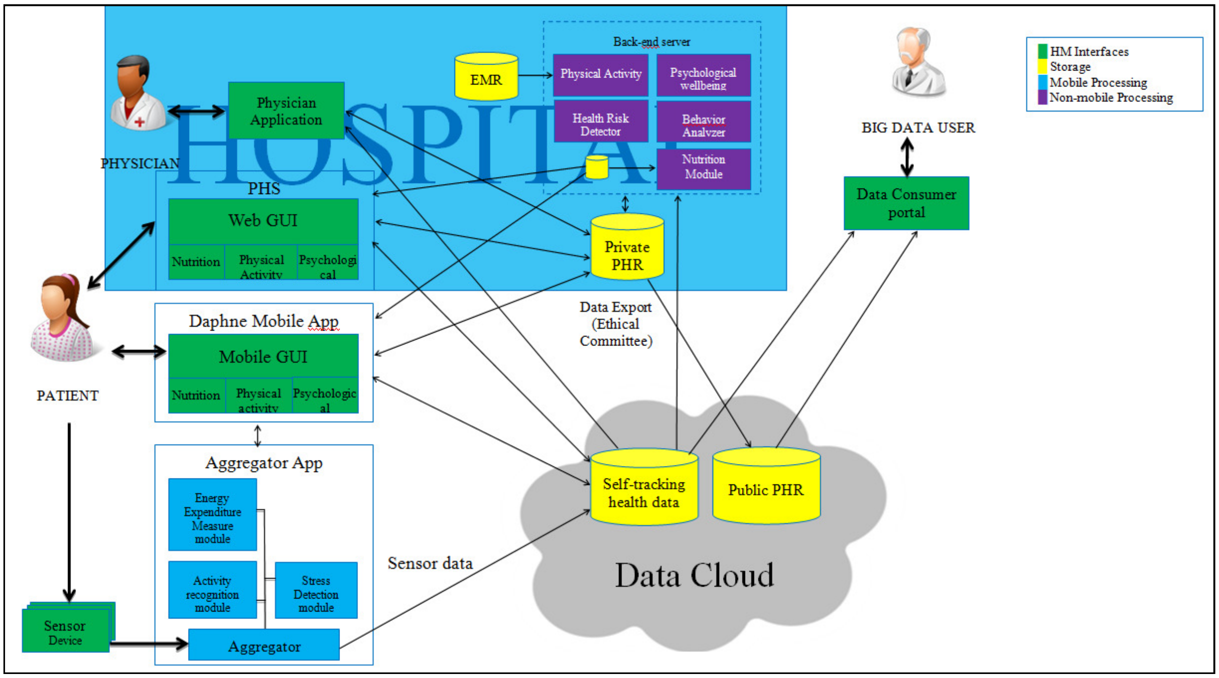

Figure 2 DAPHNE functional blocks diagram for Installation B (patients)

In D8.2 [2], the first standardization report, the relevant standards have been mapped to five different layers. The focus of these layers has been updated to the final DAPHNE architecture:

- The **Sensor Layer** is composed by all the physical devices that generate personalized user data (sensor device and movement device). This layer is in charge of gathering environmental and biomedical information of the users. The collected raw data enriched with some quality information (such as timestamps) is transferred to the aggregation layer.

- The **Aggregation & Process Layer** transforms the raw data collected from the various sensors to the Data Cloud after processing of the advanced mobile modules.

- The **Decision-making Layer** is composed by programs and intelligent systems that analyze the data generated by the lower levels and stored in the Data Cloud. These programs may use knowledge from the medical domain and may deliver decisions about the condition of the user or generate advice to the user. All the new insights are stored again in the Data Cloud.

- The aggregated data is forwarded as well as the decisions and advices from the Data Cloud to the **Application Layer.** This layer consists of web-based user interfaces with their server side services. The aggregated data in this layer is accessed and consumed by individual and collective services.

- The **Data Cloud**, the fifth layer, interacts with all the layers except of the sensor layer. The cloud provides data related services for the entire system and semantic interoperability among all the components accessing it.

To achieve the interoperability that is needed for DAPHNE platform, all the interfaces that the platform may have with external systems have to be examined. These interfaces should be supported by common standards to ensure that both syntactic interoperability and semantic interoperability are achieved.

Based on the layers described above, the following list describes the main DAPHNE components that should expose interfaces to components that are external to DAPHNE:

- **Data Cloud** – The data is stored in DAPHNE Data Cloud mainly by mobile devices and care providers. It is later consumed by advanced personalized health services for the goal of encouraging users to adapt a healthy lifestyle and by research institutions and third parties, upon approval of an ethical committee, for further analysis and data mining.

- **Open Middleware** – The Aggregator mobile application collects the measurements of a user from a sensor device, processes this data with mobile modules and sends these to the Data Cloud. To connect sensors from third parties to the DAPHNE system, the Open Middleware, the core of the Aggregator, is being used. It acts as the interface between sensor devices and the Data Cloud, handling tasks such as user authentication and authorization, and data buffering.

- All the other DAPHNE components should interact only among themselves and therefore no effort was invested to integrate standards that ensure interoperability in these components.

The following sections describe in detail the considerations regarding the standards to support by each of these components and the first insights regarding the implementation efforts.

3 Data Cloud

DAPHNE Data Cloud is divided to two different repositories:

- The Personal Health data Repository (PHR) is the repository for all the data that according to the privacy and security regulations cannot leave the hospital. To keep the same architecture approach for both installation A and B, PHR is being used in the same way whether the user acts a Patient or a Wellbeing user role; the only difference is that the PHR is deployed in the Data Cloud and not inside the hospital.
- The self-tracking health data repository in the Data Cloud is the component that provides long term, scalable and secure storage capabilities for data coming from various sources as sensors, wearable devices and mobile applications. While complying with privacy laws/directives, it offers the data for personal care and for big data analytics by third parties.

The components that act as data sources and data consumers to the Data Cloud are mobile devices, desktop applications and intelligent algorithms, operated by the patients/well being users, informal caregivers and care providers. Additional data consumers are analysis tools, operated by big data users (mainly research institutions), which aim to gain new insights from the big data.

The current components that interact with the Data Cloud are only the DAPHNE components. However, to provide the infrastructure that is needed for future integration with existing medical systems, analysis tools and mobile applications, standards are crucial.

When considering standards for the Data Cloud the two main purposes of the cloud have to be examined. The first purpose is to store the personal health data to support healthcare and wellness systems while providing care to patients and well being users. The second purpose is to provide anonymized data sets for second use of the data.

As reported in D8.2 [2], the recommended standards for the interaction with the Data Cloud for the purpose of personal care should be aligned with ITU-T H.810 [8]. However both the WAN interface and the HRN interface are only partially aligned with the requirements of the Data Cloud, as detailed in D6.1 [5]. Therefore, additional standards were considered. The following sections describe the decisions that were made in the different topics that relate to the Data Cloud standards. The decision process was followed by internal discussions among the DAPHNE partners. The full description of each of these standards is provided in the first version of the standardization report [2].

To achieve the big data goals set out by business and consumers, the standards community has launched several initiatives and working groups on big data [9]:

- In 2012, the Cloud Security Alliance established a big data working group[1] with the aim of identifying scalable techniques for data-centric security and privacy problems.
- The U.S. National Institute of Standards and Technology (NIST) working group intends to support secure and effective adoption of big data by developing consensus on definitions, taxonomies, secure reference architectures and a technology roadmap for big data analytic techniques and technology infrastructures[2].
- ISO/IEC JTC1's data management and interchange standards committee (SC32) has initiated a study on next generation analytics and big data[3].
- The W3C has created several community groups on different aspects of big data[4].

These initiatives will eventually define the recommend standards for the Data Cloud in the aspect of data-as-a-service.

[1] CSA, https://cloudsecurityalliance.org/research/big-data/
[2] NIST, http://bigdatawg.nist.gov/
[3] JTC1 SC32, http://www.jtc1sc32.org/doc/N2351-2400/32N2388b-report_SG_big_data_analytics.pdf
[4] W3C, http://www.w3.org/community/custexpdata/ and http://www.w3.org/community/bigdata/

3.1 Data

According to ITU-T H.810 the chosen standards and profiles for the data payload are:

- WAN interface - IHE DEC PCD-01 transaction with the use of HL7 V2.6 messages
- HRN interface - HL7 CDA R2 standard [HL7 CDA], profiled by the HL7 Personal Healthcare Monitoring (PHM) Implementation Guide

ISO/IEEE 11073 semantics may not be able yet to support all the input and processed data that shall be delivered by the different DAPHNE components to DAPHNE Data Cloud and therefore the mapping to HL7 V2.6 [IHE PCD-TF-2] is still difficult to achieve and a more complex representation may be needed.

In addition, the use of a data format that is based on documents/reports (as the HL7 CDA R2 standard) may cause to a significant overhead to the development of DAPHNE components while parsing the query results. These components access the Data Cloud to consume specific data. If the results are returned in a structure that is based on CDA then the results may contain a lot of information that could be not relevant to the query that was asked but must be provided according to the standard constraints. This demands a complicated parsing process to extract the relevant data.

With these constraints in mind, the JavaScript Object Notation (JSON) standard is considered. JSON is a lightweight data-interchange format which is not tightly tailored to clinical data representation. JSON has all the advantages of XML messages but is much better suited to data-interchange.

The decision regarding the standard to use for the Data Cloud is to adopt JSON, the commonly used standard by wellness mobile applications, as the basic data format that all the components that interact with the Data Cloud have to support. With the JSON format that offers a human-friendly way of representing data, new algorithms and applications, produced by other vendors, which analyze the raw, accumulated and anonymized data, can be easily integrated into DAPHNE platform. The exact JSON messages that are exchanged between the components and the Data Cloud are detailed in the Data provider API [5] and the Data-as-a-Service API [6].

The first implementation of the Data Cloud [7] is based on the definition of those interfaces with minor changes due to some clarifications of the requirements.

To support the Italian EHR Interoperability guidelines which have addressed the adoption of the HL7 standard and in particular the progressive use of CDA R2, the Data Cloud interfaces (and particularly the Data Provider API) adopts the HL7 CDA R2 standard (may be profiled by the PHMR Implementation Guide in the future) to retrieve summary of user data from DAPHNE Data Cloud. This could support the exchange of patient summary information stored in DAPHNE Data Cloud with existing EHRs deployed in medical institutions and PHRs that are personally used. The final prototype of the Data Cloud that is planned for M30 will support this standard.

3.2 Messaging exchange framework

According to ITU-T H.810 the chosen standards and profiles for the messaging exchange framework are:

- WAN interface - Web services transport which conforms to the Web Services Interoperability Organization's Basic Profile Version 1.1 [WS-I BP] and Basic Security Profile 1.0 [WS-I BSP]. The WAN message exchange framework further specifies conformance to the draft Reliable Secure Profile [WS-I RSP] to constrain the optional use of additional web service standards
- HRN interface – (IHE) Cross-Enterprise Document Sharing (XDS) profile

The recommended messaging exchange framework by ITU-T H.810 for the WAN interface is motivated by the availability of client and server implementations and a need to ensure the scalability of the receiver devices. This transport interface seems appropriate for the Data Cloud.

IHE XDS might be a feasible option for storing the data in DAPHNE Data Cloud but since it provides limited query capabilities this cannot be used by DAPHNE consumer components. Other existing healthcare systems can definitely utilize an XDS interface for sharing and retrieving user data from the Data Cloud.

Based on these considerations it was decided to use an approach of web service APIs that adhere to the REST architectural constraints. REST's client–server separation of concerns simplifies component implementation, reduces the complexity of connector semantics, improves the effectiveness of performance tuning, and increases the scalability of pure server components. REST is designed for use over the open internet/web. This is a better choice for web scale applications, and certainly for cloud-based platforms. The exact REST URLs that are exposed by the Data Cloud are detailed in the Data Cloud interfaces [5][6].

The first implementation of the Data Cloud [7] is based on the definition of those URLs with minor changes due to some clarifications of the requirements.

3.3 Interoperability

The semantic interoperability in DAPHNE Data Cloud is achieved by using international coding systems (i.e. SNOMED-CT, LOINC, ICD-10, etc.) for data representation. This enables an unambiguous understanding of the meaning of the data that is exchanged between the different components and DAPHNE Data Cloud.

Both interfaces of the Data Cloud, Data provider API and Data-as-a-Service API, are using these international codes. However, not all the data fields that are used in DAPHNE platform are represented in a known coding system (due to their specific belonging to DAPHNE solution). These data fields were defined in the same way as the other fields with the code system “DAPHNE internal”. The code is defined as a combination of 3 numbers (X.Y.Z) that uniquely defines the code; X defines the category, Y defines the sub category, Z defines an index. The mapping of the different data fields to their corresponding coding system is detailed in deliverable D6.1 Data Provider API [5]. The Data-as-a-Service API utilizes this definition of codes and retrieves the anonymized data with the same codes.

In addition to the codes, the ISO 8601 time format is being used for date and time representation.

The first implementation of the Data Cloud [7] is based on the defined codes with some additional new codes that were added due to some clarifications of the requirements.

3.4 Security

3.4.1 Consent directives

The consent of the user captures his approval to share his data with specific types of big data users (big data user profiles). As described in D6.2 [6], CDA R2 Consent Directive leverages the existing HL7 specifications and terminology standards to create a consent directive document specification.

As described in the standardization report [2], IHE Basic Patient Privacy Consents (BPPC) profile provides a mechanism to record the patient privacy consent(s) that define who can access his data and a method for consumers to use to enforce the privacy consent appropriate to the use.

Although there is a significant work that can be leveraged in standards that relate to consents, it was decided to adapt a simple and proprietary mechanism to support that within DAPHNE platform (will be developed during the 3rd year of the project). This is mainly motivated from the current ecosystem of DAPHNE which is isolated from existing systems in the medical domain. However, future work on the Data Cloud must leverage these standards and adapt the proprietary mechanism for managing consents into a standardized method that can be integrated with medical systems.

3.4.2 Anonymization

As reported by ITU [8], a progress is being made in techniques for data anonymization, the process of altering data in a way that prevents the identification of key information (e.g., personally identifiable information). However, these techniques still need to be studied and evaluated considering current (and future) data aggregation and analysis capabilities. Therefore, the anonymization process in DAPHNE Data Cloud hasn’t been decided yet. Towards the 3rd year of the project after the first prototype of the Data Cloud is developed, the anonymization technique will be decided. It will be probably based on known methods (such as k-anonymity).

3.4.3 Auditing

The IHE Audit Trail and Node Authentication (ATNA) Integration Profile provides the framework for auditing all the relevant auditable events. Events concerning Protected Health Information (PHI) use should be recorded and transmitted to a repository where they can be monitored to detect indications of inappropriate activity. In addition, ATNA provides node authentication during communications to provide authorization, confidentiality (optional), integrity and authentication for communications transferring PHI data.

As in the case of consents, it was decided to adapt a simple and proprietary mechanism for auditing in DAPHNE Data Cloud. This is mainly motivated from the current ecosystem of DAPHNE which is isolated from existing systems in the medical domain with no need to maintain a centralized audit repository. However, future work on the Data Cloud must leverage these standards and adapt the proprietary auditing mechanism into a standardized method that can be easily integrated with medical systems.

3.4.4 Communication

The communication with the Data Cloud is achieved is by using a secure HTTPS connection (TLS). All information exchanged using the HTTPS connection is encrypted, allowing the systems to securely exchange authentication tokens and measurement values. Transport Layer Security (TLS) is recommended for internal and external interfaces to provide confidential communications for protecting DAPHNE assets. TLS protocol provides an encrypted communication between the different components.

4 Open Middleware

The Aggregator is the application that runs on an Android mobile device, which collects, processes and uploads the data from DAPHNE sensor and movement devices to the DAPHNE Data Cloud. The Aggregator is based on the Open Middleware [4], which is able to support existing commercial third party sensors. To address DAPHNE needs additional functionality was added to the Open Middleware by the Aggregator, to support the unique sensors that were developed for DAPHNE.

The Open Middleware supports a wide range of Bluetooth Low Energy (BLE) standard services that are defined in the Continua Design Guidelines. This means that commercial sensor devices that are compliant with Continua can immediately and seamlessly make use of the Open Middleware and connect the DAPHNE Data Cloud. However, to support the specific and proprietary sensors developed in the DAPHNE project to address the unique requirements of DAPHNE, a set of proprietary BLE services have been added to the Open Middleware by the Aggregator, as they are not supported by the standard services.

The Open Middleware acts as the interface between any Continua sensor and the DAPHNE Data Cloud, handling tasks such as data collection, user authentication and authorization, data buffering and data forwarding (see Figure 3).

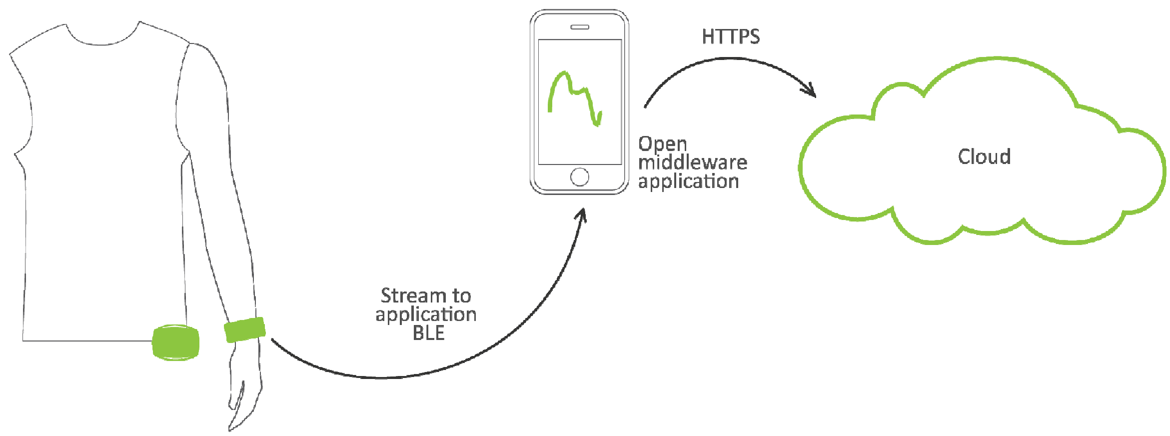

Figure 3 Communication Methods of the Open middleware

The Open Middleware is fully implemented and supports all the standards that are described below.

As described in D3.2 [4], the architecture of the Open Middleware has been divided into three layers; the service layer, the business layer and the data access layer.

The service layer handles all interaction with external entities, whether these entities are human beings (end user) or machines (sensor device, cloud server).

The business layer contains the domain-specific modules, defining algorithms to process the sensor raw data, handling DAPHNE specific authentication token management and similar tasks.

The data access layer acts as an interface between the business layer and the internal database.

Only the service layer interacts with external components and therefore the use of standards is relevant only to this layer. The service layer supports the following standards:

4.1.1 Bluetooth Low Energy (BLE)

The Open Middleware connects to a third party sensor via Bluetooth Low Energy (BLE) according to the recommendations from ITU-T H.810 [8]. BLE is the most advanced version of Bluetooth, which focuses on minimal energy use. BLE is ideally suited for streaming sets of (measurement or processed) data during an extended period of time.

4.1.2 Bluetooth Low Energy (BLE) security

The Open Middleware supports the strongest security mode and level (security mode 1 and level 3). However, it is possible to send data that requires a lower security level over a connection that is currently using this level of security. According to this security mode and level, the sensor needs to use bonding and pair with the Open Middleware authenticated. The pairing process is done with a 6-digit numeric passkey. Other methods of pairing can be added in the future (if needed). The process of bonding, using a 6-digit passkey, prevents unauthorized individuals from exchanging information with the sensor. Once bonded, the BLE connection between the sensor and the Open Middleware is encrypted, preventing eavesdropping and man-in-the-middle attacks.

4.1.3 Continua Design Guidelines (CDG) profiles

ITU-T H.810 defines the Continua Design Guidelines (CDG) which contains specifications to ensure the interoperability of devices used for applications monitoring personal health.

The Open middleware developed in the DAPHNE project supports a range of CDG profiles as Blood Pressure and Heart Rate (the full list is presented in D3.2 [4]). With these profiles the Open Middleware supports Continua compliant devices out-of-the-box. Sensors that use other (proprietary) profiles are not supported by the Open Middleware by default, but these services can be added if required.

The devices developed in the DAPHNE project, the Sensor device and the Movement sensor, include data types for which no Continua profile has been defined yet. Therefore the sensors cannot be certified under the Continua standard. As explained above, the Aggregator supports these proprietary profiles. The services that are not supported in the CDG and necessary for the DAPHNE sensors are:

- Daphne Sensor Accelerometer
- Daphne Sensor Gyroscope
- Daphne Sensor Galvanic Skin Response
- Daphne Sensor Heart Rate Service
- Daphne Sensor Temperature
- Daphne Sensor Time Service

4.1.4 JSON and REST

All the interactions between the Open Middleware and the Data Cloud are secured (as specified in section 3.4.4) and done with JSON messages and REST APIs (see section 3). The Android environment, in which the Open Middleware is built, has native support for the JSON data format. The object-oriented Android programming language allows objects to be directly translated into JSON format and vice versa. For the REST APIs, the Open Middleware has to specify the required action and resource.

5 Summary and future work

The goal of this standardization report is to coordinate all the activities related with standardization, to maximize the impact on health and expenditure. The main standardization activities that are described in this report relate to the collection of data generated by different sensor devices (aggregation layer) and uploaded to the Data Cloud, to provide a solution that can be widely adopted in medical institutions. Special attention is put on security standards to support an end-to-end secure communication while complying with legislation and increasing usability and seamless integration.

The standards that are supported for use in DAPHNE solution are the following:

Data Cloud

- Data – JSON and HL7 CDA R2
- Messaging exchange framework - REST
- Interoperability – Coding systems as SNOMED-CT, LOINC, UCUM, FHIR and ISO 8601 time format
- Communication - TLS

Open Middleware

- Communication – Bluetooth Low Energy
- Security - Security mode 1 and level 3
- CDG profiles – Generic Access, Current Time Service, Glucose, Health Thermometer, Device Information, Heart Rate, Battery Service, Blood Pressure, Weight Scale and Continuous Glucose Monitoring

The first prototype of DAPHNE platform is planned for M24 and should include all the above standards except of the HL7 CDA R2 which will be supported only in the final prototype version in M30.

Based thereupon the usage of standards, the next version of the report will examine and drive the technological transference with European projects. It will also report on the lessons learnt and recommend on further activities to promote and contribute to relevant standardization development bodies and initiatives.

References

[1] *Daphne Document of Work (2013)*. All Daphne partners

[2] *D8.2 Standarization Report (2014).* Roni Ram. Daphne

[3] *D2.7 Daphne System Architecture final design and development (2015)*. Carlos Marcos. Daphne

[4] *D3.2 WBAN Architecture and Open Middleware (2015).* Susan van Wissen. Daphne

[5] *D6.1 Data provider API (2015).* Roni Ram. Daphne

[6] *D6.2 Data-as-a-Service API (2015).* Roni Ram. Daphne

[7] *D6.3 Data cloud first prototype (ongoing).* Roni Ram. Daphne

[8] *ITU-T H.810: Interoperability design guidelines for personal health systems* [Online], https://www.itu.int/rec/T-REC-H.810

[9] *Big Data: Big today, normal tomorrow, ITU-T Technology Watch Report (November 2013)* [Online], http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000220001PDFE.pdf