



OLA – Organizational Life Assistant

FOR FUTURE ACTIVE AGEING

D3.3 Security and Privacy Infrastructure



Project Identification	
Project Number	AAL 2014-076
Duration	38 months (1 st March 2015 – 30th April 2018)
Coordinator	Carla Santos
Coordinator Organization	Inovamais, S.A. (INOVA+)
Website	http://project-ola.eu/

Document Identification	
Deliverable ID	D3.3 Security and Privacy Infrastructure Specification
Version/Date	Version b / 31.05.2017
Leader of the Deliverable	Marco Duarte, INOVA+
Work Status	Finished
Review Status	Accepted

Deliverable Information	
Deliverable Description	Specification of software components that relate to security and privacy mechanisms / compliance.
Dissemination Level	Confidential (Consortium Members + Commission)
Deliverable Type	Report
Original Due Date	M26

Authorship & Review Information	
Editor	Marco Duarte (INOVA+)
Partners Contributing	ISCTE-IUL
Reviewed by	Luís Dias, Fernando Pinto (ISCTE-IUL)



Table of Contents

1	Executive Summary.....	4
2	Document Context.....	5
2.1	Role of the Deliverable	5
2.2	Relationship to other Project Deliverables	5
2.3	Target Audience of the Deliverable	5
3	Project Description.....	6
3.1	General Description	6
3.2	System Description.....	7
3.3	Status and Future Developments	8
4	Security Specification	9
4.1	Overall Architecture	9
4.2	Authentication	10
4.3	Authorization.....	13
4.4	Auditing.....	15
5	Azure AD.....	16
5.1	Authentication on Azure AD	16
5.2	Authorization on Azure AD	16
5.3	Auditing on Azure AD.....	17
6	Privacy Specification	18
7	Conclusion	22
	References	23
	List of Figures.....	24
	ANNEXES.....	25
	1 – Data Access Permission Table.....	25
	2 – Sensor Data Structures	28



1 Executive Summary

This deliverable documents the specification of the security infrastructure that is present on the data platform of the OLA project, which is based on three pillars / concepts: authentication, authorization and auditing. These are very much influenced by the work done previously in T1.4, which researched and analyzed the requirements needed to put in place for the ethical and privacy compliance of the project. It also lays the path for the general security-related guidelines that have to be followed by other components, such as software modules.

2 Document Context

2.1 Role of the Deliverable

The role of this deliverable is to specify how the implementation of the OLA platform will comply with the security and privacy-related guidelines that were found important within the scope of the preliminary tasks performed in the project. This deliverable is a detailed / deeper view of the security-related components that are already presented in other technical documents.

2.2 Relationship to other Project Deliverables

Deliv.	Relation
D1.4	Title: D1.4 Ethical, Privacy and Legal Considerations D1.4 is the most fundamental input deliverable for the production of this very document, because it entails the European and country-wide guidelines that are in place for the management of private data, as well as the required security-mechanisms to make sure privacy is maintained.
D3.1	Title: D3.1 Design specification and integrated architecture Although D3.1 provides a comprehensive specification for the architecture behind the OLA project, this deliverable will overwrite and fill in the blanks for the security-related components mentioned in that document, as they will be less thoroughly detailed given the existence of this deliverable. Plus, some links with the other components mentioned in D3.1 will also be made here.

2.3 Target Audience of the Deliverable

The primary audience of this document is the group of technical partners, the team who will do the actual software development work. This document is a public deliverable. Still, it is mainly intended for the project partners and the European Commission services; thus, the document will be made public, but not specifically disseminated on a wider scale.



3 Project Description

3.1 General Description

This project aims to offer an answer to the societal challenges by providing an innovative Organizational Life Assistant (OLA), a virtual presence that supports instrumental activities relating to daily living needs of older adults allowing them to be more independent, self-assured and to have a healthier, safer and organized life, while easing caregivers work.

OLA will mediate and facilitate interaction (communication and collaboration) between senior citizens and their informal caregivers or other services or professionals, through technological devices such as standard computers, mobile devices (tablets) and home automation modules. These ICT (Information and Communications Technology) devices will be based on an innovative multimodal model, embracing various physical/healthy and cognitive characteristics of the older adults and will be specifically oriented to increase the level of independence of the elderly, by supporting the possibility of carers' assistance remotely and by improving the accessibility to existing services on the Web, such as on-line shopping services.

Moreover, the OLA will also provide personalized well-being and safety advices to older users in order to avoid unwanted age related health and safety situations in their own home. Such a well-being and safety advisor makes uses of a combination of user information that is collected (personal physical/health and cognitive characteristics) and extracted through emotion recognition and various sensors.


OLA also addresses a major issue that elderly face related to memory degradation and gradual decreasing of their cognitive capabilities, enabling them to remember primary health care and fiscal obligations (e.g. personal hygiene, medical and tax compliance) or helping them to find everyday items such as eyeglasses, wallet or keys. It is based on speech dialogue interfaces and space and object reconstruction and classification to capture and store daily routines and their related contexts.

The primary end-users are the big group of 65+ adults living alone with or without light physical or cognitive age related limitations, who need support from care systems. Secondary end-users are both formal and informal caregivers from public or private sectors, supporting them to cope with the increased demand for care.

3.2 System Description

OLA addresses specifically the following main issues:

- **Well-being advisor:** based on the combination of the collected user information (personal, healthy characteristics) and user interaction information extracted through emotion recognition, sensors settings and contextual recorder capturing the routines as done by the older adult) the system will propose to the older adults personal advice adapted to their situation contributing to their preservation and well-being status in home environment. In case of risk (e.g. irregular heart rate, extreme fatigue) the system may ensure an alert to a local medical emergency service.
- **Collaborative care organizer:** based on the ISCTE-IUL and LM knowledge of developing human-computer interaction platforms (HCI), OLA will provide online care collaboration between family and professional caregivers, by enabling a local care network to communicate, access sensor data, and coordinate care tasks. With the OLA assistant, seniors will be able to actively participate in the care organization through voice, even when they are unwilling or unable to use traditional web applications.
- **Safety advisor:** based on the combination of collected user environment information through real-time analysis and augmented reality settings, the system will propose suggestions of environment changes that interfere with accessible paths and provide alerts for intruders or other situations that can create hazard situations. In case of risk (e.g. checking intruders or fire), the system may contact local emergency services.
- **Every day instrumental daily living activities memory support:** the system will anticipate medical and fiscal compliances, remember primary health care and food requirements and could help elderly to find displaced everyday items.
- **Environment analysis:** algorithms for real-time object recognition and scene understanding will be developed based on a number of inputs (i.e. 3D object and space reconstruction by using time-of-flight and augmented reality technology) in order to analyze and decide which action to be taken in order support the elderly by suggesting environment changes and providing hints/advice for safety and accessible environments.
- **Multimodal interaction for elderly:** An adaptive organizational life assistant, a virtual presence will be developed in order to facilitating communication and collaboration between older-adults and informal caregivers or other services or professionals. This will be a user-friendly system that uses multimodal approaches based on non-invasive



and minimally obtrusive technologies (i.e. speech, silent speech, touch, gestures, RGB-D sensors).

The overall OLA system will be an easy to download and install software making use of multimodal integrated settings. OLA is in essence a service that enables the elderly user to reduce the demand of care through prevention and self-management, while at the same time also facilitating the supply of formal and informal care assistance.

A series of well-selected use cases where older adults have been supported by caregivers and care professional services will be developed, as well as pilots representing different use cases. Care units will use the system over a one year period. A new evaluation approach will be used during the pilots, investigating up to which point the OLA services alleviate caregivers support and maintain, or even improve the self-management, health and safe lifestyle of the older adult at home.

3.3 Status and Future Developments

This is the second and final iteration of the document, following the specifications of the implemented version, presenting the security-related software components developed, focused on registration, authentication and auditing of the data.

4 Security Specification

The first part of the deliverable will deal with the security-related mechanisms employed into the OLA architecture. Although they are part of the means used to comply with the privacy requirements, they are going to be presented as autonomously as possible, while the next chapter will specifically deal with the privacy-related issues. Also, this chapter will not delve into any security-related mechanisms that may be indirectly present or applied within the scope of the project, such in the usage of sensors / wearables (proprietary security mechanisms), before OLA's app is opened in the tablet device (mobile operating system security mechanisms), etc.

4.1 Overall Architecture

For an adequate understanding of how the security software components relate to each other and how they are integrated into the rest of the OLA architecture, it's important to remind the reader of the complete technical diagram of the platform:

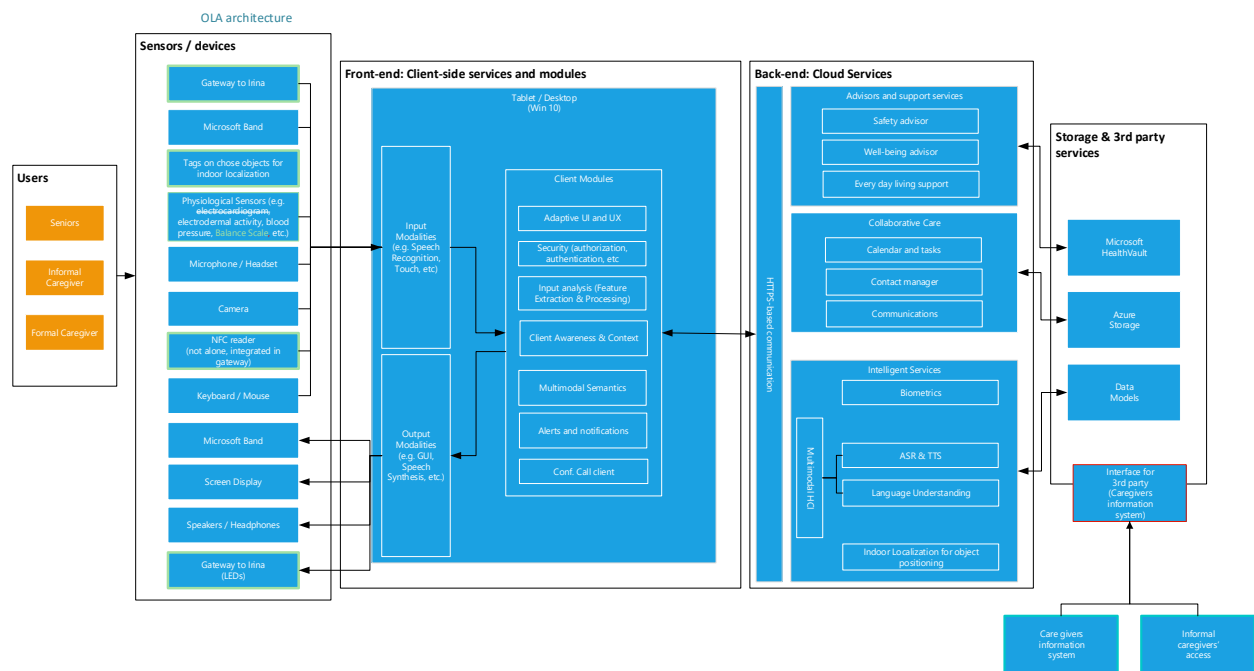


FIGURE 1 – OLA ARCHITECTURE

In the next diagram, the security-related components are highlighted:

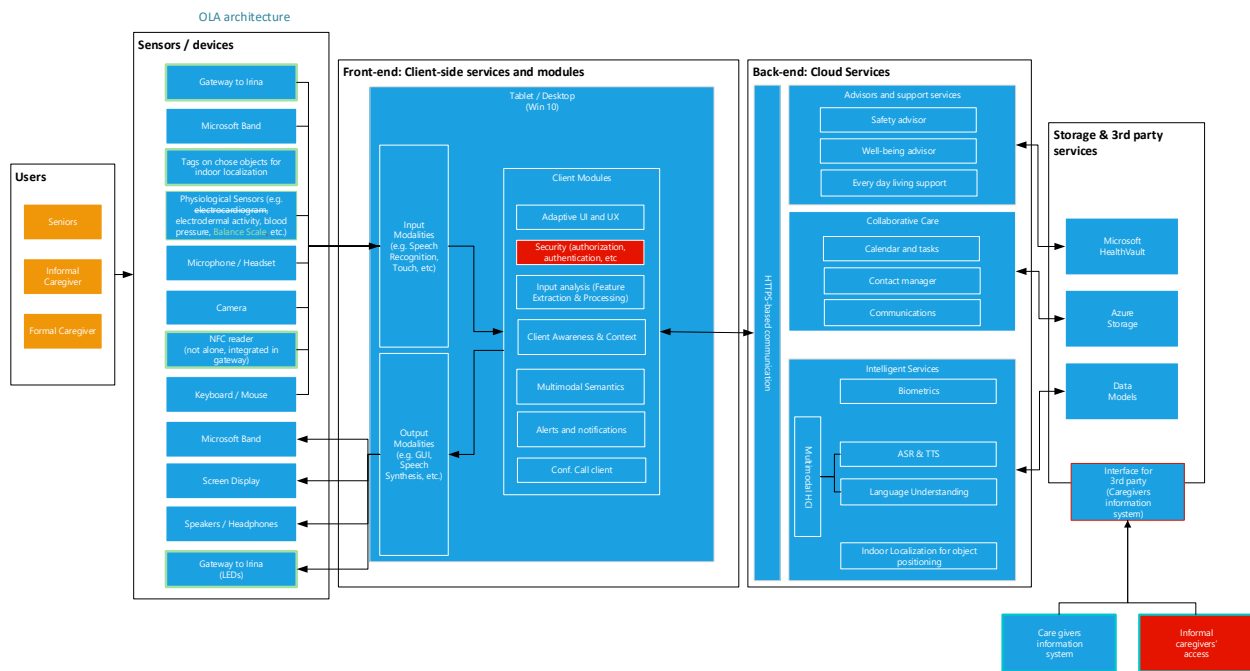


FIGURE 2 – OLA ARCHITECTURE – SECURITY HIGHLIGHTED

Security is present on the architecture of OLA through the means of three specially-tailored subcomponents, which are present also on different component groups of the overall architecture: Authentication (Front-end), Authorization (Back-end) and Auditing (Data).

4.2 Authentication

This component makes sure that any person interacting with the OLA platform is registered within the system and is indented to actually be using it. This person may pertain to any of the roles foreseen by the project, such as the elderly, an informal caregiver (including family) and formal caregiver. The authentication itself is made through the insertion of two pieces of information: username and password. After this process is cleared, the user is free to use the application within the scope of a session that will always identify him / her as the author of actions made forward, as well as show information that only regards him / her. Following is the information flow of this process:

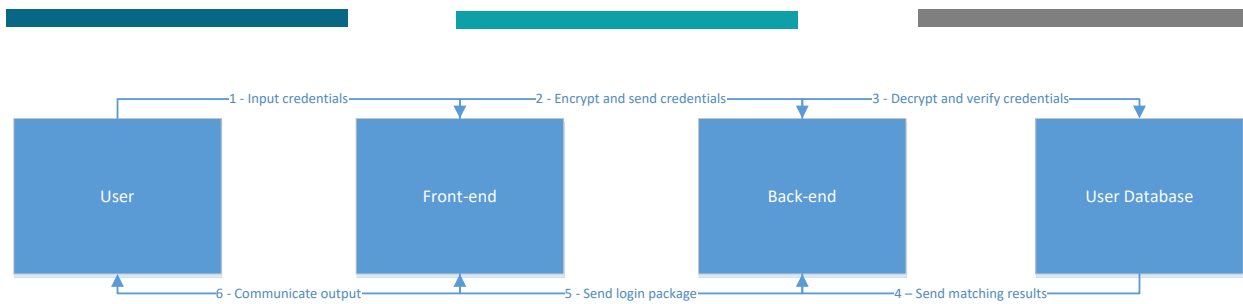


FIGURE 3 - AUTHENTICATION

The steps undertaken are the following:

1. Input credentials

The initial step of the process sees the user input his / her credentials into the login form; since this is a type of interaction the user has with the application, this can be done using a variety of modalities using the interaction framework. After that, the user acknowledges the sending of this information to the server with the purpose of validation and entering the actual homepage.

Technical details:

The username shall be something somewhat familiar to the user (especially for the elderly with memory issues), but that doesn't translate directly into actionable information about him / her (such as first + last name). A solid suggestion is for the username to be the internal number associated with that user within OLA (which will have at most 2 digits), or a combination of that with one of the names. Although the username can be the same as that number, as far as the database goes, these are different fields, since the username is kept in an encrypted state. For the (in)formal users of the application, the complexity of the username may be more enforced. This information will be managed by the consortium and provided to the users prior testing.
 Example: 23.
 Example: Joana23.

The password must have at least 8 characters, contain both letters and numbers, lowercase and uppercase characters, a special character and be kept by the users in a safe place (in case it's complex enough for an elderly person to remember).
 Example: Nachos21!

2. Encrypt and send credentials

Since user data (especially sensible data such as this) will be transmitted through means that unintended people can try to hack into, this information is encrypted prior to be sent in the user device, even if the transmission itself it also protected using other methods (see next).

Technical details:

The decryption key will be created by the consortium upon the middleware implementation and will be referenced by the source-code. Example: fh3843hg9403j73078j2039734j2
All transmissions between the main app and the back-end are made over an HTTPS connection (using SSL/TLS), which uses a security layer to encrypt the whole data sent back and forth. Only the sender and last destination of the message are able to read its contents, through the means of negotiating the usage of a genuine security certificate, which has to be acquired upon implementation (for example by Symantec).

3. Decrypt and verify credentials

The decryption of the overall message happens automatically at the server side (because it will by default possess and acknowledge the same security certificate); however, it still needs to decrypt the actual login data that was encrypted in a special way before (and using the same key). After this, it will consult directly the database to see if there are any username – password matches.

4. Send matching results

The results of the matching process are sent back to the login mechanism on the server-side. These have the format presented next.


Technical details:

Result	True False
User	User information pertinent to create the session: Id, Name, Last Login Date, Usage Token, Usage Token Expiration

5. Send login package

This step is optional and is only executed if the Result above is true, otherwise an empty login package is sent back to the interface. If a user was found, it is current usage token (a value that validates its usage of the services for a limited time window) is evaluated in terms of the expiration date. If that date has passed, another one is generated and the database (and login package) updated; if not, the login package is ready to be sent back to the user.

6. Communicate output



The interface receives the output and acts accordingly: if the login is unsuccessful, the procedure is asked to be performed again; if the login is successful, the app caches the login package and enters into the main homepage (where it will load other types of data).

4.3 Authorization

This security mechanism makes sure that accesses to the back-end's data, for whatever reason they are made, are authorized (using the login package and token information presented earlier). The very access to this security mechanism is also made within the scope of an HTTPS connection and certificate, as already explained. Furthermore, it also checks if the different types of retrieved or queried data are in line with the permissions of the user behind those communications. Following is the checklist made by this component (in which a single failed step cancels the whole request):

1. Check if request possesses token information (this is already after the request is considered valid in its format, otherwise it doesn't even get to this step and it's cancelled altogether);
2. Check if token information is valid (matching with database);
3. Check if accessed data pertains to the user impersonated in the request or to a list of people at the care of him / her;
4. Check if the type of access (add, delete, update, etc.) is allowed; for example, only a formal caregiver should be allowed to cancel or deactivate medication intake (check Annex 1 for the complete list of permissions);
5. If the access is of the type "Health Measurements" or "Activity Measurements", the system will employ an additional checklist to make sure that this data is valid according to the user and hasn't been tampered with (this checklist is presented next). It's important to mention that this data was already the subject of the "Physiological Data Preprocessing" client module (not discussed here); however, the lack of compliance of some of the steps of this checklist (especially 2 and 3 below) doesn't forfeit the actual introduction of the new data but rather the signaling that such information was added under special circumstances that need to be analyzed (this accounts for when the communication capabilities of the devices fail or when the user feels that an extra measurements is necessary, for example);
6. Perform the actual request.

Measurements Security Checklist:

1. If the measurement comes from a sensor:
 - a. Check if the sensor pertains to that person;
 - b. Check if the sensor is currently activated / being used;
 - c. Check if the health parameter can be measured by that sensor.
2. Check if the health parameter is currently being recorded;
3. Check if the moment of measurement coincides with the scheduled, given a time margin for error.
4. In the case the user pertains to a shared environment, using the NFC board, it is necessary to clearly identify the user in order the storage of health data read can be appropriately stored of the correspondent senior.

Data structures being monitored:

Users (2)	Id, Usage Toke, Role Id
Care Relationships (2,3)	Caretaker Id and Cared Id
Security Permissions (4)	Role Id, Resource Type Id, Permissions
User Sensors (5)	Sensor Id, User Id, Status
User Parameters (5)	User Id, Parameter Id
Sensor Parameters (5)	Sensor Id, Parameter Id
Sensors (5)	Sensor Id, Sensor Serial Number
Scheduled Measurement (5)	User Id, Parameter Id, Date, Time

Resource Types

1	Appointments
2	Medication
3	Diseases
4	Demographics
5	Health Measurements
6	Activity Measurements
7	Contacts
8	Notes
9	Location
10	Help Registry
11	Other Reminders

Roles

1	Elderly
2	Informal caregiver family

3	Formal caregiver
---	------------------

Permissions

1	INSERT
2	UPDATE
3	DELETE
4	SELECT

4.4 Auditing

This mechanism exists within the back-end part of the framework to register all of the accesses made to the platform's data, i.e. functionally it is executed after the Authorization step is cleared (this means that unintended accesses are not saved). Auditing allows the OLA technical partners to analyze and monitor if all accesses are made within the assumed normal security conditions of the environment it is put in, while also to comply with any data requests made by the stakeholders / users (for example to check if a particular data was inserted manually or through a sensor) and legal requirements. Following is the data structure of the auditing information:

Id
Timestamp
User Id
Secondary User Id (only used if an access is made towards data of another user)
Resource Type Id
Resource Id
Access Type Id
Automatic Id (only used if the access is made through an automatic agent, such as a sensor)



5 Azure AD

Microsoft offers a collection of integrated cloud services for developers to build, deploy and manage applications through a global network of data centres. Based on centralized policy and rules, Azure Active Directory (Azure AD) is a comprehensive, highly available identity and access management cloud solution. Azure AD is the service used by OLA for data storage in a reliable and robustly secured service.

IoT Hub enables OLA devices to be connected in a trustful and easy manner, establishing Bi-directional communication with the IoT devices with Microsoft Azure. IoT Hub authenticates on a per-device basis, assuring OLA solution retaining confidentiality of both cloud-to-device and device-to cloud messages.

The Authentication, Authorization and Auditing in Azure AD is explained below.

5.1 Authentication on Azure AD


The user registration is made by a super admin account in a management portal. A user profile containing pseudonymous data and an access account on Azure AD are both created. Simultaneously, an access account (user/password) is also created on the OLA's frontend app support server, if the caretaker or the elderly have a package to support the application.

5.2 Authorization on Azure AD

The Authorization on the consuming side is possible via a set of access rules defined by the platform's super admin on the management portal, where this user specifies which caretakers have access to which gateways/sensors. This information is used by the historical and real-time APIs to restrict data access; if the caretaker does not have permission to access the data he/she receives a forbidden notification.

Authentication on the gateway side is possible via a set of access credentials that are created on the IoT hub service (these are unique to a gateway). These are then setup on the gateway. An existing user in the system (typically an elderly user) is assigned as owner of the gateway, and the authorized devices of the gateway are also setup.

Data publishing authorization is possible via the gateway identification (which is obtained directly from the data source that IoT hub sends, based on the authentication credentials used by the gateway), and on the device Id and user Id the gateway sends on its



measurement messages. If the gateway is not authorized to publish using that device and user Id, the message is rejected, otherwise it is forward by the platform to all authorized consumers.

The gateway itself also filters devices based on its Mac addresses. These are configured in the management portal, during the gateway device setup process. This list is retrieved by the gateway during its initialization process, after it is authenticated with the IoT hub, and is periodically updated on demand, by the gateway, or by forcing an update from the management portal.

5.3 Auditing on Azure AD

The Health data is authenticated with the Azure AD credentials. The auditing workflow is managed by Azure AD's process. The process is initiated on OLA app with a set of Azure AD provided ids and a screen is presented to the user following Azure AD's workflow; at the end, an access token is retrieved, which allows the system to know the Azure AD user's Id. With this Id, we can cross-reference the health metadata database and match perfectly the health data with the proper user.

6 Privacy Specification

For the privacy compliance inside the OLA project, this deliverable will resort to the analysis made within the scope of task T1.4 - Ethical, Privacy and Legal Considerations, whose deliverable contains the mechanisms necessary to be implemented or somehow followed for the safekeeping of the user's privacy. With that said and from the output of that task, here are the technical means that will be employed specifically towards the compliance of privacy guidelines:

The separation between demographic data and health data


Legislation regarding this topic mentions that this separation needs to be "logical", which is an open concept to say the least. What is clear from reading those articles, however, is that when accessing health-related records, they cannot be easily linked with the owner of those records in the same view / data structure; this translates the separation into a more actionable task. For that purpose, in OLA all of the health-related data structures (database tables) will not include any demographic data whatsoever, being tied to the people using an unrecognizable identifier known only to the system. Here's an example of a data structure for blood pressure:

Id	3c003491-58dc-4788-9312-3f03e2f85994
User Id	34 (or a GUID too)
Value1	117
Value2	76
Timestamp	2016-08-03T15:58:45+00:00
Automatic Id	3c003491-58dc-4788-9312-3f03e2f85993
Parameter Type ID	6

As can be seen above, a look through any health register such as this doesn't provide any information whatsoever about the user behind that information. Next is an example of the demographic record of a user:

Id	34 (or a GUID too)
Age	67
Name	Maria
Gender	Female
Location	Lisboa

Besides the fact that, in terms of purely-demographic-related information, the project doesn't need to have access to a lot of data (other information, such as allergies and mobility impairments, are not considered demographic), it can also be seen above that



a read through an elderly record such as this doesn't provide enough information to uniquely identify anyone.

The demographic data is only stored in a system managed by an authorised 3rd party entity (e.g. CKPT). During the project life time, the pilots' activities will be running internally, i.e. remotely. Nevertheless, in the future the objective for this operation is to be implemented at one authorised entity.

The delete of demographic data is for integrity reasons, a soft delete, but it can be enforced an enforced 'hard delete' through a flush on the records that were subject to a 'soft delete'. On the other hand, the health data can be only removed directly from the database, also due to integrity reasons.

To further display how private data is not used or even retrieved from all devices used in the project, Annex 2 provides a complete list of data structures transferred from hardware models.

The anonymization of the health data

Since demographic data is a means to identify someone and above it was already shown how the project separates the two types of information, this requirement is achieved likewise using the aforementioned method. It's also important to clearly state that, besides demographic data (which will be marginally used anyway), not any type of uniquely-identifiable code of number will be used, such as identity card, IRS number, social security number, healthcare number, etc.

The system administrators (admins) do not have access do not have access to this information, while the super admins does not have access to this, since they are the ones who performs the system maintenance. Once the project life cycle ends, similar to the access of demographic data, the health data will be accessible for the authorised 3rd party entities which will have access to this type of data.

The application of security mechanisms for the transmission of data across the wire, wirelessly or using public networks (such as encryption)

This was already discussed before as part of the default security mechanisms of the platform.

The application of specific security criteria for the usage of passwords

This was already discussed before as part of the default security mechanisms of the platform. However, it needs to be disclosed that the specific criteria that is demanded

by some of the legislation was tighter than we had anticipated (and originally had created), so we had to change:

Original criteria for passwords	Required criteria for passwords
8 characters	8 characters
Numbers and letters	Numbers and letters
	Lowercase and uppercase letters
	Special characters

The application of backup strategies

The backup of the information being managed by the OLA platform is a feature that is automatically performed by the infrastructure where it will be hosted (Microsoft Azure); along with that process, other advantages or features are witnessed that are related to the privacy aspect of the project:

- Lack of (or extremely secured) physical access to servers (thus turning obsolete all physically-related privacy guidelines);
- Automatic replication / farming of data across servers from all around the world (relates to this very mechanism being discussed);
- Logging of all accesses made through web interface (it's not the intended way for users to access their data);
- Optimal record of uptime, fault-free environment and recoverability.


The application of logging / auditing strategies

Similar in nature, the Auditing security specification presented above already accounts for this requirement. However, logging procedures (identifying the user responsible for that action) will be implemented all-around within the software, but especially in the entry and exit points of components; following are some of the scenarios foreseen:

- Navigation between app sections;
- Calls made to the back-end services;
- Speech-recognition attempts;
- Sensor measurements;
- Access to health-related information.

The naming of the pilot managers / data controller

A data controller, which will be responsible for the acquisition of the data (in case of manual modes), the presentation of the informed consents and communication with the end-users. Within the project OLA, these data controllers will be the pilot managers within



the scope of each geographical territory where trials will be run: Portugal, Hungary and Sweden. During all the pilot activities the following pilot managers will be signed to the respective country:

- Portugal: Marco Duarte (INOVA)
- Hungary: Dénes Perenyi (BZN)
- Sweden: Morgan Fredriksson (LM)



7 Conclusion

The team behind OLA feels that the aforementioned security and privacy-related specifications adequately cater and fulfill the legal requirements that were previously researched.

According to the requirements collected in D1.1, this deliverable can confirm a robust security platform, where the seniors' data can be safely stored and users be able to recognize a trustful and secured solution (requirement #13), the prototype enables the assessment of Health data of the persons in their care at any time (requirement #19), the health data of the patients is shared to the caregivers which are assigned to them (requirement #32) and the information can be managed at the caregivers' portal (requirement #29).



References

1. D1.4 ETHICAL, PRIVACY AND LEGAL CONSIDERATIONS (INOVA+), 2016
2. D3.1 DESIGN SPECIFICATION AND INTEGRATED ARCHITECTURE (BZN), 2016



List of Figures

Figure 1 – OLA Architecture	9
Figure 2 – OLA Architecture – Security highlighted	10
Figure 3 - Authentication	11

ANNEXES

1 – Data Access Permission Table

Role	Resource	Permission
Elderly	Appointments	INSERT SELECT
	Medication	SELECT
	Diseases	SELECT
	Demographics (only UPDATE and SELECT are applicable here)	SELECT
	Health Measurements	INSERT SELECT
	Activity Measurements	INSERT SELECT
	Contacts	INSERT SELECT UPDATE DELETE
	Notes	INSERT UPDATE DELETE SELECT
	Location	SELECT
	Help Registry	INSERT SELECT
	Other Reminders	INSERT UPDATE DELETE SELECT
Informal caregiver family	Appointments	INSERT UPDATE DELETE SELECT
	Medication	INSERT UPDATE DELETE SELECT
	Diseases	SELECT
	Demographics (only UPDATE and SELECT are applicable here)	UPDATE SELECT
	Health Measurements	DELETE SELECT
	Activity Measurements	INSERT

		UPDATE DELETE SELECT
	Contacts	INSERT UPDATE DELETE SELECT
	Notes	INSERT UPDATE DELETE SELECT
	Location	INSERT UPDATE DELETE SELECT
	Help Registry	INSERT SELECT
	Other Reminders	INSERT UPDATE DELETE SELECT
Formal caregiver	Appointments	INSERT UPDATE DELETE SELECT
	Medication	INSERT UPDATE DELETE SELECT
	Diseases	INSERT UPDATE DELETE SELECT
	Demographics (only UPDATE and SELECT are applicable here)	UPDATE SELECT
	Health Measurements	DELETE SELECT
	Activity Measurements	DELETE SELECT
	Contacts	SELECT
	Notes	SELECT
	Location	SELECT
	Help Registry	UPDATE DELETE SELECT



	Other Reminders	SELECT
admin	users	SELECT
super admin	users	SELECT INSERT UPDATE DELETE

2 – Sensor Data Structures

Hardware	Data Structures
RGB-D Camera Models: Microsoft KinectOne*	DATE TIME VISUAL AND GEOMETRIC REPRESENTATION OF THE PREMISES OF THE USER (without the presence of any humans) GESTURES (discarded upon translation into commands)
ECG* Models: to be developed.	DATE TIME P WAVE PR INTERVAL QRS COMPLEX J-POINT ST SEGMENT T WAVE CORRECTED QT INTERVAL U WAVE
Weight Scale Models: Taidoc TD-2551	DATE TIME WEIGHT BMI
Blood Pressure Models: PressureTel, Taidoc TD-3250H, iHealth Wireless Blood Pressure Monitor BP5, Beurer BM70	DATE TIME SYSTOLIC DIASTOLIC PULSE RATE
Glucose Models: Taidoc TD-3250H, iHealth Wireless Smart Gluco-Monitoring System BG5	DATE TIME GLUCOSE
Oximetry Models: NONIN OnyxII SPO2, iHealth Wireless Pulse Oximeter PO3	DATE TIME PULSE OXIMETRY (SO2)
Body Balance Models: to be developed.	DATE TIME CENTER OF GRAVITY SAMPLE RATE
Microphone / Headset	DATE TIME AUDIO CLIP (discarded upon translation into text)

Camera (regular)	DATE TIME VISUAL FEED (is used in real-time for security and communication purposes, but not recorded due to storage space issues)
Eye tracker*	DATE TIME GAZE POSITION (discarded upon translation into screen region)
Keyboard / Mouse / Touch	
Multisensorial Wearable Models: Microsoft Band 2	DATE TIME HEART RATE (OPTICAL) CALORIES BURNED NUMBER OF STEPS TAKEN ATMOSPHERIC PRESSURE GEO POSITIONS DISTANCE SPEED CONDUCTIVITY OF SKIN ULTRAVIOLET LIGHT LEVEL

*Not applicable means that will only be part of research, i.e. models that will not be tested in the pilots and also not integrated in the final version of the platform.