PrivAcy pReserving Infrastructure for Surveillance

Deliverable D6.1
Biometrics Use Case Description

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D6.1
Title:	Biometrics Use Case Description
Version:	v1.0
Date:	13/6/2014
Confidentiality:	Public

Contributors: María Saornil (VT)
Francisco J. Rodríguez (UMA)
Marioli Montenegro (UMA)
Zhendong MA (AIT)

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Table of Contents

Document History

Version	Status	Date
v0.1	First draft of ToC	12/3/2014
v0.2	Contribution to section 2.1 (VT)	3/4/2014
v0.3	Contributions to sections: 2, 3, 4 and 5 (VT)	10/4/2014
v0.4	First draft of use cases (VT)	15/4/2014
v0.5	Contribution to sections: 1 and 5 (VT)	25/4/2014
v0.6	Update of system requirements of section 5 (VT)	5/5/2014
v0.7	Update of sections 3 and 5 (VT) Contribution to section 2.2 (UMA, VT)	22/5/2014
v0.8	Contributions to section 6 (VT, UMA, AIT)	5/6/2014
v0.9	Update of section 6 (VT)	6/6/2014
V1.0	Revision of the document (Namur, Thales, VT)	13/6/2014

Approval		
	Name	**Date**
Prepared	Visual Tools, AIT, UMA	13/6/2014
Reviewed	Mathias Bossuet (Thales) Claire Gayrel (Namur)	12/6/2014
Authorised	María Saornil (VT)	13/6/2014

Circulation	
Recipient	**Date of submission**
Project partners	13/6/2014
European Commission	13/6/2014

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
APDB	Authorized People DataBase
DC	Depth Camera
ICT	Information and Communication Technologies
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PIA	Privacy Impact Assessment

RIS	Re-Identification Server
SALT	Socio-ethicAl, Legal, Technical
VPU	Video Processing Unit

Executive Summary

The main goal of the PARIS project is the definition and demonstration of a methodological approach for the design of surveillance systems optimizing the surveillance capabilities together with privacy protection and integration of the concept of accountability. For this reason, we define a framework called SALT (Social, ethicAl, Legal and Technical), and two use cases for its demonstration.

This document covers the work of tasks T6.1 and T6.2 in which one use case is described, to demonstrate the adequacy of the SALT Framework for the design of surveillance systems based on biometric technologies taking into account privacy and accountability from the start.

1 Introduction

1.1 Deliverable objectives and scope

Deliverable D6.1 covers the work of tasks T6.1 and T6.2, which have these objectives:

- The collection and characterization of biometric technologies for their integration in conceptual frameworks such as the SALT framework
- The definition of the SALT representation for biometric systems
- The definition of the biometric use case to be demonstrated, including the specification of:
    - Surveillance capabilities
    - Platform to be used
    - Elements needed for the use case
    - Evaluation criteria at the SALT framework level and at the design process level

This document deals with these issues as follows:

- The section 2 provides a description of biometric systems, including detailed information about the functional blocks and the components used to implement them. This information has been used to define the SALT representation of biometric systems, which is summarized in this section and also described in depth in deliverable D4.3.
- In the section 3, the scenario and the use cases covering the main stages of the lifecycle of a biometric system are defined.
- The section 4 presents an overview of the biometric technology selected for the use case and the initial composition of the biometric system.
- The section 5 summarizes the main requirements of the system that guide the design process, for both the biometric system and the SALT Framework.
- Finally, the section 6 details the criteria for the evaluation of the system at the design level and at the SALT framework level.

2 Integrating Biometric Technologies in Conceptual Frameworks

2.1 Technical and Functional viewpoint

The objective of this section is to provide a basis for the modelling of biometric systems. Thus, a description of a generic biometric system is proposed, including the functional blocks identified, the main components used in a biometric system and the main design criteria. The section also covers an initial risk assessment overview focused on the identification of risks affecting privacy at the design stage.

2.1.1 Functional Blocks involved in Biometric processing

As mentioned in D2.1, biometric systems use biometric data to perform the recognition of individuals for their identification, verification or categorization.

Whatever the purpose of the system is, the processing of the biometric information can be divided within the following functional blocks:

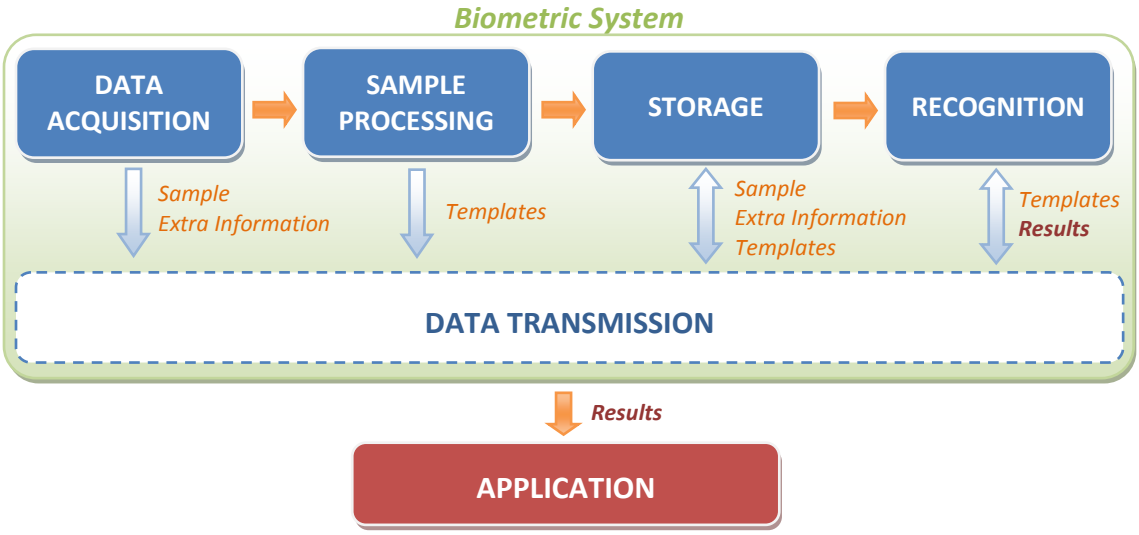

Figure 1: Functional architecture of a generic biometric system

2.1.1.1 Data Acquisition

This functional block deals with the collection of biometric data of an individual, also called *sample* or *biometric presentation*, and may also gather contextual information or other user information necessary for the matching phase.

The Data Acquisition block includes a component for data capturing and also the interfaces required to allow users to enrol or to be recognized by the system.

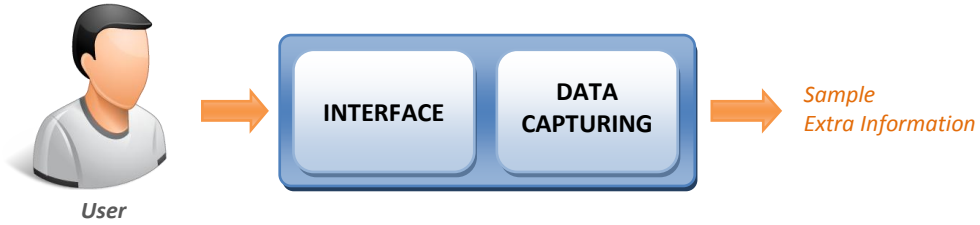

Figure 2: Functional architecture - Data Acquisition block

2.1.1.2 Sample Processing

It refers to the processing of biometric data to extract the specific *template* for the individual that is currently using the system.

In this block one or many **signal processing algorithms** are executed to prepare the biometric data for a better processing *(pre-processing),* extract the main features and generate the structured template depending on the biometric technology used.

It may also be required to implement **quality control mechanisms** to discard invalid samples.

Furthermore, **mechanisms for data fusion** may be necessary in multimodal systems to combine several inputs from the same sensor, inputs from many similar sensors or data from different types of sensors, to generate more complex and accurate templates and improve the reliability of the system.

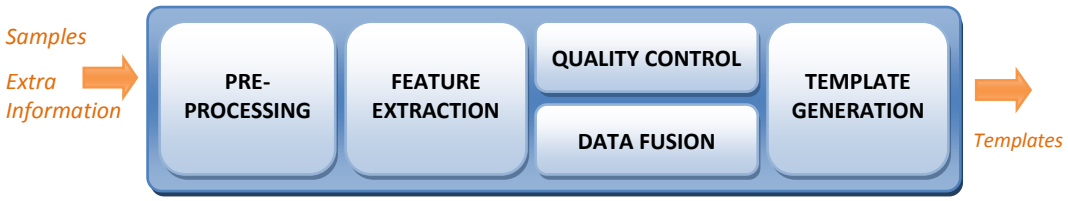

Figure 3: Functional architecture - Sample Processing block

2.1.1.3 Storage

The Data Storage keeps information of the individuals and the biometric processing in the system.

Different types of storage can be used, and the system can store not only the templates but also user information, context information or the raw samples.

Figure 4: Functional architecture - Storage block

2.1.1.4 Recognition

This block is responsible for the comparison of the information provided by the user at a certain moment with the data stored in the system in order to make a decision. The results provided by this block will be used differently depending on the application for which the biometric system is implemented.

The recognition task is performed by a **matching algorithm** that implements different types of comparisons depending on the mode of operation of the biometric system:

- *Identification*: find an individual in a database (1--> N, N: all templates stored)
- *Verification/authentication*: check if a person is who he or she claims to be (1--> 1)
- *Categorization*: check if a person belongs to a group (1--> M, M: all templates of a specific group)

Afterwards, the results of the comparison are filtered according to a defined policy to decide if the match is accepted or rejected. In the recognition process, other user information may be taken into account to consider a user recognized or not (e.g. use PIN in case of inaccurate results of template matching process).

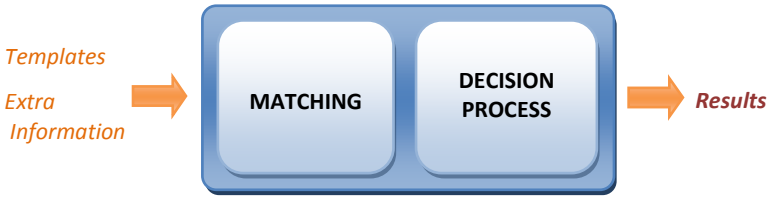

Figure 5: Functional architecture - Recognition block

2.1.1.5 Data Transmission

This element is responsible for the communication and data sharing between the different blocks. In some cases, **compression and expansion** processes are required for the optimization of the data transmission.

Figure 6: Functional architecture - Data Transmission block

2.1.1.6 Enrolment and Matching

Based on these functional blocks, the two **phases of the biometric process** are implemented as follows:

- **Enrolment**: introduction of a new individual in the system storage, which includes the biometric data acquisition from that individual, the extraction of features and the generation and storage of the corresponding template.

Figure 7: Main functional blocks involved in the enrolment phase

- **Matching**: recognition of an individual, which requires the generation of the template for that individual and its comparison with the templates stored in the system.

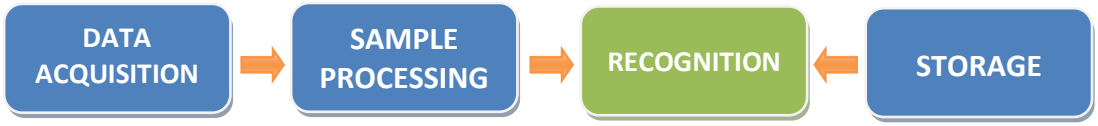

Figure 8: Main functional blocks involved in the matching phase

2.1.2 Components of a Biometric System

The functions described in the previous section are implemented by the components described below.

2.1.2.1 Sensors

Sensors perform the collection of biometric data from the individuals targeted by the system and its conversion to digital data.

The information from the sensors in a biometric system can be complemented with other data required for the enrolment or matching phase, which may be introduced in the system using other components (e.g. numeric pad, touch pad, system clock, etc.).

The sensors can be standalone, i.e. be independent equipments featuring only sensing capabilities, or they can be directly embedded in a more complex device with processing units or other components.

The type of sensor to use depends on the biometric technology selected. Here are some examples:

Biometric technology	Sensors
Fingerprint, *Palm print*	• Digital camera (2D/3D information) • Ultrasonic sensor • Capacitive scanner • Thermal scanner
Body prints	• Depth cameras (3D information)
Finger/hand geometry	• Depth cameras (3D information) • 2D cameras + angled mirrors (3D information)
Lips geometry	• Digital camera
Face recognition	• Digital camera (2D/3D information)
Iris recognition	• Iris scanner *(high resolution camera including near-infrared light)*
Retina recognition	• Retinal image scanner *(high resolution camera including infrared light)*
Signature/Handwriting	• Optical scanner • Digital camera • Touchpad • Motion recording sensor (hand)
Keystroke analysis	• Keyboard
Vascular pattern recognition *(hands, finger, eye, etc.)*	• Digital camera • Thermographic/infrared camera or scanner
Speech recognition, *Lips movement recognition*	• Microphone • Digital camera
Gait	• Motion recording sensors (e.g. accelerometers) • Digital camera (2D/3D information)
Facial Thermography	• Thermographic/infrared camera
Ear shape	• Digital camera (2D/3D information)
DNA	• DNA scan sensor
Human scent recognition	• Odour sensors (e.g. electronic noses)
Fingernails recognition	• Digital camera

Skin pattern recognition	• Optical spectroscopic sensor + near-infrared light
Blood pulse measurement	• Infrared sensor (IR LED + photodiode)
Body salinity identification	• Salinity sensor

Table 1: Examples biometric technologies and sensors used

Taking into account the examples mentioned, we can classify these types of sensors based on the nature of the data captured or, in other words, what they try to characterize:

General types of biometric sensors

- **Electrical sensors**: measure the changes in the electrical or magnetic signals of the human body (e.g. capacitive scanners, salinity sensor).
- **Optical sensors**: measure the quantity and changes in the light of the environment and converts it to digital data (e.g. optical spectroscopic sensor, IR sensor based on photodiodes).
- **Chemical sensors**: provide information about the chemical composition (e.g. CO2 sensor).
- **Mechanical sensors**: detect changes in a physical magnitude produced by force or movement (e.g. pressure sensors).
- **Thermal sensors**: measure the temperature (e.g. thermometer).
- **Acoustic sensors**: convert sound to digital data (e.g. microphones, ultrasonic sensors)
- **Radiation sensors**: measure the amount of radiation (e.g. Gamma-Ray Spectrometer).

Particular types of biometric sensors

- **Image sensors**: particular case of optical sensors that transform optical images into digital images, which are based on CCD or CMOS technologies to capture the pixels of the image. As an example, this category includes the cameras and scanners providing digital images (e.g. thermographic cameras, depth cameras, thermal scanners, iris scanners).
- **Tactile sensors**: measure the physical interaction of a user with a device or system (e.g. keyboards, touch displays). Depending on the technology used, this type can be considered a particular case of electrical sensor (e.g. common touchpads) or optical sensor (e.g. optical keyboard, optical mouse).
- **Biosensors**: measure physico-chemical-biological parameters existent in the human body (e.g. DNA sensor). It can be a sub-type of electrical sensor (e.g. salinity sensor) or chemical sensor (e.g. odour sensor), depending on how they capture the data.
- **Motion sensors**: subtype of mechanical sensors that capture any of the magnitudes which characterize human motion (e.g. accelerometers, gyroscopes, compass).**Position sensors**: another subtype of mechanical sensors that estimates the relative location of an individual (e.g. GPS sensor, proximity sensor). Location services normally use network location information (e.g. information from wireless access points), GPS sensors or motion sensors to calculate the position of the user. So, if an accelerometer is used to obtain the user location, it can be considered as a position sensor.

Other types of sensors may be found in emerging biometric systems and added to the list.

Regarding the characteristics of a sensor, the following ones are the most relevant:

- **Type**: type of the sensor taking into account the biometric property measured, and based on the classification described in the previous section.
- **Range**: minimum and maximum value of the magnitude measured over which a sensor works correctly (e.g. minimum and maximum weight for a scale, visible range for a camera, etc.).
- **Resolution**: the smallest reliable change that can be detected by the sensor (e.g. minimum grams measured by a scale).
- **Sensitivity**: ratio between the output and the input of the sensor obtained when the input is the smallest increment of change that causes a detectable change in the output.
- **Accuracy**: maximum difference between the real value of a magnitude and the value measured by the sensor.
- **Precision**: spread of the measures obtained after repeating the same measure under the same conditions.
- **Repeatability**: expected variation after repeating several times the same measure.
- **Drift**: maximum variation of the output when the input stays constant during a certain period of time.
- **Response Time**: time required to provide an output given an input.
- **Output format**. The type of sample collected will depend on the biometric technology used (e.g. image, audio file, text, etc.).
- **Operating life**: time during which the sensor will work as expected after being installed.
- **Ambient conditions allowed** (Operating Humidity, Operating temperature, etc.)
- **Dimensions**: size of the sensor (height, width, depth).
- **Others**: apart from other characteristics from sensors in general, there are also other specific features of each type of sensor. For instance, for an image sensor also the frame rate and the compression type are important properties related to image quality.

2.1.2.2 Data storage

Different types of storage can be used in the same biometric system, and different types of information can be stored to provide the service expected from the system.

The information is stored in a database, that can be a typical relational database or even a file system (*type*), and that can be centralized in the same device or distributed through the network (*configuration*).

Other relevant feature of a data storage is its *capacity*, defined as the maximum amount of information that can be stored.

2.1.2.3 Processing units

One or many processing units are required for the execution of the different algorithms involved in the biometric processing, which are:

- **Signal processing algorithms**: that deals with the analysis and processing of biometric samples. Main tasks:
    - Pre-processing *(e.g. segmentation algorithm)*
    - Extraction of features *(e.g. corner detection in images)*
    - Generation of templates
    - Quality control
    - Data fusion

- **Matching algorithm**: responsible for the comparison of templates for identification, verification or categorization.
- **Decision algorithm**: this component filters the results of the matching process according to a defined policy in order to reject them or accept them as a positive match.

Processing units have many known features, such as the number of CPU cores or as the CPU clock speed, but for the design of the biometric system the most important issues are:

- Which tasks are performed by the unit (e.g. algorithms executed)
- The response time of each process
- Which information is required and provided by the processing unit
- How is the data handled and transmitted (communication and security mechanisms)

2.1.2.4 Data transmission components

Different elements for data transmission may be required depending on the components selected for data capturing, processing and storing. Based on this, we identify two types of data transmission:

- *Transmission of information between components integrated in the same device*

  In this case the communication between the different modules is not exposed, and it is normally performed by using a common bus or other internal communication interfaces.
- *Transmission of information between components installed in different devices*, that can even be located in different networks

  In this case it is important to define how the different devices are going to be connected, particularly, if the connection is wired or wireless, and the networks required including the type (e.g. LAN, WAN), features (e.g. channel capacity, transmission methods), the needed network devices (e.g. routers, switches, etc.) and the communication technologies to use (e.g. Web Services, sockets, etc.).

The Data Transmission block may also include other components for the optimization of the transmission, such as modules for the compression/expansion of the data or encryption/decryption modules for data protection.

The different data transmission blocks that can be found in a biometric system can be characterized with these features:

- **Source:** emitter of the data transmitted
- **Destination**: receiver of the data transmitted
- **Data**: which information is transmitted
- **Data format**: format of the data transmitted
- **Method**: method for data exchange (e.g. shared memory, sockets, Web services, etc.)
- **Protocol** (e.g. HTTP, UDP, FTP, etc.)
- **Transmission rate**
- **Compression**
  - **Compression method**
  - **Compression rate**
- **Encryption**
  - **Algorithm**

Besides, some systems will require the use of one or several networks for the communications, each of them with the following features:

- **Network:**
  - **Type**: type of network (e.g. LAN, WAN, WLAN, etc.)
  - **Extension:** physical area covered by the network
  - **Components**: list of network components, for example: cables, routers, network interface cards, etc.
  - **Bandwidth**

2.1.3 Characteristics of a Biometric System

During the design phase of a biometric system, there are several properties of the system that have to be defined, which are mainly the following ones:

- **Purpose**: functionality for which the system was built.
- **Biometric technologies**: list of biometric technologies used by the system.
- **Unimodality or Multimodality**: it indicates whether they system uses one or several biometrics.
- **Mode of operation**: it can be identification, verification or categorization.
- **Phases**: different phases that take place in the biometric system. In the design stage it is important not only to identify the phases, but also to define how they are going to take place (online/offline, storage, user interactions, etc.).
- **Performance** expected:
  - **Response time**: how fast the system will respond in the worst case.
  - **Availability**: period of time during which the system will work as expected.
  - **Accuracy**: referring to the required success rate or the minimum error rate that the system will provide.
- **Area**: area covered by the biometric system.
- **Conditions**: environmental conditions in which the system operates properly.
- **Information required** by the system to perform the recognition (data captured, format)
- **System users:**
  - **Targeted number users** for which the system is designed
  - **Groups of users**, and for each their privileges
  - **Procedures**: how the system is used by the different users
- **Data management**:
  - **Data access** (who can access, limitations, if download is allowed or not, etc.)
  - **Data management** during the different phases
  - **Data exchange**: it describes the data sharing with other systems (if any), in which it is important to define the information that is exchanged and the circumstances in which it will be shared.
- **System components and configuration**:
  - **Sensors**: number and type of sensors that will be used.
  - **Processing units**: required processing units and tasks performed by each.
  - **Data storage** (number, type, configuration, minimum capacity).

- **Communication** between the different system components (data transmission elements, network configuration, etc.).

- **Security**: security for the whole system in general (data storage, communications, etc.).

2.1.4 Design process for Biometric Systems

2.1.4.1 System requirements

The first step of the design process is the extraction of the different requirements for the system, which are usually provided by the customers and the characteristics of the environment where the system is going to be deployed. From the list of requirements, the main characteristics of the system can be obtained.

The general requirements that apply to most of the biometric systems were detailed in section 3.1.1 of deliverable D4.1 and they are summarized in the table below.

Functional Requirements *(functions performed by the system)*	**Enrolment**
	• Is the enrolment phase required? • Extra information from users needed (e.g. PIN, password) • Type of enrolment (online/offline)
	Matching
	• Type: identification, verification or categorization • Actions taken by the system in case of positive match • Actions taken by the system in case of negative match
	Data Management
	• Information required and stored in the system • How the system is going to use the data • Criteria for data deletion
	Special functions
	• Other functions required (e.g. open electronic door)
Operational requirements *(how the system will be used)*	• Groups of users and their privileges • System availability • Organizations involved • User actions in case of positive/negative match • Unattended operations handling • Information flow • Data source • Where data is processed • Where data is stored • Which data is transferred between organizations • Interactions between the users and the system
Technical requirements *(technical decisions and non-functional requirements)*	• Central or distributed system • One or several data storages • Communication requirements (connectivity and security requirements for data transmission) • Number of users and size of the system (scalability) • Performance: accuracy and response time (criticality) • Integration issues
Environment requirements *(physical and environmental*	• Operation indoors or outdoors • Light, humidity, noise and temperature conditions

constraints)	• Area to cover
Privacy requirements *(protection of the privacy of system users and stakeholders)*	• Which personal data is collected, for which purpose, how it is used and user rights to access, modify or delete • Consequences of system failure • Consequences of misuse of the data processed and stored • Specification of mechanisms for data protection • Accountability procedures

Table 2: Summary of the requirements for a biometric system

2.1.4.2 Selection of biometric technologies

The selection of the specific biometric technologies to be implemented depends on the following aspects:

- **Ease of use**, which depends on the profile of the users of the system, but in general the system should be as simple to use as possible.
- **Error Incidence**: which refers to the conditions that affect significantly the performance of the system.
- **Accuracy** or error rate expected from the system.
- **User Acceptance**, which depends mainly on how invasive is the system and also in other user concerns (privacy or security concerns, religion, etc.). The invasiveness of the system is one key feature from the user point of view, and it is directly related to the privacy of the persons.
- **Security level required** for the application, which includes the probability of the biometric data to be tampered. For high-security applications, normally biometrics based on physiological data (e.g. fingerprints, face recognition) are more adequate than behavioral biometrics (e.g. gait, voice recognition).

  The confidentiality of the data captured is also important, but it depends mainly on how the system is built, and not so much in the technology selected.

  The security level provided is the most relevant aspect to take into consideration in the selection of the biometric technology from the privacy perspective. In deliverable D2.2, particularly in section 4.2.1, there is a table summarizing the potentials risks for the main biometric technologies.
- **Long-term stability**, which is influenced by the maturity of the technology and other factors [1].

Other factors can be applied to the selection of the technologies, as well as to the design of the whole system:

- **Response time**: in some cases the system will be required to work in almost real-time (for example: to open a door), in other cases the time will not be a limitation.
- **Environmental constraints:** the place where the system is going to be deployed establishes several limitations and requirements for the system, such as the operational conditions, that also affect the technologies for data acquisition.
- **Business constraints**: budget limitations, strict schedule for the implementation, need to reuse existing infrastructures or equipment or to select specific Hw/Sw, etc.

The following table shows a comparative of the main biometric technologies based on some of this criteria [1]:

Feature	Ease of Use	Error Incidence	Accuracy	User acceptance	Required security-level	Long-term stability	Cost
Fingerprints	High	Dryness, dirt, age	High	Medium	High	High	Low
Iris	Medium	Poor lightning	Very high	Medium	Very high	High	Very High
Face	Medium	Lightning, age, glasses, hair	High	Medium	Medium	Medium	Low
Hand Geometry	High	Hand injury, age	High	Medium	Medium	Medium	Medium
Retina	Low	Glasses	Very high	Medium	High	High	High
Voice	High	Noise, colds, weather	High	High	Medium	Medium	Medium
Signature	High	Changing signatures	High	Very high	Medium	Medium	Low
DNA	Low	-	Very high	Medium	Very high	High	Very high

Table 3: Summary of the selection criteria regarding the technology used for a biometric system

It is important to consider how the biometric technologies affect not only the privacy of individuals in general, but also how they affect to the different types of privacy. In section 4.3.3 of deliverable D2.2, the seven types of privacy identified are explained, and the relationship between these types and the main biometric technologies is summarized in the following table:

Tech \ Privacy Risk	P. of Person	P. behaviour and action	P. of communication	P. of data and image	P. of thoughts and feelings.	P. of location and space	P. of association
Fingerprints	X		X	X*		X*	
Iris	X	X		X*	X	X*	
Face	X	X		X*	X	X*	
Hand Geo.	X			X*		X*	
Vein Scan	X			X*		X*	
Ear Geo.	X			X*		X*	
Palm prints	X		X	X*		X*	
Retina Scan	X	X		X*		X*	
Gait	X	X		X*	X	X*	
Voice Reco.	X		X	X*	X	X*	
Signature	X		X	X*	X	X*	
DNA	X	X	X	X*		X*	X
Multimodal systems	X	X	X	X*	X	X*	X

X depends on the system not on the technology itself*

Table 4: Biometric technologies VS. the seven types of privacy

2.1.4.3 Selection of sensors

From the system designer point of view, the selection of the sensors is based on the following aspects:

- The biometric technologies selected and type of biometric system
- The areas to be covered by the system
- The technical features of the sensors, mainly:
    - Features related to the sensing capabilities: range, resolution, sensitivity, etc.
    - Features related to the performance: accuracy, response time, operating life, etc.
    - Operational conditions
- Business constraints

The main risks affecting individuals' privacy identified during the data acquisition process are:

- *Identity theft or spoofing*. The system should implement the necessary mechanisms to guarantee the user authenticity.
- *Data tampering*. The system should implement the necessary mechanisms to guarantee the integrity of the data captured.
- *Disclosure of personal identifiable information*. The user confidentiality is crucial during all the biometric process, and specially during the data capturing process. Adequate actions should be performed to avoid data disclosure without the user consent, in terms of security (e.g. anonymization) and accountability of every entity involved in the biometric process.

2.1.4.4 Selection of processing units

These components are responsible for the processing of the biometric data captured and also the management of other information required for the recognition process. Technically, the selection of the processing units depends on these factors:

- Resources required by the algorithms that have to be executed
- Response time required for the system
- Business constraints

The main risks affecting privacy in the processing of information are:

- *Data tampering*. The system should implement the necessary mechanisms to guarantee the integrity of the data processed.
- *Component manipulation*. The system should implement the necessary mechanisms to ensure the integrity of the elements involved in the processing of information (e.g. algorithms).
- *Disclosure of personal identifiable information*. Adequate actions should be performed to avoid data disclosure without the user consent, in terms of security (e.g. anonymization) and accountability of every entity involved in the biometric process.

2.1.4.5 Selection of data storage

The selection of the data storages for the biometric system depends on:

- Type of data that has to be stored in the system
- Access required to the information (e.g. volume of queries, export capabilities, etc.)
- Size of the data to be stored
- Business constraints

These are the main risks affecting privacy identified related to data storage:

- *Data tampering*. The system should implement the necessary mechanisms to guarantee the integrity of the data stored. Besides, it is necessary to provide to users access to their personal identifiable information stored in the system, and let them modify it or delete it if necessary.
- *Unauthorized access to the information*. Security mechanisms shall be implemented to prevent unauthorized accesses to the data stored and facilitate its audit (e.g. access logs).
- *Misuse of the data stored in the system*. Appropriate policies must be defined to inform users about how their personal information is used. Furthermore, sufficient mechanisms shall be implemented to identify the misuse of data.
- *Disclosure of personal identifiable*. Adequate actions should be performed to avoid data disclosure, in terms of security and accountability.

In general, small distributed data storages present lower impact on individuals' privacy than large centralized data storages.

2.1.4.6 Selection of components for data transmission

Once selected all the other components of the system, the elements for data transmission will be chosen based on:

- System architecture
- Type of data to be transmitted
- Environmental conditions
- Capabilities of the different devices selected
- Business constraints (e.g. reuse of existing infrastructures)

The main privacy risk in data transmission is the unauthorized access or disclosure of personal identifiable information. For this reason, the transfer of information between the different components and with other systems must be carefully defined at the design stage, and security mechanisms should be implemented to protect the data shared.

2.1.4.7 Privacy risks identified at the design stage

This list summarizes the main privacy risks identified during the design of the biometric system:

- Identity theft or spoofing *(user authenticity)*
- Data tampering *(data integrity, data origin authenticity)*
- Component manipulation *(system integrity)*
- Disclosure of personal identifiable information *(confidentiality, unlinkability)*
- Unauthorized access to the information *(confidentiality)*
- Misuse of the data stored in the system

In general, it is important to manage adequately the data during all its lifecycle, which includes the data capturing, the transmission, the storage and the deletion of the information once the service is concluded.

Besides, it is necessary to identify all the entities and people involved in the biometric process, even third parties, and assign the responsibilities for each *(non-repudiation, accountability)*.

All the measures implemented for privacy protection, as mentioned in D4.1, will have an impact on the design of the system so they have to be selected carefully, although the degree of freedom for this will depend on the application for which the system is built and the environmental and business constraints.

2.2 Representation of biometric technologies in a modelling framework

The representation of biometric technologies in a modeling framework is addressed twofold in this section:

- Firstly, an overview of the general SALTed design process is described for better presentation and understanding of the context,
- Secondly, the UML profile defined for a generic biometric system is presented.

2.2.1 Design process for SALT compliant biometric systems

The SALT Framework captures the knowledge from different experts in the fields of information technology, laws, ethics and sociology to provide guidelines for the implementation of Privacy by Design and Accountability by Design in surveillance systems. These guidelines are given in the form of SALT references that designers can consult and analyze to develop a SALT compliant biometric system that optimizes the surveillance and the privacy protection features, while integrating the concept of accountability.

The references include information about what concerns shall be taken into consideration by designers to develop a SALT compliant system, and what measures can be implemented to apply the SALT principles regarding those concerns. The references are provided in a human-readable language, but it is also possible that they include a set of rules in OCL language that the system must follow to be SALTed, in which case they are considered complete references. Only the complete references can be automatically checked using a specific tool included in the SALT Framework.

Taking all this information into account, the SALT Framework can be used for three main tasks during the lifecycle of a biometric system described in deliverable D4.1 (Figure 9):

- **Extraction of concerns and recommendations** on privacy and accountability for the design of a system according to the SALT principles.
- **Validation of the design of the system according to the SALT principles**, which can be performed at the design phase but also anytime the system is modified, for instance after the system testing or for maintenance purposes.
- **Consulting references related to a specific system for auditing purposes**, which is normally performed by the Data Protection Officers in order to verify that the system complies with the current regulations on privacy and data protection.

All in all, the design process of a SALT compliant system starts with the collection of different types of requirements from customers and service providers. This initial set of requirements shall be completed with the concerns and recommendations provided by the SALT Framework for that particular design, after which a complete specification is obtained taking into consideration privacy and accountability. The biometric system shall be designed based on this resulting specification.

Before the implementation, the system designed should be reviewed in order to check if it addresses the concerns provided by the SALT framework about privacy and accountability. The SALT Framework includes a tool for the validation of systems that can be applied to those systems with complete SALT references. Other systems cannot be verified automatically with this tool of the SALT Framework, which does not mean they are not SALT compliant, they just have to be validated in a different way.

During the testing phase, some modifications may be required (e.g. to improve the performance of the system). Anytime a change is made in the system, the resulting design should be validated again to check if it addresses the concerns provided by the SALT Framework.

Once the system is tested and verified as compliant with the SALT concerns, it shall be properly deployed and configured to work under the conditions defined in the initial specification, after which the system is ready to be used for the purpose it was built.

The system may be subject to audit at any moment by the Data Protection Agencies to check if it complies with the current regulations on privacy and data protection. As the system has been designed based on the guidelines provided by the SALT Framework, the auditors may require to consult the recommendations and SALT references used to develop the system.

The last phase is the maintenance of the system, which may also require to perform changes in the system, that shall also be validated.

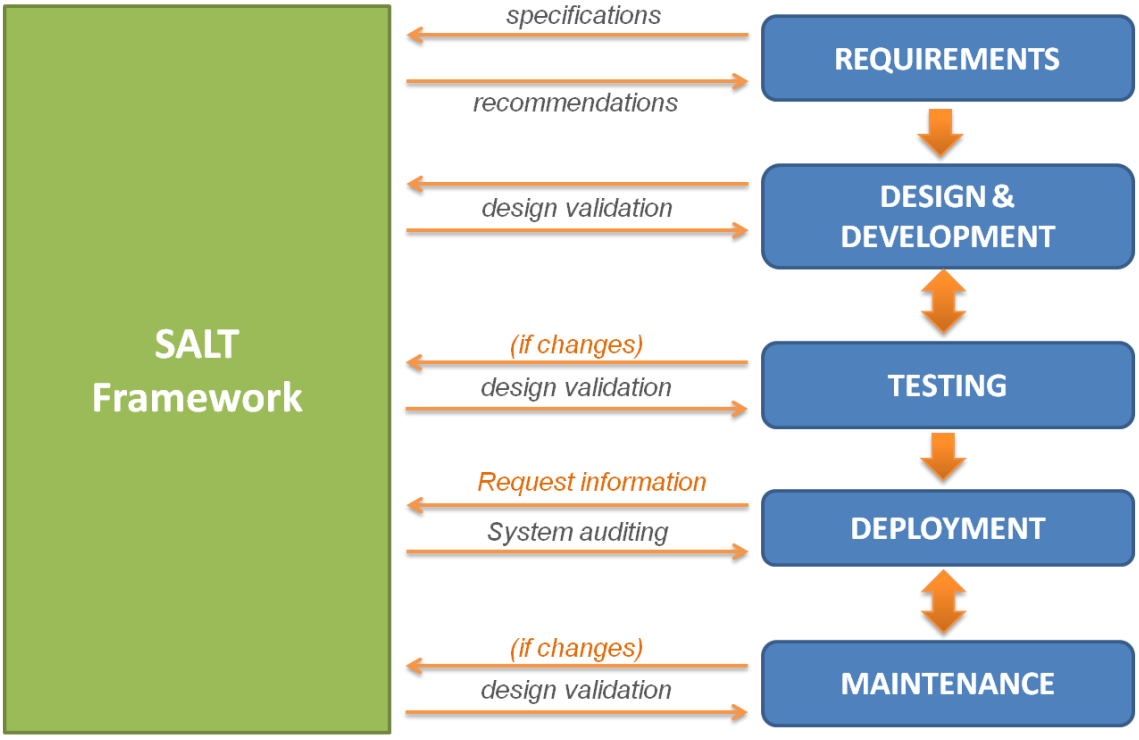

Figure 9: Role of the SALT Framework at the different stages of the system lifecycle

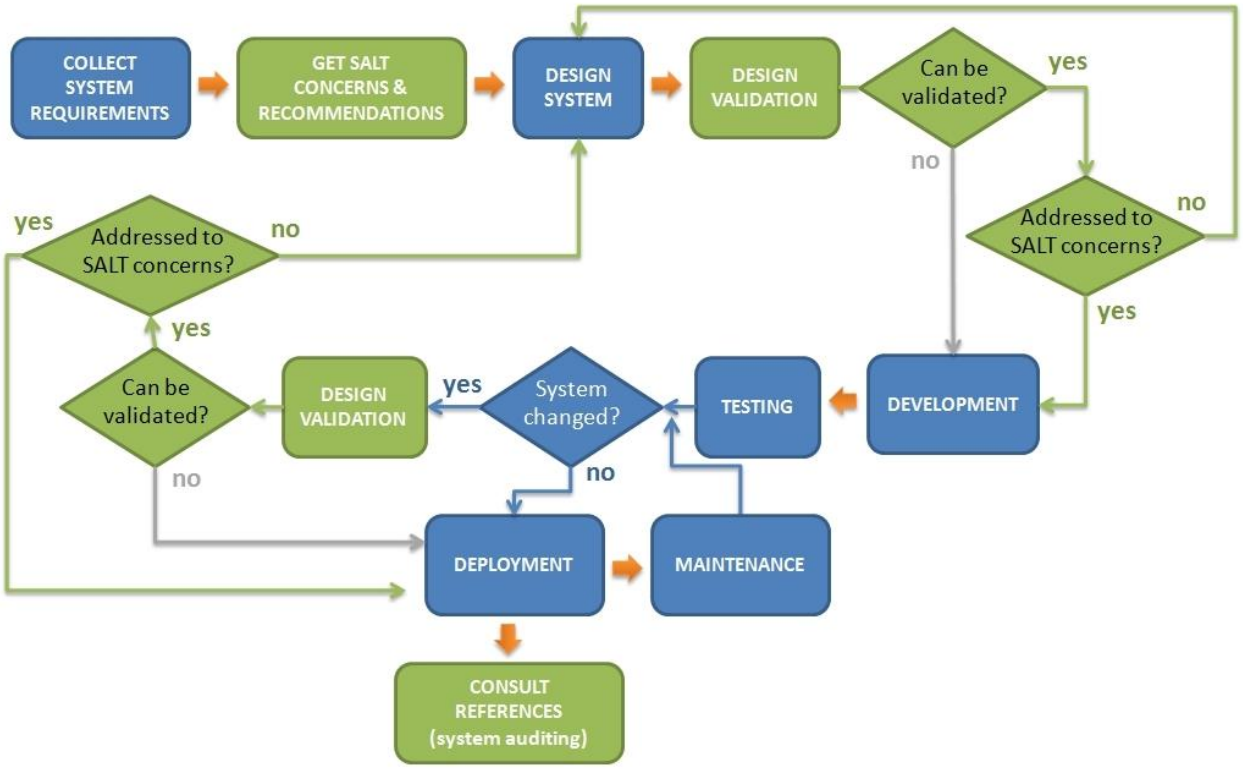

Figure 10: Design process of a SALT compliant biometric system

Figure 10 depicts the process of design of a SALT compliant biometric system. If the design can be validated through the OCL rules, it is possible to certify with the SALT Framework if the system is SALT compliant or not. Otherwise, the system cannot be validated automatically with the corresponding tool of the SALT Framework, but in those cases that SALT Framework provides assistance for the preparation of the necessary documentation for an external audit of the compliance of the system with the SALT principles.

2.2.2 Profiling biometric systems

To provide enough elements to design a biometric system we have created a UML profile. A profile in the Unified Modeling Language provides a generic extension mechanism for customizing a UML model for particular domains and platforms. Then, the profile contains a set of artifacts that model biometric elements based on information provided by the experts.

The components for the description of biometric systems have been modeled using stereotypes. A stereotype is a mechanism in UML that can be used by designers to create new UML model elements from existing ones by extending or altering their properties for a particular usage or a specific problem domain. A stereotype can be applied to a class, or a method or to an attribute of a class. Therefore, the stereotypes represent the necessary components to design a complete biometric system.

Since the designer does not have to know about UML, the SALT Framework will provide a graphical user interface that abstracts the use of UML and allows the designer to create the biometric system without having to learn UML. This interface will be implemented as a friendly environment in Magic Draw [2], where the different stereotypes characterizing a biometric system are represented by icons. These icons have been designed by the UMA in order to be intuitive. As an example, in Figure 11 we can see three of the available icons, which correspond to the stereotypes of *System*, *Data* and *Network Link*.

Figure 11: Biometric Stereotype Icons

In order to shape a particular biometric system, the system designer just have to drag and drop the icons from the menu to the design panel. In that moment, a box will appear with the different properties and methods of the related stereotype, and the icon placed in the top right of the box (see Figure 12). The system designer then will be able to edit the value of the stereotype properties in order to adequate them to his design.

The steps of the whole process for the design of a biometric system using this tool are the following:

1.- Import the information obtained from the SALT Framework for that system into the design tool. At least the OCL rules can be imported, and the UMA is currently working on the import of SALT references to facilitate even more the design with this tool.

2.- Drag and drop the necessary elements to the design panel to compose the biometric system.

3.- Edit the attributes of those elements, giving values according to the biometric system designed and application of stereotypes to other biometric attributes.

4.- Validate the design with OCL rules. This step is done in execution time.

As a result, the designer obtains a SALT compliant biometric system design.

It is important to highlight that we provide the tool and some guidelines to help the designer in the creation of a SALT compliant system. The tool can even check that the designer has followed some of the recommendations provided in the SALT references. However, the designer can include recommended methods that do not work properly. Since these methods can be implemented in multiple ways it is not possible check their internal function ability. In other words, the SALT compliance does not ensure performance compliance of the system.

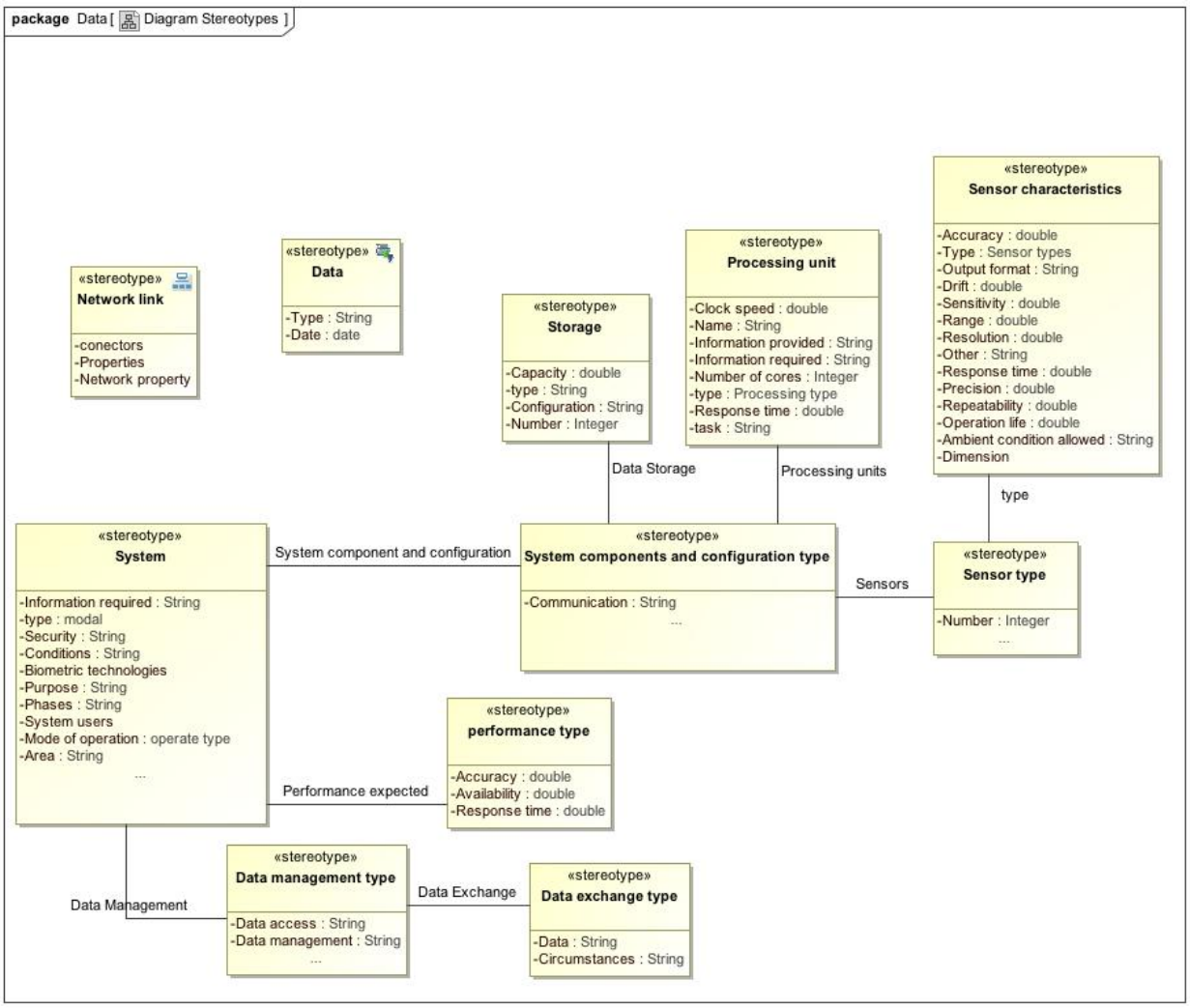

Figure 12: Stereotype Diagram

In Figure 12, we can see the most relevant elements that can appear in a biometric system. The main component is the *System* stereotype, which represents the core of the design. It contains the principal attributes to represent the characteristics of a biometric system. As we can see in the image, this attributes match the aforementioned properties (section 2.1.3 Characteristics of a Biometric System).

The *System* stereotype is related with the *System component and configuration* that allows indicating which databases are going to be used, their capacities, their configuration and finally the number of databases used. It is also connected with the sensors used in the system and it can access and edit all sensor properties.

The *Processing unit* stereotype, which is connected with the *System component and configuration* too, represents the characteristics required for the execution of the different algorithms involved in the biometric processing.

Performance type stereotype represents the qualities of the system sensors and the different options that could be selected depending on the sensor type.

The stereotype *Performance type* shows the performance expected, through accuracy, availability and response time.

The stereotype *Data* shows type of data that is going to be store and the expiration date of it, and the stereotype *Data management type* allows modeling the access, the management and the exchange of that data.

Finally, a system is normally made up of several components connected through a network. This connection is modeled with the *Network link* stereotype, that can also be used to represent the data transmission block between different systems.

3 Biometrics Use Cases and Scenario

3.1 Scenario description

The scenario is based on the development of a system capable of detecting unauthorized people in a building with access restrictions by using biometric technologies.

The scenario selected is a **private office** with security requirements, located in **Spain** (Visual Tools' Headquarters), where at certain hours only a few people are authorized to enter. Thus, an **authorized person** is defined as someone that is allowed to be inside the building at a defined period of time, that in this case corresponds to non-working hours, when only the security guards and the maintenance or cleaning employees are allowed to access the building.

A **video-based biometric system** will cover the main transit areas of the office. Anytime a person appears in the scene, the system shall be able to detect it and shall be capable of deciding if the person is authorized or not to access the building at that time. Furthermore, the system shall manage the results of the decision process according to a defined action protocol.

Initially, the action protocol consists of **generating and sending an alarm** to the security guard in case an unauthorized person is detected. Optionally, the system could also send an image of the intruder with the message to the security guard or to an operator responsible for monitoring the office, in order to determine if it is a false alarm. That image can be stored in the system in case the organization needs to give it to the authorities.

3.2 User groups

During the lifecycle of the system, which covers its design, development and use, we can identify the following users:

- *System Designer*: person in charge of the design and development of the biometric system. This user interacts with the SALT Framework to get recommendations for the design of the system and to verify that the system created is SALT compliant.
- *Service Provider*: company responsible for the provision of the biometric system performing the detection of unauthorized people in the selected scenario. Several people from different departments of the company can perform the role of a *Service Provider*, all of them with a clear goal: refining requirements for the specification of the system according to the best interests of the company. Thus, the *Service Provider* is the user that has in mind the business constraints and the legal requirements for the system at the design stage.
- *System Owner*: company requiring the biometric system and providing most of the requirements for the system. The *System Owner* is responsible for the use made of the system, which should comply with the existing regulations, and for the protection of the data collected.
- *Installer*: person responsible for the deployment of the system, who is also in charge of facilitating the access to the system to the *System Administrator*. Optionally, the *Installer* could train the system users (*System Administrator* and *System Operator*) to help them understand how the system works and facilitate their daily routines.
- *System Administrator*: person responsible for the management of the system who has all the privileges to configure it and to manage the data stored. This user is in charge of providing authorization to other users to access the information stored in the system.

- *System Operator*: person responsible for monitoring the facilities and managing the alarms, who has limited access to the information stored in the system. The System Operator can be a security guard or one another person in charge of monitoring the facilities.
- *Person Accessing*: person appearing in the scene, that can have permissions to access the building at the defined period or not.

  Regarding the group of authorized people, it is composed of a maximum of 10 people including security guards, and maintenance or cleaning employees.
- *Data Protection Officer:* person responsible for ensuring that the system built and the services provided comply with the existing regulations on privacy and data protection.
- *Police Officer*: person responsible for law enforcement in case an intrusion is detected.

Normally the design process starts when the *System Owner* demands a specific service from the *Service Provider* which involves the implementation of a biometric system in the *System Owner's* facilities. Then, the *Service Provider* is in charge of collecting all the requirements from his customer (*System Owner*) and from his company (business and legal requirements), and for organizing the work of the *System Designer* and the *Installer* to provide the required service to the *System Owner*. As a result, the biometric system needed to perform the detection of unauthorized people should be installed at the selected office and ready to use. Once the system is deployed, the *System Owner* is accountable in law for the use made of the biometric system.

3.3 Use Cases

As explained in section 2, the lifecycle of a biometric system can be divided in different phases. In this section we present the main use cases identified during the lifecycle of the proposed demonstration biometric system.

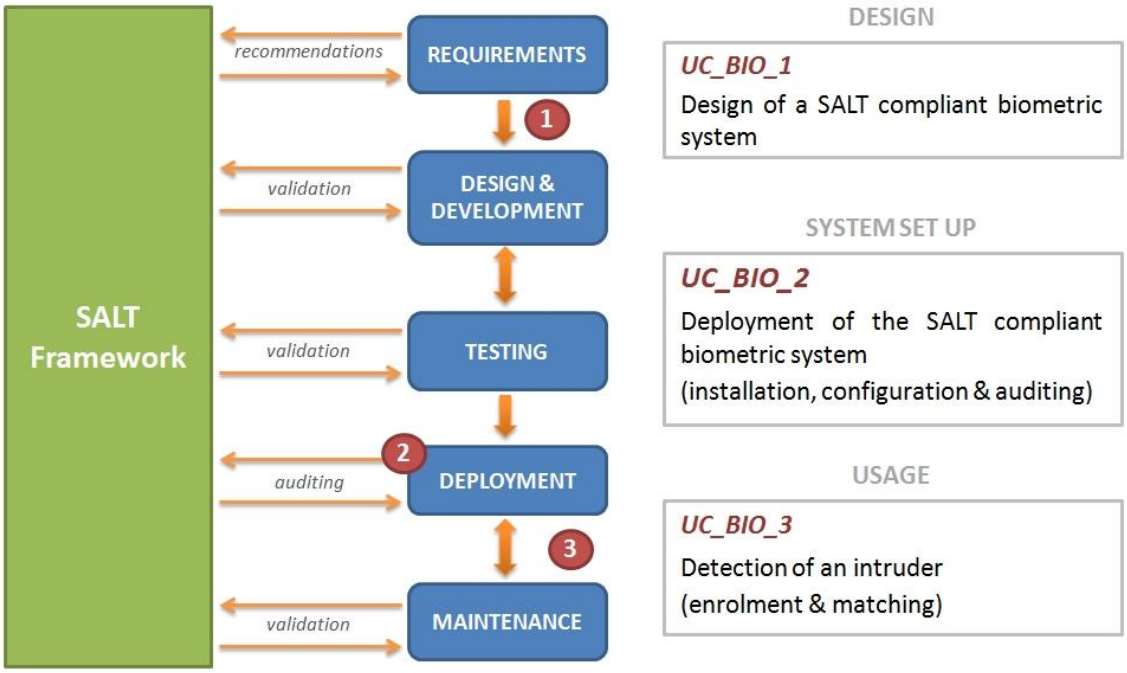

Figure 13: Relationship between the defined use cases and the system lifecycle

3.3.1 Design of a SALT compliant video-based biometric system

A use case is defined for the design of a SALT compliant system, in which the system designer makes use of the SALT framework to obtain the necessary information regarding privacy and accountability to build a system addressing the SALT principles.

These are the actors identified in this stage:

- *System Designer* (SD), dealing with the design of the system taking into account the requirements and constraints provided as well as the SALT references.
- *System Owner* (OW), referring to the entity requiring the biometric system.
- *Service Provider* (SP), responsible for the provision of the biometric system.
- *SALT Framework* (SF), that provides guidelines for the design of systems in terms of privacy and accountability and that provides a tool to validate certain systems as concerned with the SALT principles.

3.3.1.1 Use Case I: Design of a SALT compliant biometric system

ID	**UC_BIO_1**
Name	**Design of a SALT compliant biometric system**
Actors	• *System Designer (SD)* • *System Owner (OW)* • *Service Provider (SP)* • *SALT Framework (SF)*
Aims	Design of a video-based biometric system complying with the references provided by the SALT Framework.
Preconditions	The OW has demanded a service from the SP that requires the implementation of a biometric system for intrusion detection at a private office.
Description	1. The SD collects different requirements and constraints for the system from the SP and the OW. 2. The SD requests guidelines in terms of privacy and accountability to the SF for the design of the system. For this, the SD provides information of the specification of the system and the context. 3. The SF provides to the SD a set of concerns related to the system specified, and some recommendations about measures or mechanisms that can be applied to address those concerns. The SF also provides with the recommendations OCL rules that facilitate the automatic validation of the system. 4. The SD designs the system taking the SALT guidelines into account. 5. The SD requests to the SF the validation of the system designed. For this, the SD provides an UML description of the system. 6. If the system includes OCL rules, the SF verifies automatically if the system addresses the SALT concerns.
Exceptions	*a) The SALT reference provided for the system does not include OCL rules* a.6 The SF cannot verify if the system addresses the SALT concerns or not, so the compliance of the system with the SALT principle cannot be granted with the SALT Framework. The system can be verified as SALT compliant in other ways (e.g. checking manually the deployment made and the different procedures). *b) System not SALT compliant* a.6 The SF checks the SALT compliance of the system and concludes it is not.. a.7 The SF provides information about the concerns not fulfilled to the SD. a.8 The SD revises and modifies the system.

	a.9 Steps 4-5 are repeated.

Table 5: Use Case I description - Design of a SALT compliant biometric system

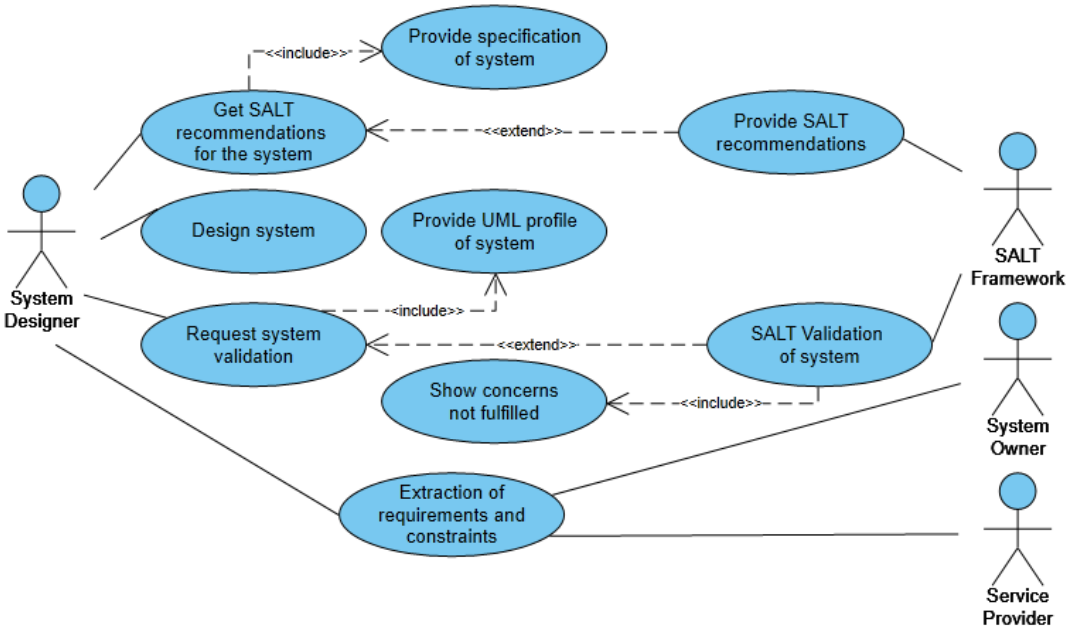

Figure 14: Use Case I diagram - Design of a SALT compliant biometric system

3.3.2 Deployment of a SALT compliant video-based biometric system

The objective of this stage is to set up the system and get it ready to use. For this, a use case has been defined to cover the following tasks:

- Installation of the SALT compliant system.
- Configuration of the system according to the conditions of the defined scenario.
- Audit of the system to verify the compliance with the existing regulations on privacy and data protection.

These are the actors identified at the deployment stage:

- *Installer* (IN), dealing with the deployment of the system.
- *System Administrator* (SA), responsible for the management of the system.
- *System Operator* (SO), responsible for the monitoring the intrusion detection process.
- *Data Protection Officer* (DPO), responsible for ensuring that the system built and the services provided comply with the existing regulations on privacy and data protection.
- *SALT Framework* (SF), in charge of the provision of guidelines for the design of systems in terms of privacy and accountability.

3.3.2.1 Use Case II: Deployment of the SALT compliant biometric system

ID	**UC_BIO_2**
Name	**Deployment of the SALT compliant biometric system**
Actors	• *Installer (IN)* • *System Administrator (SA)* • *System Operator (SO)* • *Data Protection Officer (DPO)*

	• *SALT Framework (SF)*
Aims	Deployment of a video-based biometric system complying with the current regulations on privacy and data protection. After this use case, the system should be ready to use.
Preconditions	The system has already been developed, tested and validated as addressing the SALT concerns. After the installation and configuration, the DPO wants to verify the compliance of the system with the current regulations.
Description	1. The IN installs the biometric system at the selected office based on the SALTed design and the system specification. 2. The IN configures the system to set up the detection of unauthorized people in the selected environment. 3. The IN give access to the system to the SA for system management. 4. The SA configures the detection period. 5. The SA creates new system users with the adequate privileges to monitor the intrusion detection process (SO). 6. Optionally, the IN trains the SA and/or the SO in the usage of the system. 7. The DPO verifies the compliance of the system with the current regulations on privacy and data protection. For this, the DPO requests authorization to the SA to access the information stored in the system. This process is traced. 8. The DPO may also require access to the SF to review the information provided for the design of the system being audited.
Exceptions	-

Table 6: Use Case II description - Deployment of the SALT compliant biometric system

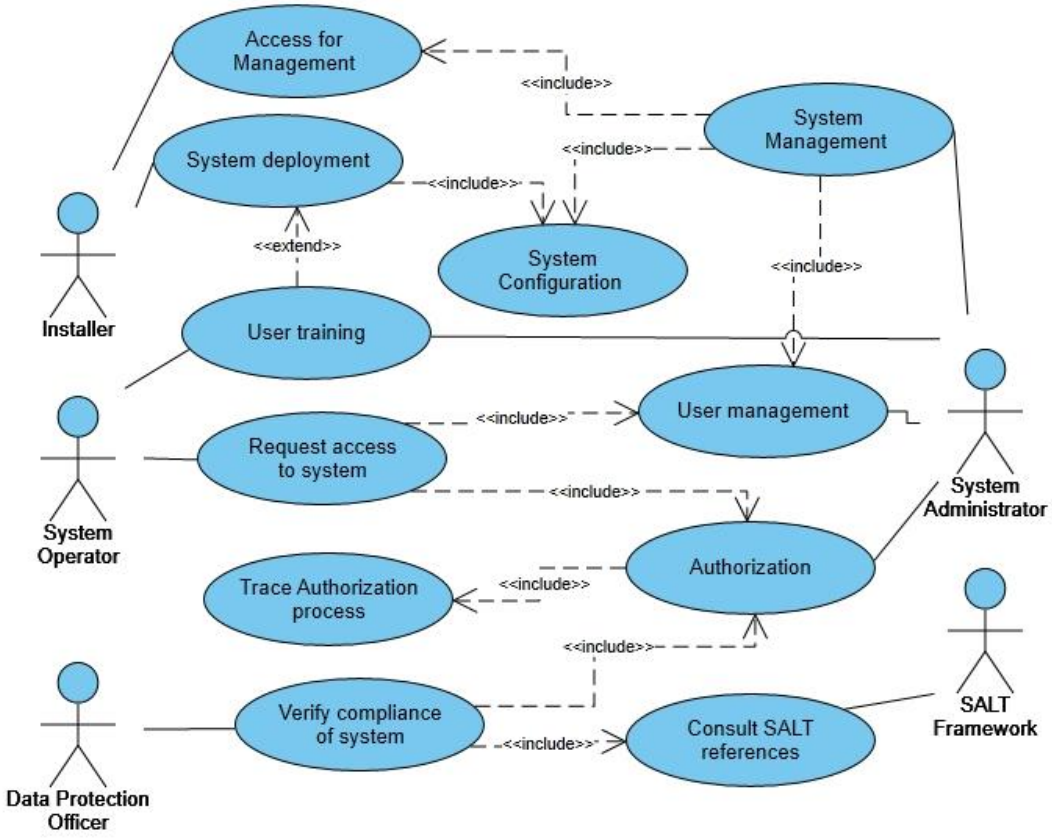

Figure 15: Use Case II diagram - Deployment of a SALT compliant biometric system

3.3.3 Detection of unauthorized people

Finally, a third use case is defined to describe how the system is used once it is operational, which can be divided in two main tasks:

- Enrolment of authorized people in the system
- Detection of an intruder

These are the main actors of this stage:

- *System Administrator* (SA): person responsible for the management of the system who has all the privileges to access to the information stored.
- *Biometric System* (BS), performing the necessary tasks for the detection of unauthorized people at the office and generating alarms.
- *System Operator* (SO): person responsible for monitoring the facilities who has limited access to the information stored in the system.
- *Person Accessing* (PA): person appearing in the scene, who can have permissions to access the building at the defined period or not.
- *Police Officer* (PO): person responsible for law enforcement in case an intrusion is detected.

3.3.3.1 Use Case III: Detection of unauthorized people

ID	**UC_BIO_3**
Name	**Detection of authorized people**
Actors	• *System Administrator (SA)* • *Biometric System (BS)* • *Person Accessing, that can be authorized (APA) or not authorized (NAPA)* • *System Operator (SO)* • *Police Officer (PO)*
Aims	Detection of unauthorized people in the selected office. Facilitate law enforcement in case of intrusion.
Preconditions	The system is correctly installed and configured, and it complies with the current regulations on data and privacy protection. After the enrolment, a NAPA appears in the scene.
Description	1. The authorized people (APA) is enrolled in the BS. This task requires the participation of the SA, who initiates and monitors the process. 2. A NAPA enters the building and accesses to one of the areas being monitored by the BS. 3. The BS detects the NAPA and automatically starts the recognition process to determine if the person is authorized or not. 4. The BS decides that the NAPA is not authorized. 5. The BS generates an alarm and sends it to the SO. 6. The SO verifies that the alarm is correct. For this purpose, the SO may require to consult some information stored in the BS. The SA is responsible for providing access to the SO to the system. 7. The SO reports the incident to the local authorities. 8. The PO request authorization to the SA to get the information stored in the system related to the incident reported. 9. The PO verifies the intrusion and take the adequate measures for law enforcement
Exceptions	*a) Not detection* a.3 The BS does not detect the person crossing the monitored areas.

	a.4 Use Case ends. b) *Wrong categorization* b.4 The BS indicates that the PA belongs to the group of authorized people. b.5 The BS does not generate any alarm and the SO is not warned about the intrusion. b.6 Use Case ends. *c) Insufficient or inaccurate information provided with the alarm* c.6 The SO cannot verify if the information is correct. c.7 The SO reviews the monitored areas to check if there is an intruder, and in that case the SO reports it to the PO and tries to collect manually information about the intrusion. c.8 PO request authorization to the SA to get the information stored in the system related to the incident reported . c.9 The PO verifies the intrusion and take the adequate measures for law enforcement. *d) Insufficient or inaccurate information collected by the system* d.8 The PO cannot verify the intrusion. d.9 Use Case ends.

Table 7: Use Case III description - Detection of unauthorized people

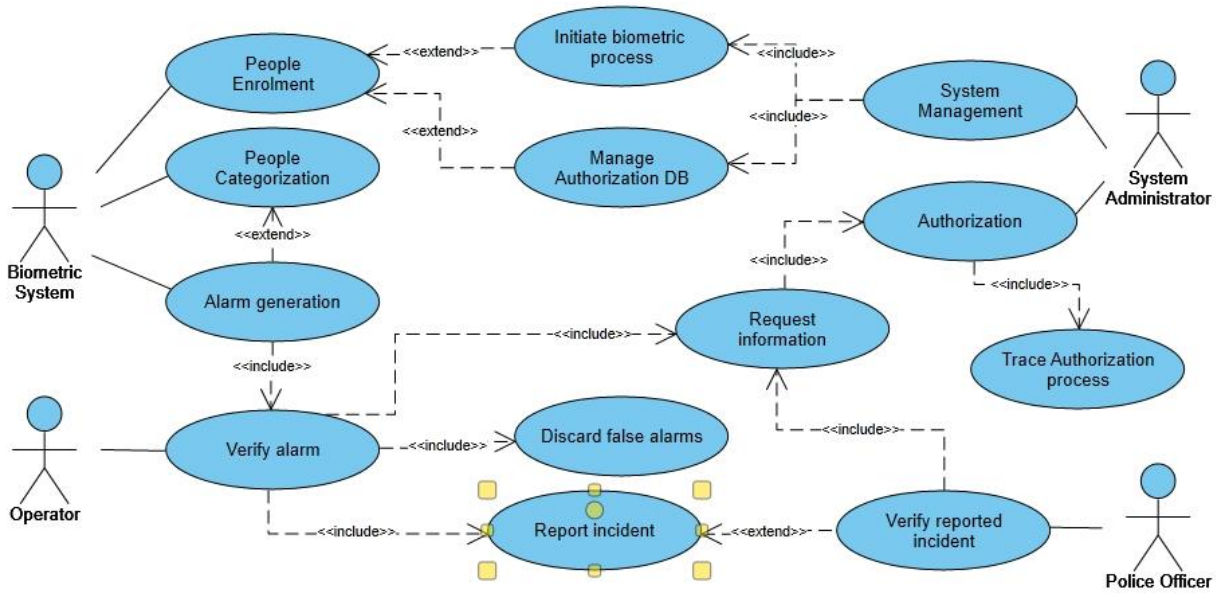

Figure 16: Use Case III diagram - Detection of unauthorized people

4 System overview

4.1 Technologies

For the recognition of people, the system will include a mechanism based on what we call **bodyprints**. A *bodyprint* is a vector of features of a person that uses physical characteristics, such as the height and width of a person and the color of his/her clothes, which are sufficiently distinctive to allow identifying and discriminating people, even with similar clothes.

For the extraction of a bodyprint, it is necessary to obtain 3D information of a scene and perform **segmentation and tracking algorithms** to detect a person in the images and collect enough information to generate the corresponding bodyprint.

Another specific algorithm is required for the **comparison** of templates, which is based on the particular features of the bodyprints.

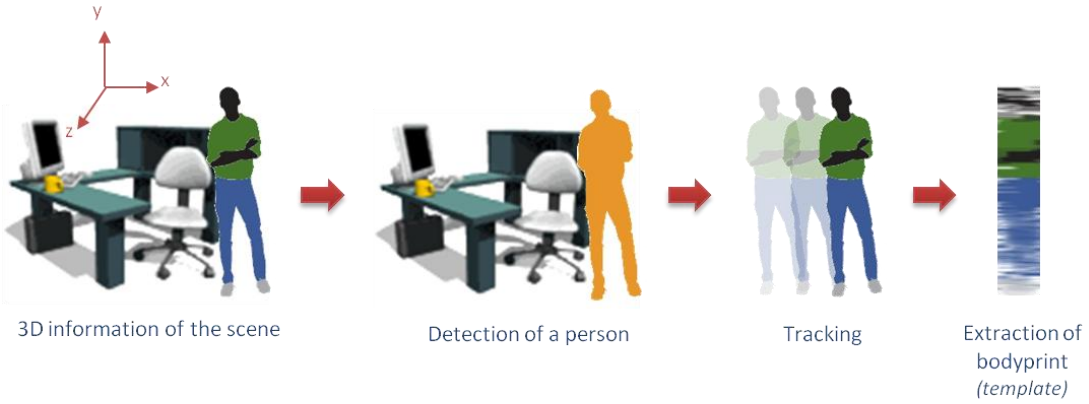

Figure 17: Extraction of bodyprints

4.2 Architecture Overview

The diagram below depicts the high-level physical architecture of the system, which is derived from the functional architecture proposed in the section §2.1.1. In this architecture, no physical devices are dedicated specifically to the enrollment of authorized people, as the enrollment is realized using the same devices as the one used to perform the surveillance of the building.

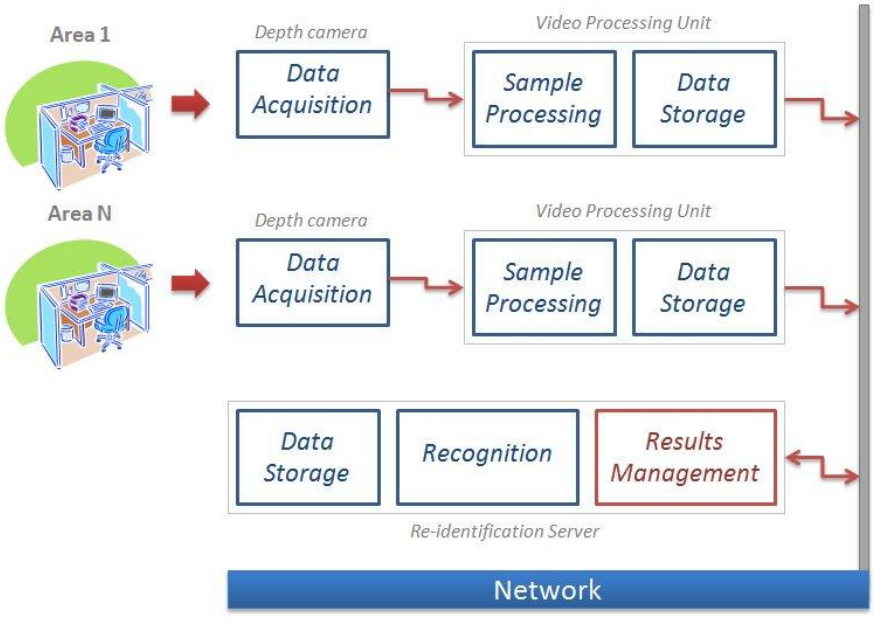

Figure 18: System diagram for the use case based on bodyprints

4.3 Components

The main elements composing the system are:

- *Depth cameras (DC)*: responsible for the capture of RGB and depth information of the scene, which will allow to extract biometric data from the individuals appearing in the images.

  The number of cameras to use depends of the area that has to be covered.

  Initially the depth camera selected is a Microsoft Kinect sensor, but other types of depth cameras, such as stereo cameras, are being tested to be used in the demonstrator.

- *Video Processing Units (VPU)*: responsible for the execution of the algorithms required for the detection and tracking of people in the images provided by the depth cameras, and the extraction of the corresponding bodyprints. This component will also store temporary the bodyprints extracted and the results of the tracking process.

  For each depth camera, a video processing unit is required.

  Still to be decided the specific platform for the video processing unit.

- *Re-identification server (RIS)*: responsible for the collection of bodyprints from the different VPUs and its comparison with the *Authorized People Database* (APDB).

  The APDB stores a set of bodyprints corresponding to the people authorized to enter the building at the defined period, which initially will be a maximum of 10 authorized people. This database will be implemented inside the RIS but could also be elsewhere.

  The RIS executes the matching and decision algorithms, and it is also in charge of generating and sending the alarms when necessary. Another database is required to keep information of the results of the recognition and the alarms generated to facilitate the auditing by the system operators or the authorities.

  Only one server will be used for all these tasks.

- *Data transmission blocks*:
  - *DC - VPU*: the cameras are directly connected to the video processing units through a data transmission cable.

    Data transmitted: RGB images, depth information.
  - *VPU - RIS*: the processing units and the server are connected to the same network (probably a Local Area Network), so network devices will be required. Depending on the capabilities of the selected server and processing units the connection can be wired or wireless, and different types of communication interfaces can be used (e.g. sockets, Web services).

    Data transmitted: Bodyprints, tracking information.
  - *RIS - System operators*: still to be decided how the biometric system will communicate with system operators to send them alarms anytime an unauthorized person is detected.

    Data transmitted: Alarms, *(optionally)* images.

5 Requirements

The objective of this section is to provide a set of requirements for both the biometric system and the SALT framework providing guidelines for its design.

Sections 5.1 to 5.5 describe the main requirements for the biometric system grouped by type, while section 5.6 collects all the requirements for the SALT framework for the design of the proposed biometric system.

5.1 Functional Requirements

This section describes the main functions that the biometric system shall perform for the detection of unauthorized people in the selected scenario.

5.1.1 Phases

The use of bodyprints to identify unauthorized people require two phases for the biometric process: enrolment and matching.

5.1.1.1 Enrolment

In this phase, the system extracts the *bodyprints* of the authorized people and stores all the data in a specific database (APDB). As mentioned in the scenario description, the APDB will store information of a maximum of 10 authorized people including security guards, and maintenance employees.

The enrolment requires two steps: the collection of data from the person to enrol with a depth camera and the processing of that information to extract the bodyprints. Both tasks can be performed online, but it is also possible to record the images at a certain moment and process the information later. Only the information obtained from the depth camera is required to enrol a person.

Anyway, the process is initiated and supervised by the System *Administrator*, who asks the people authorized to set themselves in the monitored areas in order to be captured by the depth cameras and detected. The processing of biometric samples is performed by one of the VPUs of the system, and once the bodyprints are obtained, they are stored in the database of authorized people (APDB) that is located in the RIS.

This is a summary of the enrolment process:

1. **Data Acquisition**
   - The system captures information from the person to be added to the group of authorized people.
   - *Output*: RGB and spatial information
   - *Components*: a depth camera (DC)
   - *Users*: Person Accessing (authorized person), and the System Administrator who initiates and manages the enrolment process
2. **Sample Processing**
   - The system processes the information captured and obtains the bodyprint for the person to be enrolled.
   - *Output*: bodyprint, tracking information
   - *Components*: a video processing unit (VPU), transmission cable to get data from the DC

- *Users*: the System Administrator can monitor the sample processing during the enrolment

3. Storage

- The system stores the information obtained in the previous step in the database of authorized people.
- *Components*: the VPU used, the Authorized People Database (APDB), a communication interface between the VPU and the APDB
- *Users*: the System Administrator can verify that the information has been stored correctly

This phase is included in **UC_BIO_3**.

5.1.1.2 Matching

For the matching phase it is first necessary to define the period of time in which the system should look for intruders, which in this biometric system demonstration corresponds to the non-working hours. During that time, when the system detects an individual, it obtains the associated feature vector (VPU) in order to compare it with the stored *bodyprints* (RIS). The aim of this comparison is to know whether or not the person appearing in the images of the office belongs to the group of authorized people, so the mode of operation of the system is: **categorization**.

This is the action protocol defined initially for the management of the results of the recognition process:

- *Positive match: authorized person detected*

  The system will not do anything with the results of the re-identification.
- *Negative match: the person is not in the database of authorized people*

  The system will generate an alarm, and will send a message to the System Operators providing information of the time and area where the intruder has been detected. The System Operators are in charge of verifying the alarms generated by the system and of taking the necessary steps anytime an intrusion is detected, which include reporting the incident to the local authorities.

This is the summary of the matching process for the categorization of authorized people:

1. Data acquisition

- The system captures information from a person appearing in the scene.
- *Output*: RGB and spatial information
- *Components*: the depth camera covering the area where the person appears (DC)
- *Users*: Person Accessing (authorized or not)

2. Sample processing

- The system processes the information captured and obtains the bodyprint for the person detected.
- *Output*: bodyprint, tracking information
- *Components*: a video processing unit (VPU), transmission cable to get data from the DC
- *Users*: None (automatic process)

3. Recognition

- The system compares the bodyprint extracted with the data stored in the system to decide if the Person Accessing is authorized or not.
- *Components*: the VPU used, the Authorized People Database (APDB), the Re-Identification Server (RIS) in charge of the comparison and the decision, a communication interface between the VPU and the RIS, a communication interface between the RIS and the APDB
- *Users*: None (automatic process)

4. Results management

4.1. Positive match

- The system does not do anything.
- *Components*: RIS
- *Users*: None (automatic process)

4.2. Negative match

- The system generates an alarm and sends it to the System Operator.
- *Output*: alarm (information of the incident)
- *Components*: RIS, device for alarm display, communication interface between these two components
- *Users*: System Operator

The main interactions of the users with the system during the matching phase are described in use case III for the particular case of a negative match (**UC_BIO_3**).

5.1.2 Data Management

The minimal information required by the system to perform the detection of unauthorized people is:

- The data captured by the depth cameras (RGB and spatial information)
- The period of time in which the system should perform the detection

Besides, it will be necessary to store other information from the users accessing the information stored in the system for management, verification or auditing tasks:

- Name or ID of the user
- Privileges (administrator/operator)
- Contact information (email/phone)

Any access to the data stored in the system should be recorded, in particular:

- Date and time of the access to the information
- Data that is consulted
- User having access to the information

The data management performed at the different phases of the biometric process can be summed up as follows:

People Enrolment

During the enrolment phase, this is the information captured and stored in the system for each authorized person:

- Identifier of the biometric template
- Biometric template *(bodyprint)*
- Date and time of the creation of the template
- User supervising the enrolment (administrator/operator)

This information will be consulted during the matching phase by the comparison process executed in the RIS, anytime a person is detected in the scene, to verify if that person belongs to the group of authorized people.

People Categorization

For the recognition, the information managed from each detected person is:

- Identifier of the biometric template
- Biometric template *(bodyprint)*
- Date and time of the creation of the template

This information is temporary stored in the VPU responsible for its capture until it is sent to the RIS for the comparison of templates. Once in the RIS, the biometric template is compared with each of the templates stored in the APDB to categorize the person detected.

The information used in the comparison and the results are stored in the RIS during the defined period for data retention.

Alarm management

In case there is a negative match, the system will generate an alarm and send it to the System Operator including at least this information:

- Date and time of the intrusion
- Area in which the intrusion was detected (camera ID)
- Identifier of the biometric template of the intruder

With this information, the System Operator can consult the RIS to get more information of the detected intrusion.

Optionally, the system could send directly an image of the intruder with the alarm to facilitate the verification process to the System Operator. If this image is required, it can be obtained during the people detection process, and stored in the RIS until the alarm is verified by the System Operator or the local authorities.

The history of alarms generated will be also stored in the system during a period of time defined by the Service Provider.

Data retention

It is important to define the criteria for data retention and deletion, particularly with regards to the biometric data stored in the system.

On the one hand, the information stored from the authorized people shall be updated and stored during all the lifecycle of the system since it is operational.

By the other hand, the biometric information of the people detected at the matching phase should be stored in the system during a period of time sufficiently long to allow the detection and verification of intrusions by the local authorities.

The data retention period is normally defined by the Service Provider, and should comply with the existing regulations on data protection. For example, the Instruction 1/2006 of the Spanish Data Protection Agency stipulates that the maximum period for the conservation of images is

one month [3]. Thus, if finally images of the intruders are used by the system, they will be stored for a period of time of minimum one day and maximum one month.

5.1.3 List of functional requirements

Taking into account the scenario described, these are the minimal functions that the system should perform:

Id	Functional requirement
FR_1	The system shall be able to capture spatial and RGB information
FR_2	The system shall be able to detect people appearing in the scene
FR_3	The system shall be able to track the people detected
FR_4	The system shall be able extract features of the people detected
FR_5	The system shall be able to create a template for each person detected
FR_6	The system shall allow to discard low quality templates
FR_7	The system shall be able to store information of the people detected
FR_8	The system shall be able to compare and match the templates of the people detected
FR_9	The system shall be able to decide if a person detected belongs to a defined group
FR_10	The system shall be able to generate alarms
FR_11	The system shall be able to send alarms to certain users
FR_12	The system shall be able to store information of certain users
FR_13	The system shall allow to discard false alarms
FR_14	The system shall allow to access the information of the people detected
FR_15	The system shall allow to delete the information of the people detected
FR_16	The system shall allow to configure the recognition parameters
FR_17	The system shall allow to define the detection period
FR_18	The system shall allow to initiate manually the enrolment process
FR_19	The system shall be able to record the accesses to the information of the people detected
FR_20	The system shall be able to delete automatically certain information stored after a defined period of time

Table 8: List of functional requirements

5.2 Operational Requirements

The main concepts for how the system is used are described in this section.

5.2.1 System operations

The system performs several operations automatically, such as these:

- Initiating the recognition process during the detection period
- Detection and tracking of people appearing in the scene
- Extraction of biometric templates from the people detected
- Categorization of the people detected
- Generation of alarms in case of negative match
- Record the accesses to the information stored in the system

Other operations require the supervision or the participation of one of the system users:

- The enrolment of authorized people in the system, which is initiated and monitored by the *System Administrator*.
- The configuration and start up, which is performed by the *System Administrator*.
- Management of the Authorized People Database (APDB), that may require the update, modification or deletion of the information stored, which is handled by the *System Administrator*.
- Creation of system users and authorization, that is the responsibility of the *System Administrator*.
- Verification of system alarms, that is performed by the *System Operator*.

The VPUs and the RIS, once configured, are able to communicate and perform the biometric process for the detection of unauthorized people without any user interaction, and in general, all the interactions of the users with the system are performed through the RIS, either using a specific user interface or directly connecting to the server.

The flow of information during the categorization process is initiated when the VPU detects a person in the images provided by the depth camera. This component processes the biometric sample to extract the bodyprint of the detected person, which is temporary stored in this VPU with the tracking information used to obtain the mentioned bodyprint. The VPU performs also a quality control process to discard low-quality samples.

Once a VPU extracts a bodyprint, it sends it automatically to the RIS that performs the comparison and decide if the person is authorized or not. In case of negative match (not authorized), the RIS generates an alarm including information related to the alleged intrusion and sends it to the *System Operator*. This can be implemented in different ways:

- The RIS sends an email or other type of notification to the device for surveillance of the System Operator (e.g. a mobile phone, a tablet PC, a netbook, etc.).
- The RIS publishes the alarms generated in a private user interface that is being monitored by the *System Operator* using a device for surveillance (e.g. a computer, a mobile phone, etc.).

For the verification of alarms, the *System Operators* or the auditors access the information stored in the system through the RIS. For this, they have first to request authorization to the *System Administrator*.

5.2.2 User interactions

These are the users interacting directly with the biometric system:

User	Actions	Privileges	Skills
System Administrator	• Configuration of the system • Creation of system users • Provide authorization to other users to access certain information • Technical assistance to auditors • Enrolment management • Manage the APDB (add/edit/remove) • Access to all the information stored in the system	*All privileges*	*Advance knowledge on computers (DB management, user management)* *Basic knowledge on how the system works*

System Operator	• Reception of alarms • Review of information related to an alarm • Deletion of alarms • Report incidents to local authorities • Collaboration with local authorities	*Read access to certain information, deletion of alarms*	*Basic knowledge on computers*
Auditor	• Review information related to an incident • Review information stored in the system	*Read access to certain information*	*None*

Table 9: Summary of user interactions

5.2.2.1 System Administrator

The *System Administrator* is responsible for the global management of the system. Thus, this user should have advanced knowledge on computers, particularly on database management and user management. Furthermore, this user should know how the system works as it is also responsible for the user enrolment.

The core of the biometric system is located at the Re-Identification Server (RIS), therefore the *System Administrator* should have access to this component and all the privileges to perform the tasks as administrator. This user can connect to this server locally or remotely (e.g. via SSH).

Preferably, all the interactions should be performed via user interfaces that simplify the tasks of the *System Administrator* and that reduce the skills required for this user, but it is not mandatory.

For the configuration of each Video Processing Unit (VPU), the *System Administrator* should also have access to these components, either directly or through the RIS.

Some tasks are performed just at the set-up stage of the system, such as the configuration that, if correct, should not be changed except for editing the detection period. Also at this stage, the "operator" users can be created with enough privileges to access information related to incidents.

The provision of authorization for other users will be performed on demand, that is to say, anytime a user requires access to any information stored in the system for auditing purposes.

During the auditing process, the *System Administrator* will also assist the *Police Officer* or the *Data Protection Officer* to retrieve the information they request from the system.

In the biometric process, the tasks executed by the *System Administrator* that are critical for the success in the detection of unauthorized people are the configuration of the system and the correct enrolment of authorized people.

5.2.2.2 System Operator

The *System Operators* are mainly responsible for the management of the results of each recognition process. For this, they receive the alarms generated in case of unauthorized access and they shall be able to verify the intrusion.

The *System Operators* can be the security guards or other people in charge of monitoring the facilities, which should have the minimum necessary skills to retrieve information related to an incident from the system without the assistance of the *System Administrator*.

Anytime the system detects an intrusion, the *System Operator* shall receive a notification or a message warning about the incident. The next step is to connect to the RIS and get more information related to the event, such as tracking information, or check manually if there is an intruder by reviewing the live videos provided by the video surveillance system or by patrolling the office. The false alarms are discarded, that means that they are deleted from the history of alarms or marked as false alarms.

In order to retrieve information from the system, there are several possibilities:

- The system can provide a user interface to facilitate the access to the incidents detected, which can be located in the RIS.
- The *System Operators* are educated on how to get the information manually with a set of simple guidelines. The information is directly extracted from the component that stores it (RIS, APDB or VPU).

For the access to the information stored in the system, the *System Operator* has to request authorization from the *System Administrator*, and any access to the information shall be recorded. This request can be performed as soon as a person is assigned to be a *System Operator*. At that moment, the *System Administrator* creates a new system user with the necessary privileges to access the information related to incidents.

Once an intrusion is confirmed, the *System Operator* is in charge of reporting the incident to the local authorities. The *System Operator* shall also collaborate with them on anything required.

The most critical task of this user is the correct verification of alarms.

5.2.2.3 Auditors

These users are the *Police Officers* or the *Data Protection Officers* who require access to certain information stored in the system to verify an incident or the compliance of the system with the current regulations.

In any case, they will first have to request authorization to the *System Administrator* to have access to the information, for which they have to identify themselves correctly and indicate the purpose of the access to the information.

Once they have registered to access the information, as they are not required to have special skills, they should be able to get the information as easily as possible. For this, there are several possibilities:

- The SA records the requested information in a portable drive and provides it to the auditors.
- The system provides a user-friendly interface facilitating the access to the information stored. In this case, the UI will be hosted in the RIS, as it centralizes the information related to the alarms generated and it has access to the APDB.
- The auditors are educated on how to get the information manually with a set of simple guidelines. In this case, the data is directly extracted from the component that stores it (RIS, APDB or VPU).

Anyhow, they can be assisted in the process by the *System Administrator*.

The information provided with the alarm and the tracking information recorded when a person is detected can be useful to verify an unauthorized access.

To verify that the system complies with the current regulations, it may be required to provide also the system logs and the information stored in the APDB.

In this case, the critical task is the collection of information.

5.2.3 Operational performance parameters

5.2.3.1 Response time

The response time of the biometric system refers to the period of time required since a person is detected until the result of the categorization process is available.

The requirements for this parameter are provided by the *System Owner*. In this case, it is not necessary to perform the detection in real time, as anytime an intrusion is detected it requires time to verify it and report it to the authorities, and the necessary law enforcement measures can be applied in subsequent days. On the other hand, an early detection may allow *System Operators* to collect more evidences of the intrusion that can be useful for law enforcement. Thus, the system should provide a result as soon as possible but in this case there is no response time constraint. In general, a response time of less than an hour can be considered as useful.

5.2.3.2 Availability

The whole system (VPUs, RIS and ADPB) shall be operating correctly during the enrolment process and the detection period defined. The access to the data stored for verification or auditing purposes does not require the system to process biometric samples.

The maintenance operations should be preferably performed out of the detection period, when they have no impact in the process of detection of unauthorized people.

5.2.3.3 Accuracy

The accuracy refers to the capability of the system to operate correctly. We will focus on the accuracy of the biometric process, i.e. on the expected and accepted errors in the recognition process.

A false negative, which means that a person authorized is matched as non-authorized (no match), has less impact on the surveillance goal than a false positive (match), as every negative match produces an alarm that can be verified and discarded by a *System Operator* while a false positive does not. Anyway, each time a person is detected in the scene the biometric system will try to recognize him/her, and the same person may be detected many times during the same period of access to the office, so the system can make several attempts to detect an intrusion correctly and reduce the error rate.

To reduce the impact of false positives, the system will store temporary the information of the people categorized in a session for at least one day. The maximum retention period for this data will be decided by the *Service Provider* according to the existing regulations.

All in all, an error rate of around 20% in the categorization process is considered reasonable as a performance target, as the technology used for the recognition is still under development and the system errors can be easily corrected.

5.2.4 List of operational requirements

List of operational requirements:

Id	Operational requirement
OR_1	The system shall be able to initiate the recognition process automatically
OR_2	The system shall be able to perform the categorization process automatically
OR_3	The system shall be able to generate alarms automatically when an unauthorized person is detected
OR_4	The VPU and the RIS shall be able to communicate without any user interaction
OR_5	Information about how to configure the system shall be provided to the System Administrator

OR_6	Information about how to access certain information shall be provided to the users with authorization to retrieve it
OR_7	The System Administrator shall be educated on how the biometric system works
OR_8	The System Administrator shall be able to manage other system users
OR_9	The System Administrator shall be able to authorize the access to the information stored in the system
OR_10	The System Administrator shall be able to configure the recognition parameters
OR_11	The System Administrator shall be able to define the detection period
OR_12	The System Administrator shall be able to initiate the enrolment process manually
OR_13	The System Administrator shall be able to access the information stored in the system
OR_14	The System Administrator shall be able to delete the information of the people detected
OR_15	The System Administrator shall assist the Police Officers and the Data Protection Officers for auditing tasks
OR_16	The System Operator shall be able to receive notifications of the system in case of alarm
OR_17	The System Operator shall be able to access the information of the people detected
OR_18	The System Operator shall be able to discard false alarms
OR_19	The System Operator shall be able to report incidents to local authorities
OR_20	The System Operator shall collaborate with the local authorities in the verification of an intrusion
OR_21	The Police Officer shall be able to obtain information related to a particular incident
OR_22	The Data Protection Officer shall be able to obtain information stored in the system
OR_23	The system should be available at least during the period defined for detection
OR_24	A reasonable error rate for the system is 20% of false recognitions

Table 10: List of operational requirements

5.3 Technical Requirements

The biometric technology selected imposes most of the technical requirements for the system. On one hand, it requires the use of depth cameras and a large processing capacity for the extraction bodyprints, that requires the execution of algorithms for detection, tracking and feature extraction. The number of cameras depends on the area to cover, that should be at least the main transit areas of the office. To generate the bodyprints in a reasonable period of time, it is recommended to use one processing unit (VPU) per depth camera (DC), so the number of VPUs will be the same as the number of DC.

To coordinate the work of the different processing units and facilitate the comparison process, the system will be **centralized**. A central server (RIS), will be responsible for collecting and comparing the bodyprints from the different processing units.

Regarding the data storage, every processing unit will include a storage for the temporary information obtained during the image processing for the extraction of bodyprints. Besides, the RIS includes the APDB and other storage for the data obtained from the VPUs, the results of the comparison and the alarms generated. The type of data storage will depend on the format of the data stored. In general, file systems and basic databases will be used.

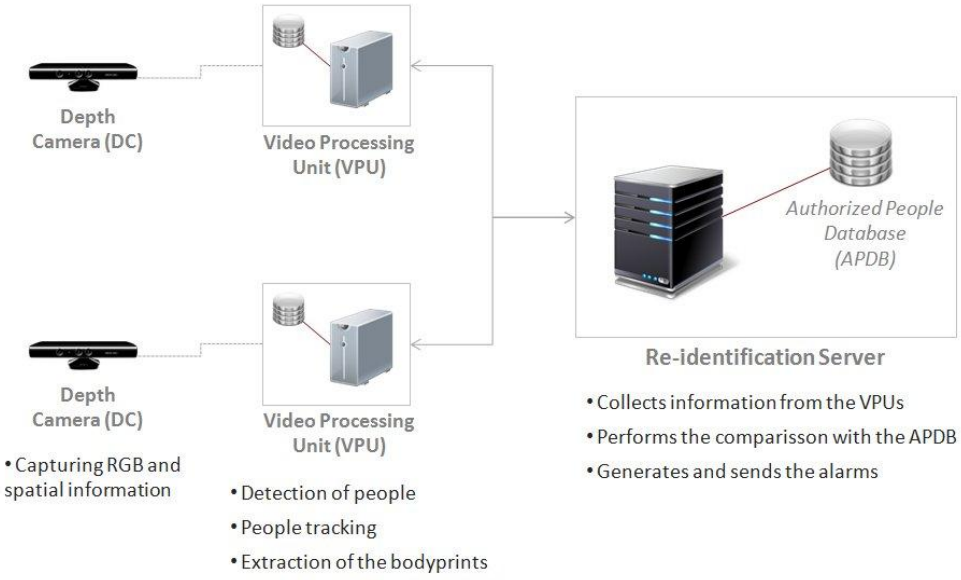

Figure 19: Centralized system configuration

For the implementation, the DC will be directly serving images to the VPU through a data transmission cable. It is just required a program for video stream capturing in the VPU to obtain the RGB and depth images from the camera.

The APDB, as mentioned, will be included in the RIS to simplify the implementation. This database will store templates from a maximum of 10 authorized people. Although the templates do not reveal any personal information, the access to this information will be tracked.

The most critical block in the data transmission of the biometric system is the communication between the VPUs and the RIS. The VPUs may optionally provide tracking information to the RIS for auditing purposes that could include images of the scene. This images will be properly secured by partial or total encryption during the transmission. Once stored in the RIS, only the *System Administrator* should have access to that information.

To reduce the exposure of the communication, the VPUs and the RIS will transmit the information through a Local Area Network (LAN) with the adequate security measures to protect the information shared. The connection of the different components to the network can be wired or wireless depending on the capabilities of the selected devices. Still to be decided the communication interfaces that will be used (e.g. sockets, Web services).

The RIS will also have to provide information to the *System Operators*. If the alarms include images to facilitate its verification, those images will be properly protected during the communication between the RIS and the device used by the System Operator for monitoring the facilities.

Any other user requiring information from the system will have to access that information through the RIS using one or several user interfaces with authentication and authorization mechanisms. The users can connect directly to the RIS or remotely. In any case, the access to the information stored in the RIS will be controlled and recorded.

The system does not have special requirements of scalability, as it is not expected to have many users connected to the system at the same time or a huge database of authorized people. Only the number of DC-VPU pairs may be increased to cover more areas in the office. In this case the RIS shall be able to handle them and still provide the results in the required response time, but

if necessary, more servers can be used as RIS sharing the same APDB. For this implementation only two or three DC-VPU pairs will be implemented, so only one RIS is necessary.

Furthermore, for the execution of the algorithms for bodyprint extraction and comparison, Linux or MAC OS is required, so the VPUs and the RIS shall use one of those operative systems.

This is a summary of the technical requirements:

Id	Technical requirement
TR_1	The cameras used shall cover the main transit areas of the office
TR_2	There shall be one VPU per DC
TR_3	The system shall be centralized
TR_4	Each VPU shall include data storage for the temporary files
TR_5	The RIS shall be connected to the APDB
TR_6	The RIS shall include data storage for the results of the comparison and the alarms
TR_7	The access to the APDB shall be able to store templates from at least 10 people
TR_8	The access to the APDB shall be traced
TR_9	The communication between the VPUs and the RIS shall be properly protected
TR_10	The user interfaces in the RIS shall implement access control mechanisms
TR_11	Authorization shall be required to access the images stored in the system
TR_12	The VPUs shall use Linux or MAC OS
TR_13	The RIS shall use Linux or MAC OS

Table 11: List of technical requirements

5.4 Environmental Requirements

As mentioned in the scenario description, the system will be implemented in a private office, so it shall be designed to operate **indoors**. The system shall cover the main transit areas of the office to detect the access of any authorized person to the facilities.

Regarding the environment, each component requires different conditions. The sensors are the most critical elements in this case limiting the light, humidity and temperature conditions. Initially, the sensor selected for the capture of RGB and spatial information is a *Microsoft Kinect sensor*, that can operate correctly under the conditions of a common workplace (17 - 27 °C)[4]. The most relevant factors for the sensors are the light and the position of the sensor:

- The light conditions shall be adequate to distinguish correctly the people in the images. Besides, the sensors shall be kept out of direct light.
- The distance from the sensor to the elements being monitored determines the spatial and depth resolution, which for a Kinect sensor is as follows [4]:
    - Spatial resolution (@ 2m distance) = 3mm
    - Depth resolution (@ 2m distance) = 1cm

  In this case, the depth sensor also includes a limitation for the distance to the objects being monitored, ranging from 0.8 to 3.5 meters.

  The recommendation for the correct extraction of bodyprints is to use one Kinect sensor to cover an area of a maximum of 5 x 3 meters.

List of operational requirements:

Id	Environment requirement
ER_1	The system shall operate indoors
ER_2	The system shall be able to operate correctly at temperatures ranging from 17°C - 27°C
ER_3	The system shall be able to operate correctly in normal humidity conditions
ER_4	The system shall be able to operate correctly with ambient lightning
ER_5	Each depth camera shall cover a maximum area of 5 x 3 meters
ER_6	Each depth camera shall be placed at a minimum of 0.8 meters of the objects

Table 12: List of environmental requirements

5.5 Privacy and Security Requirements

In this section, the most important requirements related to privacy and security are presented. These concerns are normally provided by the *System Designers*, but under the SALTed design process, we expect to get all this information from the SALT Framework.

Figure 20 shows the most critical elements of the demonstration biometric system affected by security or privacy threats.

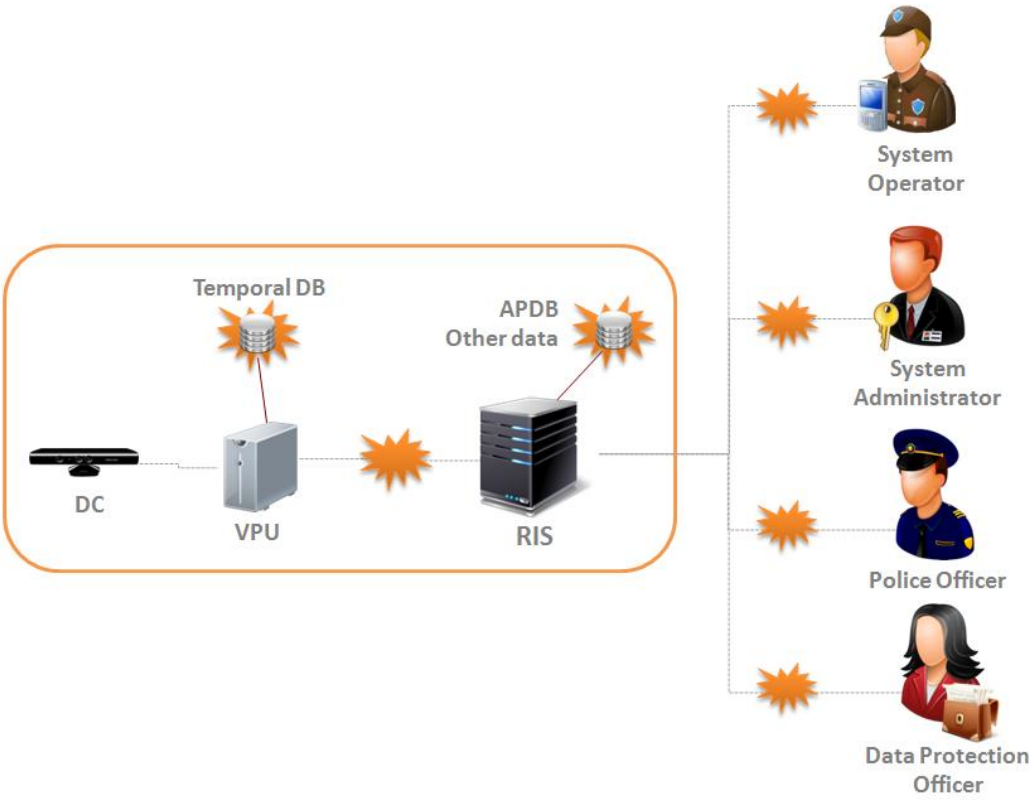

Figure 20: Critical elements of the system in terms of privacy and security

5.5.1 System components

Regarding the data storages, any information obtained from the system users (PA) should be adequately protected to prevent it from being stolen, misused or manipulated.

In this system, the only personal identifiable information collected are the images captured by the depth cameras. Those images are used to obtain tracking information that is necessary for the generation of bodyprints, and they can also be used to verify the alarms generated, so they will be temporary stored in the system (initially in the VPUs, and later in the RIS).

Regarding the bodyprints, they do not reveal by themselves any personal information, as they contain information of the color and shape of a person that is saved in the system as an abstract image. The problem is that a bodyprint can be temporary linked with one of the images of a person stored in the system through the template identifier. Those images can be used to determine that a specific individual was in a specific place at a certain hour, which clearly affects the privacy of the individual. For all these reasons, the images shall be properly protected, for example, with total or partial encryption, so that it is not possible to retrieve the clear images without authorization. This protection mechanisms shall be implemented in any component of the system that stores images (VPU, RIS).

The only users that should have access to the bodyprints and to the complete images are certain authorized employees responsible for monitoring system (e.g. the *System Administrator* and the *System Operator*), the certified auditors *(Data Protection Officer*) and the authorities (*Police Officer*). The roles of each of these users have to be defined from the start, being the *System Administrator* the only user with permissions to add, delete or modify the data storage in the system. Besides, the *System Administrator* is responsible for authorizing any access to the system. The other users will only have read access to the information and should request access to the *System Administration* before consulting the data stored in the system. Anyway, for accountability purposes, every access to the personal identifiable information shall be recorded.

Moreover, for the proper detection of intruders in the selected scenario, it is necessary to guarantee the integrity of both the templates of the authorized people stored in the system and the templates obtained during the detection period (i.e. the bodyprints). The use of tampered templates could cause errors in the categorization of people, which is specially critical in the case of a false positive, where an intruder is recognized as authorized person and enters the restricted area. It is then necessary to implement mechanisms for the protection of the bodyprints in any component that stores them (VPU, RIS, APDB).

In addition to all these risks, the system availability can also be reduced through a denial of service attack, which will cause the suspension of the intrusion detection service temporarily or indefinitely. The RIS is the component more susceptible to this kind of attacks, as it performs the categorization and stores the templates of the authorized people and the images associated to the alarms generated. The VPUs are also important, as they capture the images and generate the bodyprints, but with just one VPU it is possible to provide an intrusion detection system. Thus, the VPUs and the RIS should implement adequate security measures to prevent or mitigate a denial of service attack.

5.5.2 Data Transmission

During the detection of unauthorized people, the communications between the VPU and the RIS are the most susceptible to be interfered. If the VPU captures an unauthorized person but the corresponding template is lost or manipulated before getting to the RIS, that could affect the categorization of people, which again is particularly serious in case it produces false positives.

The alarms generated could also be intercepted before being displayed to the *System Operator,* who may not be warned about the intrusion if the alarm is lost. As the alarms can include an image of the intruder, this could lead to an unwanted disclosure of personal identifiable information. To prevent this, the transmission shall be adequately protected, and the alarms should be sent periodically until the *System Operator* verifies them. In addition to this, a history of the alarms generated will be stored in the RIS, which could mitigate the loss of alarms.

As the depth cameras are directly connected to the VPUs through a data transmission cable, that transmission block is not susceptible to be intercepted.

To reduce the risks of external attacks, all the components should be connected through a Local Area Network (LAN).

5.5.3 Other considerations

The Spanish Data Protection Agency (AEPD in the Spanish acronym) provides a guide on video surveillance that collects all the recommendations and obligations that must be followed to perform video surveillance activities complying with the current regulations in Spain regarding privacy and data protection [5].

The video-based biometric system for intrusion detection described in this document, will be deployed at the Visual Tools headquarters in Madrid as an extension of the existing video surveillance system. This deployment will serve as a real case study to demonstrate the use of the SALT Framework for the design of a biometric system to control the access to the office at non-working hours taking into account the privacy and accountability concerns.

This biometric system shall comply with the principles provided by the AEPD regarding image capturing and processing for security purposes, that point to the following legislation [5]:

- The Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD)
- The Regulation developing the Data Protection Act 15/1999 of 13th of December (RDLOPD), approved by Royal Decree 1720/2007 of 21st of December
- The Instruction 1/2006 of 8th of November of the Spanish Data Protection Agency on the processing of personal data for surveillance purposes by means of camera or video camera systems

These regulations establish a few obligations that must be carried before starting any video surveillance activity:

- **File registration**: First of all, the AEPD must be notified about any video surveillance activity that requires the creation of files, which includes the recording or storage of images. For this, it is necessary the registration of the system in the Agency's General Register. In this registry, the policies on privacy and data protection are specified, including the type of data recorded and purpose of the collection of the information, the rights of the users to update or delete their information, and the contact information of the entity who is responsible for the data.
- **Duty to inform**: Instruction 1/2006 imposes the obligation to use and display a specific informative sign that shall be placed at least at the entrances to the areas under surveillance.

5.5.4 List of privacy and security requirements

Id	Privacy and security requirements
PSR_1	The images stored in the system shall be protected
PSR_2	The bodyprints stored in the system shall be protected
PSR_3	The alarms generated shall be periodically sent until they are verified by the System Operator
PSR_4	A history of the alarms generated shall be stored in the system
PSR_5	The System Administrator is the only user with permissions to add, modify or delete the data stored in the system
PSR_6	The System Administrator is the responsible for providing authorization to access the data stored
PSR_7	The system shall record any access to the information stored in the system

PSR_8	The communication between the VPUs and the RIS shall be adequately protected
PSR_9	The system should implement adequate security measures to prevent or mitigate a denial of service attack
PSR_10	The different components should be connected through a LAN network
PSR_11	The system shall comply with the Spanish regulations on privacy and data protection

Table 13: List of privacy and security requirements

5.6 SALT framework requirements

Only two users interact with the SALT Framework during the lifecycle of the biometric system:

- The *System Designer*, who uses the framework to get recommendations concerning privacy and accountability for the design of the biometric system, and who also uses the framework to validate the design as SALT compliant.
- The *Data Protection Officer*, who may require access to the recommendations that have been provided for the design of the system being audited.

The following sections describe the interactions of these users with the system in each case.

In any case, the users should first know which tools are provided by the SALT Framework, and which information can be extracted with them and how, so the framework shall be adequately documented.

It is also desirable that the information shared with the SALT framework is adequately protected and not shared to third parties, unless it is required for auditing purposes. In the same way, the accesses by the different users to the SALT Framework for the extraction of recommendations or for validation should be recorded.

5.6.1 Obtaining information from the SALT Framework

This task corresponds to use case **UC_BIO_1**: once the *System Designer* has collected all the requirements from the *System Owner* and the *Service Provider*, it is time to get some guidelines from the SALT framework that facilitate the design of the biometric system taking into account the privacy and accountability aspects from the start. These guidelines are provided in the form of concerns and recommendations that can be implemented to take into account those concerns. Besides, in some cases, the recommendations will be given with a set of OCL rules that can be used for the validation of the system.

As the guidelines depend on the specific context and features of the system, the *System Designer* shall be able to provide the characteristics of the system based on the requirements collected to the SALT Framework. This action require the use of an interface that allows the *System Designer* to introduce information of the different types of requirements (operational, technical, business constraints, etc.), features and procedures that are relevant for the selection of policies and recommendations concerning privacy and accountability.

The SALT Framework will analyse these specifications and will search in the knowledge repository the instances that are most adequate for that particular system. This instances shall be provided to the *System Designer* in a user-friendly way, taking into account that the *System Designer* does not necessary have background on ethics or laws, so it would be useful to provide also complementary information on how to apply the different recommendations.

The interface used for this process should be suitable at least for a user with the profile or skills of a *System Designer*, who has certain technical knowledge, and should provide feedback and visual hints to facilitate the process of extraction of knowledge from the framework.

5.6.2 Validating the system design

The validation of the system is also described in use case **UC_BIO_1**: the *System Designer* elaborates a design of the biometric system based on the requirements given by the *System Owner* and the *Service Provider*, and also based on the guidelines obtained from the SALT Framework. Before the implementation and deployment of the system, the *System Designer* should verify that the design complies with the recommendations on privacy and accountability provided by the SALT framework. If the recommendations obtained in the previous phase include OCL rules, this verification can be automatically performed using the SALT Framework. In that case, an interface is required to introduce the design created and display the results of the validation process. This interface should be adapted for a user with a technical profile that may not have knowledge on system modelling, so the design shall be introduced in a format easily understandable by the *System Designer*. Besides, this interface should provide feedback and visual hints to facilitate the process of validation, including clear warnings to point to the concerns not fulfilled.

After being implemented, the system should also be validated anytime it is modified to check that the resulting system also addresses the SALT concerns.

5.6.3 Auditing the system

This task is described in **UC_BIO_2**. During the audit of the system, the *Data Protection Officer* may require access to the SALT Framework in order to review the technical privacy policies, logs and compliance rules in the SALT knowledge repository that have been used to elaborate the recommendations for the system being audited. The user of the SALT Framework in this case has background in laws and current regulations, but does not have to have any technical expertise, so appropriated documentation about how to use the framework is required.

5.6.4 List of requirements for the SALT Framework

Some of the requirements for the SALT Framework have already been defined in D3.1 *(REQ_FU_X)*. We add to that list other requirements focused on improving the user experience *(REQ_FU_X.*X related to a more general requirement *REQ_FU_X)*.

Id	SALT Framework requirement
REQ_FU_0	General requirements for the SALT Framework
REQ_FU_0.1	Users should be adequately informed about the different tools provided by the SF, for which purpose and how to use them
REQ_FU_0.2	The information shared with the SF shall be adequately protected and not shared with third parties except for auditing purposes
REQ_FU_0.3	The accesses by the different users to the SF shall be recorded
REQ_FU_2	The SALT management tool should provide an interface to system designer for describing context information of design requirements
REQ_FU_2.1	The interface for the extraction of recommendations shall be adequate for a user with technical profile
REQ_FU_2.2	The interface for the extraction of recommendations shall provide feedback and visual hints to facilitate its use
REQ_FU_2.3	The interface for the extraction of recommendations shall be adequately documented
REQ_FU_3	The SALT management tool might document the purposes and reasons for all decisions

	made in the design process
REQ_FU_4	The SALT management tool might be able to verify a system design is SALT-compliant or prompt warnings if the technical decisions harm privacy
REQ_FU_41	The interface for the validation of the system shall be adequate for a user with technical profile and without knowledge of system modelling
REQ_FU_42	The interface for the validation of the system shall provide feedback and visual hints to facilitate its use, especially when the system is not valid
REQ_FU_43	The interface for the validation of the system shall be adequately documented
REQ_FU_5	The Surveillance system designer introduces in the SALT management tool the specification of the Surveillance system
REQ_FU_5.1	The designer shall be able to introduce different type of requirements and features for the system
REQ_FU_6	The SALT management tool has to select a proper instance or instances based on the specification done by the system designer
REQ_FU_7	The SALT management tool shows in a proper way the recommendation to the new system based on the instances
REQ_FU_7.1	The information shall be provided in a user-friendly way, taking into account that the System Designer does not necessary have background on ethics or laws
REQ_FU_7.2	The framework should optionally provide information on how to apply the different recommendations
REQ_FU_8	Auditors should have access to technical privacy policies, logs and compliance rules in the SALT knowledge repository through the SALT management tool
REQ_FU_9	The SALT management tool should provide pointers to existing compliance checking mechanisms to users of the framework, depending on the privacy policy language used, if any exist.
REQ_FU_10	The SALT management tool should provide pointers to relevant information, such as official specifications, in case the privacy policy language is a commonly used one
REQ_FU_11	The SALT management tool might be able to issue a certificate guarantying the design process has been SALTed
REQ_FU_12	The SALT management tool might be able to propose a check list that enables to check periodically that the system privacy level has not been modified
REQ_FU_13	The SALT management tool may be able to propose light guidelines enabling fast SALT compliance checking when slight modifications are realized

Table 14: List of requirements for the SALT Framework

6 Evaluation criteria

In this section, several notions for the evaluation at SALT framework level and at biometric system level are presented. These criteria cover the different stages during the lifecycle of the biometric system. Other aspects related to the introduction of information in the SALT knowledge repository are kept out of this section.

6.1 Evaluation at the SALT framework level

The objective of this section is to specify a set of criteria that serves to evaluate if the SALT framework provides the results expected (this at the different stages of the lifecycle of the system proposed). For this, it is first necessary to define the **goals** or aspects of the framework that have to be evaluated (SFG_X).

- *SFG_1: Functional aspects of the SALT Framework*

  The SALT Framework shall provide all the capabilities required by the different users during the biometric system lifecycle, thus the first goal consists of evaluating if the SALT Framework includes all the functionalities needed, which are:
  - Provide a tool to introduce the specification of a system.
  - Provide a list of references about accountability and privacy for a particular system.
  - Provide a tool to introduce in the SF the profile of a biometric system.
  - Provide a tool for the validation of the system (OCL rules).

- *SFG_2: Data requirements for the SALT references*

  The SALT references shall provide useful information for the design, development and deployment of SALT compliant systems. Thus the second goal is to verify that the references provide the necessary concerns and recommendations about privacy and accountability, and that they are adequate to the system specified. For the evaluation of each reference, these are the aspects that will be considered:
  - If they are able to provide useful information to help make design decisions
  - If they are reliable and cover the most important concerns
  - If they do not provide unrelated information or the amount of unrelated information is acceptable

  A set of test use cases can be used for the evaluation of this criteria, allowing to verify if the SALT Framework provides the references expected for existing and known SALT compliant systems.

- *SFG_3: Usability of the SALT Framework*

  The SALT Framework shall be adequate to its users, so this goal will be focused on evaluating usability of the framework. In particular, the requirements of section 5.6.4 will be checked. This evaluation can be performed through surveys and questionnaires that collect the feedback of a group of test users about the utilization of the SALT Framework.

The following table summarizes the aspects that should be evaluated for each of the goals defined:

Goal	Evaluation criteria	Aspect to evaluate	Type of evaluation	Instrument
SFG_1	The SALT Framework includes all the capabilities required during the design process	Usefulness/ Functionality	qualitative	Human inspection: verification that all the tasks listed under SFG_1 can be performed with the SALT Framework.
SFG_2	Relevance of the references to the system specified	Efficiency	qualitative	Human inspection: check if the recommendations are really applicable to the system specified. Use of test cases.
SFG_2	Provision of concerns about accountability	Efficiency	qualitative	Human inspection: check if the references cover the main accountability concerns for the system specified. Use of test cases.
SFG_2	Provision of concerns about privacy	Efficiency	qualitative	Human inspection: check if the references cover the main privacy concerns for the system specified. Use of test cases.
SFG_2	Accuracy of the references	Reliability	qualitative	Software or human inspection (experts) of the information sources: check if the references are valid and updated. Use of test cases. ** UMA is studying to apply reputation software based on user and expert opinion.*
SFG_3	Easy to learn	Usability	quantitative	Time required to perform several predefined tasks
SFG_3	Easy to use	Usability	qualitative	Survey to extract the opinion of different users

Table 15: Evaluation criteria at SALT Framework level

6.2 Evaluation at the system level

In this case, the criteria are focused on evaluating if the design process defined leads to the creation of a SALT compliant system. For this evaluation, these are the goals defined (*DPG_X*):

- *DPG_1: Functional aspects of the biometric system*

  A SALT compliant biometric system shall provide a certain surveillance service, so the first goal of the evaluation at this level is the verification that the system does what it is supposed to do, which in this case is the detection of non-authorized people in a private office. For the evaluation of the functional aspects of the system, the following acceptance test cases will be used, which are based on **UC_BIO_3** and cover the positive scenarios:

TEST_CASE_1: Detection of a non-authorized person	
Preconditions	The biometric system has been properly installed and configured.

	The biometric system covers the main transit areas of the private office. The authorized people have already been enrolled in the system.
Test case	An unauthorized person enters the office.
Expected result	The system generates an alarm giving information of the intrusion and sends it to the *System Operator*.
TEST_CASE_2: Detection of an authorized person	
Preconditions	The biometric system has been properly installed and configured. The biometric system covers the main transit areas of the private office. The authorized people have already been enrolled in the system.
Test case	An authorized person enters the office.
Expected result	The system recognizes the person as authorized, and does not generate any alarm.

Table 16: Acceptance test cases for the biometric system

- *DPG_2: Legal requirements*

  A SALTed system shall comply with the current regulations on privacy and data protection in the context for which it was built, so the compliance of the legal requirements shall also be evaluated. This task should be performed by law experts.

- *DPG_3: Socio-ethical requirements*

  A SALTed system shall also take into consideration the socio-ethical issues, thus the awareness of the system about the socio-ethical concerns shall also be evaluated by experts on this field.

- *DPG_4: Privacy and accountability requirements*

  Finally, the measures implemented for privacy and accountability will be evaluated. It is important to verify if the mechanisms for data and privacy protection, and the different policies and procedures defined are sufficient to cover the main privacy and accountability requirements. This evaluation can be performed by inspection, and also through a set of test cases covering the negative scenarios where the threats to privacy appear. The following test cases have been defined according to the risks identified in section 5.5:

MISUSE_CASE_1: Malicious modification of the stored data *(Data Integrity)*	
Preconditions	The biometric system stores biometric templates or images.
Test case	The biometric templates or the images stored temporarily in the system are modified or deleted maliciously (at least an attempt to perform this modification or deletion occurs).
Expected result	The access to the information for its modification is recorded, including the timestamp and the user who accessed to the data. The system implements the adequate measures to prevent or mitigate the corruption of data.
MISUSE_CASE_2: Loss of alarms *(Data Integrity)*	
Preconditions	A malicious user has the means to intercept the alarms generated by the

	RIS and sent to the System Operator.
Test case	An alarm notifying an intrusion is intercepted and deleted.
Expected result	The System Operator does not receive the alarm. The system provides a backup of the alarms generated and not verified, so the System Operator can look at the information later and be aware of the intrusion.
MISUSE _CASE_3: Unauthorized access to stored data (Privacy)	
Preconditions	The biometric system stores images of people. A malicious user has the means to access the images stored in the system.
Test case	A malicious user has access to the images stored in the system.
Expected result	The malicious user cannot identify anybody in the images.

Table 17: Misuse cases defined for the biometric system

This tables enumerates the main evaluation criteria to consider at design process level:

Goal	Evaluation criteria	Aspect to evaluate	Type of evaluation	Instrument
DPG_1	The system provides the surveillance service for which it was built	Usefulness/ Functionality	qualitative	Human inspection: check if the system performs the detection of unauthorized people. Use of acceptance test cases.
DPG_2	The system complies with the laws in the context for which it was built	Legality	qualitative	Human inspection: check if the system complies with the current legislation.
DPG_3	The system shall take into consideration the main socio-ethical concerns	Socio-ethical awareness	qualitative	Human inspection: check if the system addresses the main socio-ethical concerns.
DPG_4	The system shall take into consideration the main accountability concerns	Accountability	qualitative	Human inspection: check if the system addresses the main accountability concerns.
DPG_4	The system shall cover the main privacy requirements	Privacy	qualitative	Human inspection: check if the system addresses the main privacy concerns.

Table 18: Evaluation criteria at design process level

7 References

[1] Liu, S., and Silverman, M.,"A practical guide to biometric security technology," IT Professional, vol. 3, pp. 27-32, 2001.

[2] Magic Draw for UML modelling, No Magic, Inc. More information at the company's URL: http://www.nomagic.com/

[3] Instruction 1/2006 , of 8 November, by the Spanish Data Protection Agency, on processing personal data for surveillance purposes through camera or video-camera systems. Available here: http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Instruccion_videovigilanci_EN.pdf

[4] M.R. Andersen, T. Jensen, P. Lisouski, A.K. Mortensen, M.K. Hansen, T. Gregersen and P. Ahrendt, Department of Engineering – Electrical and Computer Engineering, Aarhus University, "Kinect Depth Sensor Evaluation for Computer Vision Applications". Aarhus University © 2012.

[5] "Guide on Video Surveillance", © AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (SPANISH DATA PROTECTION AGENCY), Official Publications Identification Number: 052-08-007-8, available online here: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia_en.pdf