PrivAcy pReserving Infrastructure for Surveillance

Deliverable D6.3

Biometrics Use Case

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D6.3
Title:	Biometrics Use Case
Version:	v1.0
Date:	17/07/2015
Confidentiality:	Public
Contributors:	Visual Tools (VT) Universidad de Málaga (UMA)

Funded by the European
Union's Seventh
Framework Programme

Table of Contents

Document History

Version	Status	Date
v0.1	First draft of ToC	6/11/2014
v0.2	Contribution to section 2 by VT	5/1/2015
v0.3	Contribution to section 4.1 by VT	15/4/2015
v0.4	Update of section 2 and contribution to section 3 by VT	9/6/2015
v0.5	Contribution to section 3 by UMA; Contribution to sections 4-7 & update of the other sections by VT	1/7/2015
v0.6	UMA revision (integration of comments and corrections)	16/7/2015
v0.7	Thales revision (integration of comments and corrections)	17/7/2015
v1.0	Addition of conclusion (VT). Final version	17/7/2015

<table>
<tr><th colspan="4">Approval</th></tr>
<tr><td></td><td colspan="2"><b>Name</b></td><td><b>Date</b></td></tr>
<tr><td>Prepared</td><td colspan="2">Visual Tools, UMA</td><td>1/7/2015</td></tr>
<tr><td>Reviewed</td><td colspan="2">UMA, Thales</td><td>16/7/2015</td></tr>
<tr><td>Authorised</td><td colspan="2">Trialog</td><td>17/7/2015</td></tr>
<tr><th colspan="4">Circulation</th></tr>
<tr><td colspan="2"><b>Recipient</b></td><td colspan="2"><b>Date of submission</b></td></tr>
<tr><td colspan="2">Project partners</td><td colspan="2"></td></tr>
<tr><td colspan="2">European Commission</td><td colspan="2"></td></tr>
</table>

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
AEPD	Spanish Data Protection Commissioner’s Office
APDB	Authorized People Database (also known as biometric enrolment database)
DC	Data Controller
DCAM	Depth Camera
DPA	Data Protection Authority
DPO	Data Protection Officer
DS	Data Subject
ICT	Information and Communication Technologies
LAN	Local Area Network
LOPD	Spanish Organic Law 15/1999 of Personal Data Protection
PAERIS	PrivAcy-by-design EngineeRIng aSsistant
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PIR	Passive Infrared
RDB	Results Database

RIS	Re-Identification Server
RMS	Results Management Server
SA	System Administrator
SALT	Socio-ethicAl, Legal, Technical
SF	SALT Framework
SFMT	SALT Framework Management Tool
SO	System Operator
SSP	Surveillance Service Provider
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 describes the results of task T6.4 and task T6.5, including the process followed for the design and development of the biometrics use case defined in D6.1 and D6.2 using the SALT Framework resources, and the procedures, mechanisms or measures (artifacts) implemented to address the identified privacy and accountability concerns.

This work serves as an example to show the value of the SALT Framework for the development of biometric systems during all their lifecycle.

1 Introduction

This document is aimed at describing the process followed for the development of the biometrics use case defined in D6.1 and D6.2 using the SALT approach. It is divided in the following sections:

- Section 2*: Biometrics use case overview* summarizes the goals and requirements for the use case, as well as the artifacts selected to address the privacy and accountability concerns. All of them were already explained in D6.2.
- Section 3*: SALT Framework specialized for biometrics* describes the SALT design process defined and the available resources in the SALT Framework that can be applied for the development of biometric systems.
- Sections 4, 5 and 6 describe the use cases defined, that cover all the stages of the lifecycle of the biometric system. We have just finished the implementation of the different modules composing the system, **the system is currently at the end of the development stage**, therefore the first stages are explained in-depth, including details about how the SALT Framework resources have been used to take the different design decisions. On the other hand, the sections explaining the stages of deployment, operation & maintenance and retirement describe the next steps that will be carried out and evaluated during the next months in order to assess the value of the SALT Framework in all the system lifecycle.

It is important to point out that because of resource reasons, the system has not been fully developed: only the most important components and artifacts that allow to prove the value of the SALT Framework for the design and development of this use case have been implemented. Moreover, we have used a first version of the SALT processes and tools developed so far in this project (WP2-WP4), that may be subject to updates or improvements during the next semester.

2 Biometrics use case overview

This section summarizes both the surveillance goals and the privacy and accountability requirements for the use case.

2.1 Scenario description and goals

The use case goal is the **detection of unauthorized accesses to a building with security requirements preserving users' privacy**.

The stakeholder company is Visual Tools, that requires a solution to protect all the material stored in their headquarters, located in Madrid (Spain), during the night period (9:00 PM to 7:00 AM), without interfering with the work of the maintenance employees.

In particular, the system designed should fulfill the following requirements from the stakeholder *(surveillance goals)*:

1. Prevention against theft (deterrence);
2. Facilitation of the work of security operators during the night period, reducing the false alarms;
3. Facilitation of the collection of evidences for law enforcement.

To address the stakeholder needs we have designed a biometric system based on video analysis that is capable of detecting unauthorized accesses in the scenario defined. The system will cover the main transit areas of the office with cameras, providing depth and spatial information that will be analyzed to detect the people accessing to the office. It will also include a mechanism for re-identification allowing to match any person detected with a database of authorized people. In case the system does not recognize the person detected, an alarm will be generated and displayed to the operator responsible for monitoring the facilities.

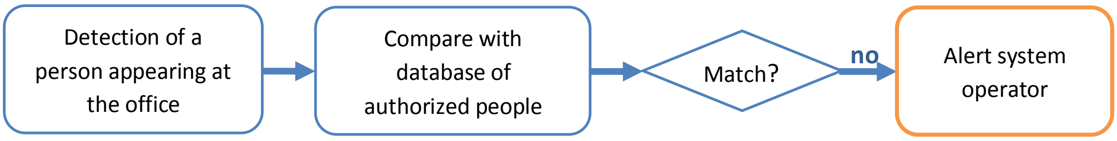

Detection of a person appearing at the office
Compare with database of authorized people
Match?
no
Alert system operator

Figure 1: Summary of the functioning of the proposed system

These are the main features provided by the system that will serve to solve the stakeholder problems:

- **Re-identification capability**, allowing to compare any data subject with a database of authorized people.
- **Management tool** displaying the results of the re-identification process, that can be used by security operators to react earlier in case of intrusion, and also to discard false alarms more easily.
- **Collection of information** of any access detected, such as the date and time, which will facilitate the video search in case of incident, and therefore the provision of evidences to local authorities.

2.2 Privacy & accountability requirements

The following table enumerates the main privacy and accountability requirements identified and detailed in D6.2. The different requirements have been extracted from the following sources:

- *(REQ_QUE_*)*: The SALT questionnaire for biometrics developed in WP2.
- *(REQ_SOC_*)*: The socio-ethical assessment described in D6.2.
- *(REQ_VSS_*)*: The Spanish DPA's guideline for video surveillance systems, based on the Spanish legislation.
- *(REQ_LEG_*)*: Legal requirements extracted from the end-to-end accountability assessment described in D6.2.
- *(REQ_ACC_*)*: Other accountability concerns extracted from the end-to-end accountability assessment described in D6.2, that are not covered by other requirements.

ID	**Requirement**
REQ_QUE_1	Define clearly the purpose of the processing of personal data
REQ_QUE_2	Indicate and justify the legal ground on which the biometric system relies
REQ_QUE_3	Justify the necessity and suitability
REQ_QUE_4	Evaluate the interference with privacy rights
REQ_QUE_5	Transparency of the enrolment process
REQ_QUE_6	Transparency of the matching process
REQ_QUE_7	Privacy impact of the technology selected
REQ_QUE_8	Nature of the data collected
REQ_QUE_9	Expected system accuracy
REQ_QUE_10	Limitation of the access to personal data
REQ_QUE_11	Disclosure of personal data
REQ_QUE_12	Storage of personal data
REQ_QUE_13	Security of the data stored
REQ_QUE_14	Retention and deletion of personal data
REQ_QUE_15	Protection of personal data communications
REQ_QUE_16	Privacy impact of system failures
REQ_QUE_17	Control of unattended operations
REQ_QUE_18	Stability of biometric templates
REQ_QUE_19	Anti-spoofing measures
REQ_SOC_1	Didactic explanation of the objectives and functioning of the surveillance system during the enrolment phase.
REQ_SOC_2	Mitigate the social impact of any change in the group of people enrolled.
REQ_SOC_3	Mitigate the social impact of the dependence of the system performance on the clothes of the people enrolled in the system.
REQ_SOC_4	Reduce the intrusive impact of the system on employees due to the use of a silent technology.
REQ_SOC_5	Mitigate the impact on the social behavior of employees of the installation of a surveillance system.

REQ_VSS_1	Use of informative signs
REQ_VSS_2	Use of an informative handout
REQ_VSS_3	Inscription of the system in the General Register
REQ_VSS_4	Location of the cameras
REQ_VSS_5	Retention period for the images stored
REQ_VSS_6	Security level of the images stored
REQ_VSS_7	Security obligations of people allowed to access the data
REQ_ACC_1	Documentation and communication of policies, procedures and practices
REQ_LEG_1	Carry out a Privacy Impact Assessment (e.g. through the SALT questionnaire for biometrics)
REQ_LEG_2	Consultation of stakeholders
REQ_LEG_8	Data subject rights (access, rectification, deletion)

Table 1: Summary of privacy and accountability requirements identified for the use case

It is important to highlight the evolution of the privacy and accountability requirements from the initial list identified at the beginning of the project in D6.1, to the list of requirements of Table 1 obtained from the different evaluations carried out following the SALT approach. As can be seen comparing Table 1 and Table 2, the new list of requirements is much more elaborated and cover more aspects than the requirements listed in deliverable D6.1.

Id	Initial Privacy and security requirements	Covered by
PSR_1	The images stored in the system shall be protected	REQ_QUE_13
PSR_2	The bodyprints stored in the system shall be protected	REQ_QUE_13
PSR_3	The alarms generated shall be periodically sent until they are verified by the System Operator	OR_3, OR_16
PSR_4	A history of the alarms generated shall be stored in the system	REQ_QUE_9, REQ_QUE_18-19
PSR_5	The System Administrator is the only user with permissions to add, modify or delete the data stored in the system	REQ_QUE_10, REQ_QUE_13
PSR_6	The System Administrator is the responsible for providing authorization to access the data stored	REQ_QUE_10, REQ_QUE_13
PSR_7	The system shall record any access to the information stored in the system	REQ_QUE_10, REQ_QUE_17 REQ_QUE_19,
PSR_8	The communication between the VPUs and the RIS shall be adequately protected	REQ_QUE_13
PSR_9	The system should implement adequate security measures to prevent or mitigate a denial of service attack	REQ_QUE_13
PSR_10	The different components should be connected through a LAN network	REQ_QUE_13, REQ_QUE_15
PSR_11	The system shall comply with the Spanish regulations on privacy and data protection	REQ_LEG_*

Table 2: List of initial privacy and accountability requirements

2.3 Other requirements

In the following table, the technical requirements identified in D6.1 are listed with the stage of the lifecycle in which they can be checked. Note that some of the requirements have been updated after the different revisions of the use case. The updates are also indicated in the table.

Id	Technical requirement	Stage
TR_1	The cameras used shall cover the main transit areas of the office	Deployment
TR_2	There shall be one VPU per DC	Design/Development
TR_3	The system shall be centralized	Design/Development
TR_4	Each VPU shall include data storage for the temporary files	Design/Development
TR_5	The RIS shall be connected to the APDB	Design/Development
TR_6	The RIS shall include data storage for the results of the comparison and the alarms *** Updated: The comparison tasks have been separated from the alarm management. Now, the results are stored in the RDB, and displayed through the RMS. We could add this new requirements now:* TR_6: The RIS shall include data storage for the results of the comparison TR_14: The RMS shall include data storage for the alarms TR_15: The RMS shall be connected to the RDB	Design/Development
TR_7	The access to the APDB shall be able to store templates from at least 10 people	Design/Development
TR_8	The access to the APDB shall be traced	Design/Development
TR_9	The communication between the VPUs and the RIS shall be properly protected *** As there is a new component now (RMS), this requirement should be re-written:* TR_9: The communication between the system components shall be properly protected	Design/Development
TR_10	The user interfaces in the RIS shall implement access control mechanisms *** This should be applied to any user interface:* TR_10: The different user interfaces shall implement access control mechanisms	Design/Development
TR_11	Authorization shall be required to access the images stored in the system	Design/Development
TR_12	The VPUs shall use Linux or MAC OS	Design/Development
TR_13	The RIS shall use Linux or MAC OS	Design/Development
Id	**Operational requirement**	**Stage**
OR_1	The system shall be able to initiate the recognition process automatically	Design/Development
OR_2	The system shall be able to perform the categorization process automatically	Design/Development
OR_3	The system shall be able to generate alarms automatically when an unauthorized person is detected	Design/Development
OR_4	The VPU and the RIS shall be able to communicate without any user interaction *** As there is a new component now (RMS), this requirement should be re-written:* OR_4: The VPU, the RIS and the RMS shall be able to communicate without any user interaction	Design/Development
OR_5	Information about how to configure the system shall be provided to the System Administrator	Deployment
OR_6	Information about how to access certain information shall be provided to the users with authorization to retrieve it	Deployment
OR_7	The System Administrator shall be educated on how the biometric system works	Deployment
OR_8	The System Administrator shall be able to manage other system users	Design/Development
OR_9	The System Administrator shall be able to authorize the access to the information stored in the system	Operation
OR_10	The System Administrator shall be able to configure the recognition	Design/Development

	parameters	
OR_11	The System Administrator shall be able to define the detection period	Design/Development
OR_12	The System Administrator shall be able to initiate the enrolment process manually	Design/Development
OR_13	The System Administrator shall be able to access the information stored in the system	Design/Development
OR_14	The System Administrator shall be able to delete the information of the people detected	Design/Development
OR_15	The System Administrator shall assist the Police Officers and the Data Protection Officers for auditing tasks	Operation
OR_16	The System Operator shall be able to receive notifications of the system in case of alarm	Design/Development
OR_17	The System Operator shall be able to access the information of the people detected	Design/Development
OR_18	The System Operator shall be able to discard false alarms	Design/Development
OR_19	The System Operator shall be able to report incidents to local authorities	Operation
OR_20	The System Operator shall collaborate with the local authorities in the verification of an intrusion	Operation
OR_21	The Police Officer shall be able to obtain information related to a particular incident	Operation
OR_22	The Data Protection Officer shall be able to obtain information stored in the system	Operation
OR_23	The system should be available at least during the period defined for detection	Design/Development
OR_24	A reasonable error rate for the system is 20% of false recognitions	Operation
Id	**Functional requirement**	**Stage**
FR_1	The system shall be able to capture spatial and RGB information	Design/Development
FR_2	The system shall be able to detect people appearing in the scene	Design/Development
FR_3	The system shall be able to track the people detected	Design/Development
FR_4	The system shall be able extract features of the people detected	Design/Development
FR_5	The system shall be able to create a template for each person detected	Design/Development
FR_6	The system shall allow to discard low quality templates	Design/Development
FR_7	The system shall be able to store information of the people detected	Design/Development
FR_8	The system shall be able to compare and match the templates of the people detected	Design/Development
FR_9	The system shall be able to decide if a person detected belongs to a defined group	Design/Development
FR_10	The system shall be able to generate alarms	Design/Development
FR_11	The system shall be able to send alarms to certain users	Design/Development
FR_12	The system shall be able to store information of certain users	Design/Development
FR_13	The system shall allow to discard false alarms	Design/Development
FR_14	The system shall allow to access the information of the people detected	Design/Development
FR_15	The system shall allow to delete the information of the people detected	Design/Development
FR_16	The system shall allow to configure the recognition parameters	Design/Development
FR_17	The system shall allow to define the detection period	Design/Development
FR_18	The system shall allow to initiate manually the enrolment process	Design/Development
FR_19	The system shall be able to record the accesses to the information of the people detected	Design/Development
FR_20	The system shall be able to delete automatically certain information stored after a defined period of time	Design/Development
Id	**Environment requirement**	**Stage**
ER_1	The system shall operate indoors	Development / Deployment
ER_2	The system shall be able to operate correctly at temperatures ranging from 17°C - 27°C	Development / Deployment
ER_3	The system shall be able to operate correctly in normal humidity conditions	Development /

		Deployment
ER_4	The system shall be able to operate correctly with ambient lightning	Development / Deployment
ER_5	Each depth camera shall cover a maximum area of 5 x 3 meters	Deployment
ER_6	Each depth camera shall be placed at a minimum of 0.8 meters of the objects	Deployment

Table 3: List of technical requirements for the biometrics use case

2.4 Artifacts

As explained in D6.2, these are the artifacts selected to address the most important privacy and accountability concerns identified for this use case:

ID	Artifacts
A1	SALT Framework questionnaire for biometrics (PIA)
A2	Public privacy policy
A3	Inscription of the system in the General Register
A4	Use of informative signs
A5	Definition of a procedure for enrolment in which the collaboration of the data subject is required
A6	Role-Based Access Control
A7	Training sessions for the different system users
A8	Data collection logs
A9	Data access logs
A10	System logs
A11	System documentation
A12	Data encryption
A13	Connection of devices through a Local Area Network (LAN)
A14	Alarm management separated from the matching process
A15	Performance monitoring
A16	System monitoring
A17	Periodic revision of policies and procedures
A18	Creation of a record containing the results of the recognition process
A19	Procedure to let data subjects access their personal information
A20	Access control mechanism for the Web Services
A21	Access control mechanisms for the User Interfaces
A22	Periodic revision of the need for the system
A23	Document signed by the installer
A24	Action plan in case of unauthorized access
A25	Didactic sessions for data subjects
A26	Provision of "surveillance breaks"

Table 4: List of artifacts to be implemented

Because of resource reasons, the system will not be fully developed, and only the most important components and artifacts that allow to prove the value of the SALT Framework for the design and development of this use case will be implemented, while the rest will be just explained in the system documentation.

3 SALT Framework specialized for biometrics

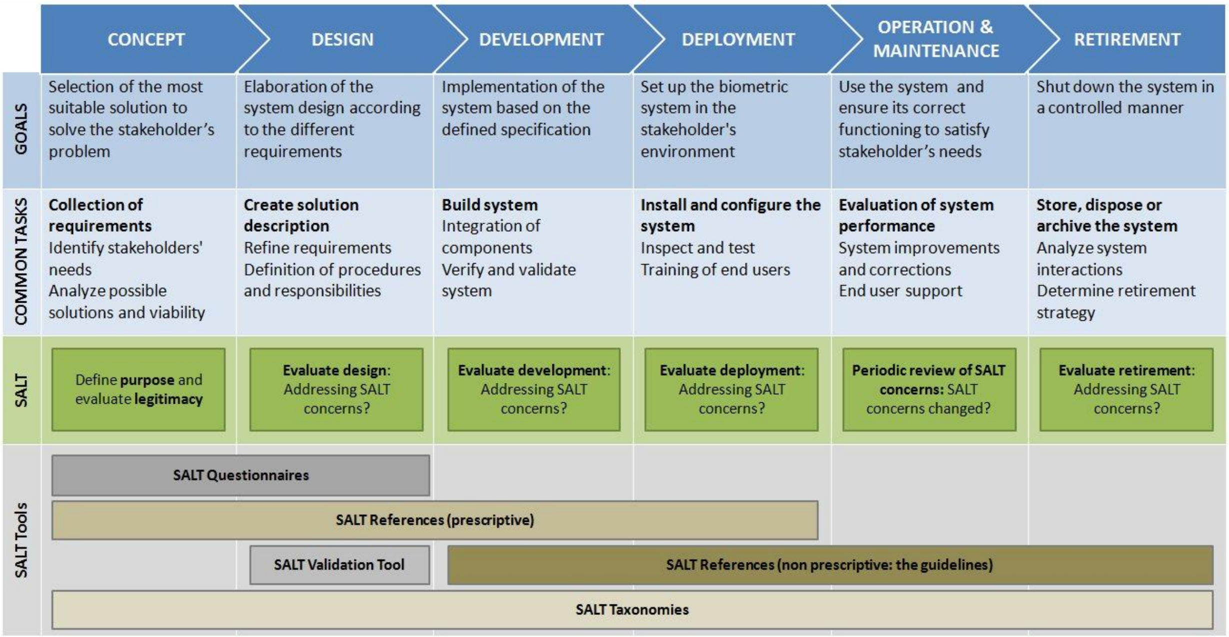
The SALT Framework provides guidelines and tools for both biometric and video surveillance systems, and there is no need to use a specific framework depending on the type of system. That said, it is important to point out that not all the contents stored in the repository can be applied for all type of surveillance systems. This is mainly because biometric systems are considered more intrusive due to the nature of the data collected, and they are normally regulated by specific legislation or recommendations, requiring a more exhaustive assessment of the procedures and measures implemented for privacy and data protection.

Below, the design process defined and the SALT Framework Tools that can be used for biometric systems are explained, indicating in each case the particularities of the SALT resource for the biometric use case presented in WP6.

3.1 Design process using the SALT Framework

After several iterations through the diagram describing the lifecycle of SALT compliant systems, we realized that the design process strongly depends on the system development lifecycle used by the company producing the system. **There is no separation into a design process for biometrics and a design process for video surveillance**, the most critical element in the definition of a design process for a surveillance system is the model followed by the developer company (SSP) for the elaboration of their products (e.g. Waterfall, Spiral, V-model, Agile models, etc.).

As the SALT design process to be defined is not intended to change or re-design the development models or lifecycles used by a company, we have decided to elaborate a new type of diagram that provides a higher level of abstraction to describe the lifecycle of a system that follows the SALT paradigm. This new diagram is presented in Figure 2, and shows the different stages of any system lifecycle including their goals, examples of tasks that are carried out in each stage, that also depend on the way of working of each company, the additional tasks that have to be performed to ensure that at the end of the process the system obtained addresses the main privacy and accountability concerns *(SALT)*, and the SALT resources available in each case *(SALT Tools)*.



	CONCEPT	DESIGN	DEVELOPMENT	DEPLOYMENT	OPERATION & MAINTENANCE	RETIREMENT
GOALS	Selection of the most suitable solution to solve the stakeholder's problem	Elaboration of the system design according to the different requirements	Implementation of the system based on the defined specification	Set up the biometric system in the stakeholder's environment	Use the system and ensure its correct functioning to satisfy stakeholder's needs	Shut down the system in a controlled manner
COMMON TASKS	**Collection of requirements** Identify stakeholders' needs Analyze possible solutions and viability	**Create solution description** Refine requirements Definition of procedures and responsibilities	**Build system** Integration of components Verify and validate system	**Install and configure the system** Inspect and test Training of end users	**Evaluation of system performance** System improvements and corrections End user support	**Store, dispose or archive the system** Analyze system interactions Determine retirement strategy
SALT	Define **purpose** and evaluate **legitimacy**	**Evaluate design**: Addressing SALT concerns?	**Evaluate development**: Addressing SALT concerns?	**Evaluate deployment**: Addressing SALT concerns?	**Periodic review of SALT concerns**: SALT concerns changed?	**Evaluate retirement**: Addressing SALT concerns?
SALT Tools	**SALT Questionnaires**					
	SALT References (prescriptive)					
		SALT Validation Tool	**SALT References (non prescriptive: the guidelines)**			
	SALT Taxonomies					

Figure 2: Lifecycle of SALT compliant systems

This new diagram shows six well differentiated stages covering the entire life cycle of the system, that can be identified somehow in any system lifecycle:

- **Concept stage**, in which the stakeholder's problems are analyzed in order to select the most suitable solution. The specific context in which the system will be deployed, the different requirements and constraints from the organizations involved in the development of the system and the potential users are taken into consideration in this initial stage.

  In order to integrate privacy and accountability in this stage, it is essential to define clearly the purpose of the system and evaluate its proportionality and legitimacy. This assessment should be performed by a person with certain legal expertise, but it is also important to involve a technical expert in this stage to analyze the viability of the possible solutions from a technical point of view. It is not necessary to decide yet all the components and mechanisms that will be implemented, but it is important to have at least an idea about how the system can be configured and the type of data that will be collected and processed, as the collection and processing of data has to comply with the existing legislation.

  The SALT Framework provides questionnaires to guide the Privacy Impact Assessment and facilitate the evaluation of the need and proportionality of the system. Besides, the SALT Repository may include several references providing guidance for this stage of the process, and also information of the data protection risks associated to different technologies.

- **Design**: once the system purpose has been evaluated, it is time to specify the strategy to follow to produce the system that will fulfill that purpose. In this stage, the list of system requirements, that have been completed with a set of concerns extracted from the PIA, are examined more deeply. Other tasks performed at this stage are the definition of the system architecture and the selection of the most appropriate system components and technologies. As a result of this phase, a detailed design specification for the system is obtained.

The system design has to be evaluated in order to check if it addresses the main privacy and accountability concerns before the development phase, and in case the system design does not fulfill a requirement it should be reviewed and changed (if possible). In this evaluation at least a person with technical profile is required, but it would also be good to involve other type of experts from different fields (socio-ethics, legal, etc.) to ensure that the system design takes into account concerns of a different nature.

Apart from the questionnaires and the SALT references, the SALT Framework provides another tool for the validation of system designs that highlights the main privacy and accountability concerns filled (and not filled) by a given design.

- **Development**: implementation of the system based on the design specification elaborated in the previous phase.

  This stage is basically technical, and which is more important here in terms of privacy and accountability is to check at the end of the stage the different system components behave as expected, particularly the operations related to the collection and processing of data.

  The SALT Framework can also provide guidance for this stage in the form of SALT References.

- **Deployment**: the goal of this stage is to set up the biometric system in the stakeholder's environment. This work includes the installation of the system in the target location, its configuration and other supporting actions such as user training. At the end of this phase, the system is fully operational according to the defined requirements.

  The references stored in the SALT Repository can also provide some guidelines for this stage, such as legal requirements that have to be fulfilled before using the system for surveillance (e.g. how to install and position the cameras).

  In this stage, at least the stakeholder (DC), the installer and the surveillance service provider (SSP) are involved. It is not only important to set up correctly the system in the deployment stage, but also to prepare the documentation required (e.g. system manuals, privacy policies...), and define the responsibilities and procedures related to the processing of the data stored in the system.

- **Operation & maintenance**: the system is monitored in terms of performance and availability to ensure that it works as expected and that it does not become obsolete. Different types of maintenance shall be required to keep the system under appropriate conditions (preventive maintenance) or to detect and repair a system flaw (corrective maintenance).

The System Operator (SO) and the System Administrator (SA) are normally in charge of the operation & maintenance tasks.

There can also be SALT references in the SALT repository providing guidelines for this stage, for example, recommending certain procedures or technical mechanisms to facilitate the maintenance of the system taking into account privacy and accountability.

> **Operation & maintenance stage of a biometric system**
>
> Although this diagram just provides several examples of tasks that can be performed at the different stages, it is important to mention that the stages of the lifecycle are quite similar both for video surveillance and biometric systems, except for this stage.
>
> Biometric systems have two modes of operation: **enrolment** and **matching,** and this may require to set up additional mechanisms and procedures for maintaining the integrity and accuracy of the biometric information stored in the system.

- **Retirement**: this is the end of the biometric system life cycle. The system is disposed normally due to business decisions (e.g. replacement of legacy systems) or changes of the stakeholder needs (e.g. the system is no longer required), and its retirement has to be carried out in a controlled manner according to laws and regulations. In the case of biometrics, as for any identity management system, it is important to ensure that all identity information is completely deleted, or otherwise rendered useless when the system is no longer operational.

  A person with technical background should be in charge of the retirement of the system, but it would be also good to include somebody with legal background to verify that the procedure complies with the current legislation.

  Again, the SALT references can provide guidance to facilitate the retirement of the system taking into account privacy and accountability.

We haven't considered *Testing* as a stage itself, as several tests can be conducted during the lifecycle of a system for the evaluation of its performance (e.g. technology testing, scenario testing or operational testing). In this diagram the testing operations are included as tasks carried out in specific stages.

Taking into account the stages described, we have defined the lifecycle model used normally by Visual Tools for its systems and products, where iteration and recursion is possible on the main paths:

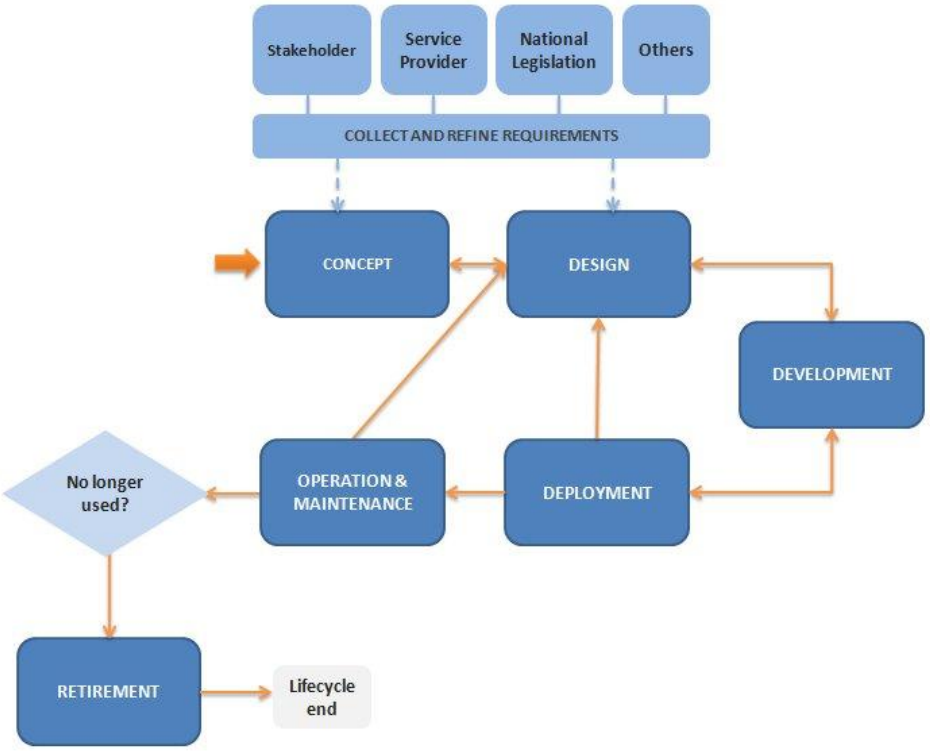


Figure 3: Common lifecycle of Visual Tools' systems

As Visual Tools is the *Surveillance Service Provider* (SSP) in this case, this development lifecycle (Figure 3) is the one used to implement the biometric system required for the detection of unauthorized accesses in the Visual Tools' premises.

Applying the SALT approach, the lifecycle read as follows:

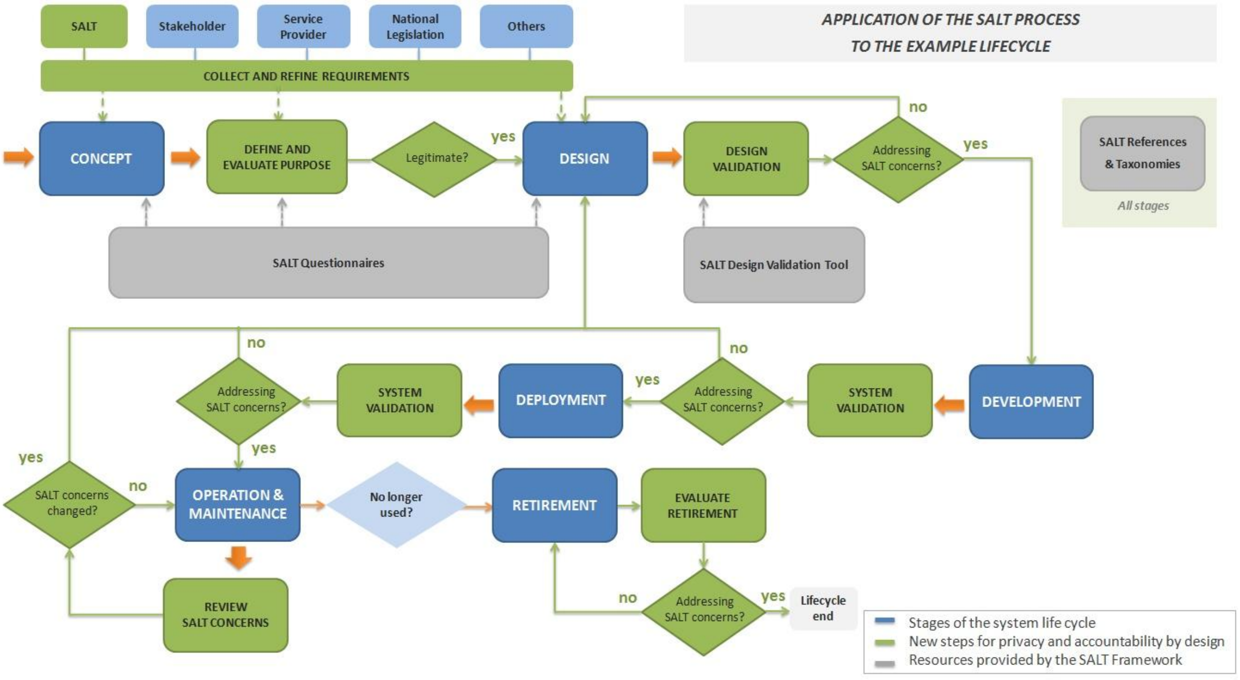

SALT
Stakeholder
Service Provider
National Legislation
Others
APPLICATION OF THE SALT PROCESS TO THE EXAMPLE LIFECYCLE
COLLECT AND REFINE REQUIREMENTS
CONCEPT
DEFINE AND EVALUATE PURPOSE
Legitimate?
yes
DESIGN
DESIGN VALIDATION
Addressing SALT concerns?
no
yes
SALT References & Taxonomies
All stages
SALT Questionnaires
SALT Design Validation Tool
no
no
Addressing SALT concerns?
SYSTEM VALIDATION
DEPLOYMENT
yes
Addressing SALT concerns?
SYSTEM VALIDATION
DEVELOPMENT
yes
yes
SALT concerns changed?
no
OPERATION & MAINTENANCE
No longer used?
RETIREMENT
EVALUATE RETIREMENT
REVIEW SALT CONCERNS
no
Addressing SALT concerns?
yes
Lifecycle end
Stages of the system life cycle
New steps for privacy and accountability by design
Resources provided by the SALT Framework

Figure 4: Lifecycle of Visual Tools' systems applying the SALT methodology

As shown in the previous figures, the SALT approach add specific requirements to take into account privacy and accountability in the different stages of the development process. Furthermore, it requires to carry out different evaluations and revisions at the end of the stages to ensure that the system addresses the SALT concerns during all its lifecycle.

3.2 SALT Framework Tools

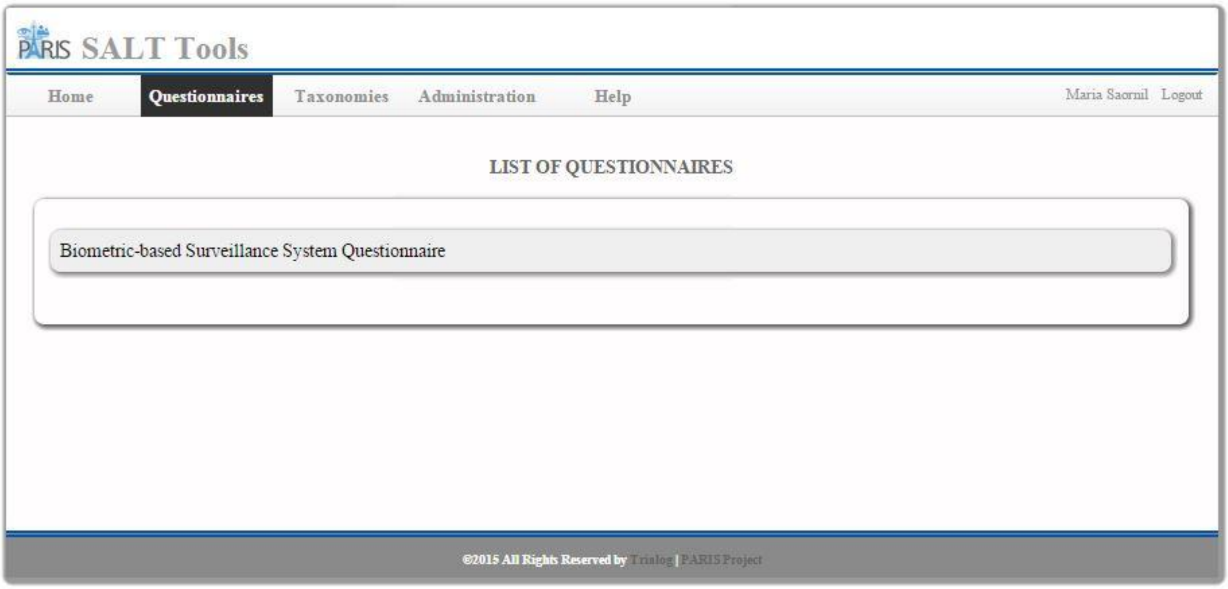
In this section, the SALT Framework Tools that can be used for the development of biometric systems are explained.

3.2.1 Questionnaire for biometrics

As explained in D6.2, under WP2 several questionnaires have been developed to provide guidance at the first stages of a system, where the concept is evaluated and the system is designed. Most of the questions are addressed to users with legal background, but there are also sets of questions for which certain technical expertise is required. Thus, we think that is necessary to involve legal and technical people for answering the questionnaires (e.g. *System Proposer* & *System Designer*), and also several iterations through the questions may be required.

In the particular case of biometric systems, the different groups of questions that can be used for their evaluation are presented in the form of one specific questionnaire that allows to identify the most important concerns on privacy and accountability at an early enough stage to make the right design choices. This questionnaire can be found in the SALT Repository under the section "Questionnaires".

The version of the questionnaire used for the assessment of this use case was included in deliverable D6.2 in the section *Appendix A: SALT questionnaire for biometrics*.

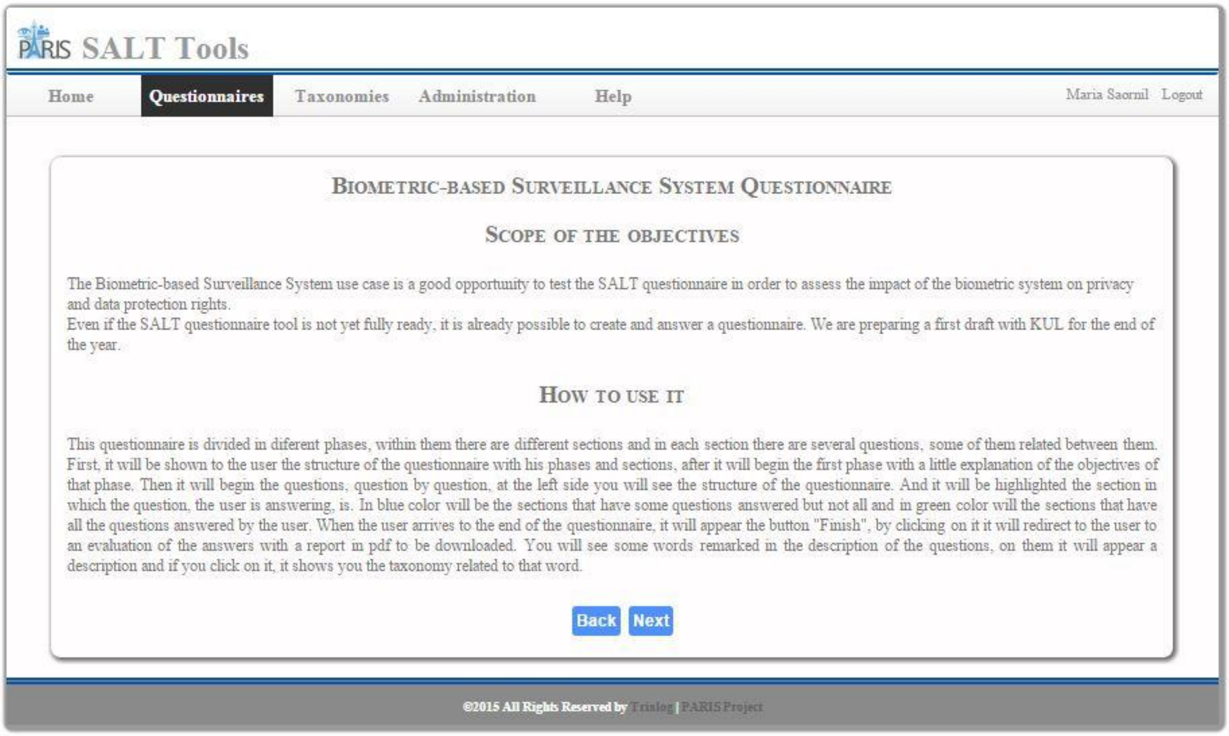


LIST OF QUESTIONNAIRES

Biometric-based Surveillance System Questionnaire

©2015 All Rights Reserved by Trialog | PARIS Project

Figure 5: Biometric-based Surveillance System Questionnaire (I)



BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

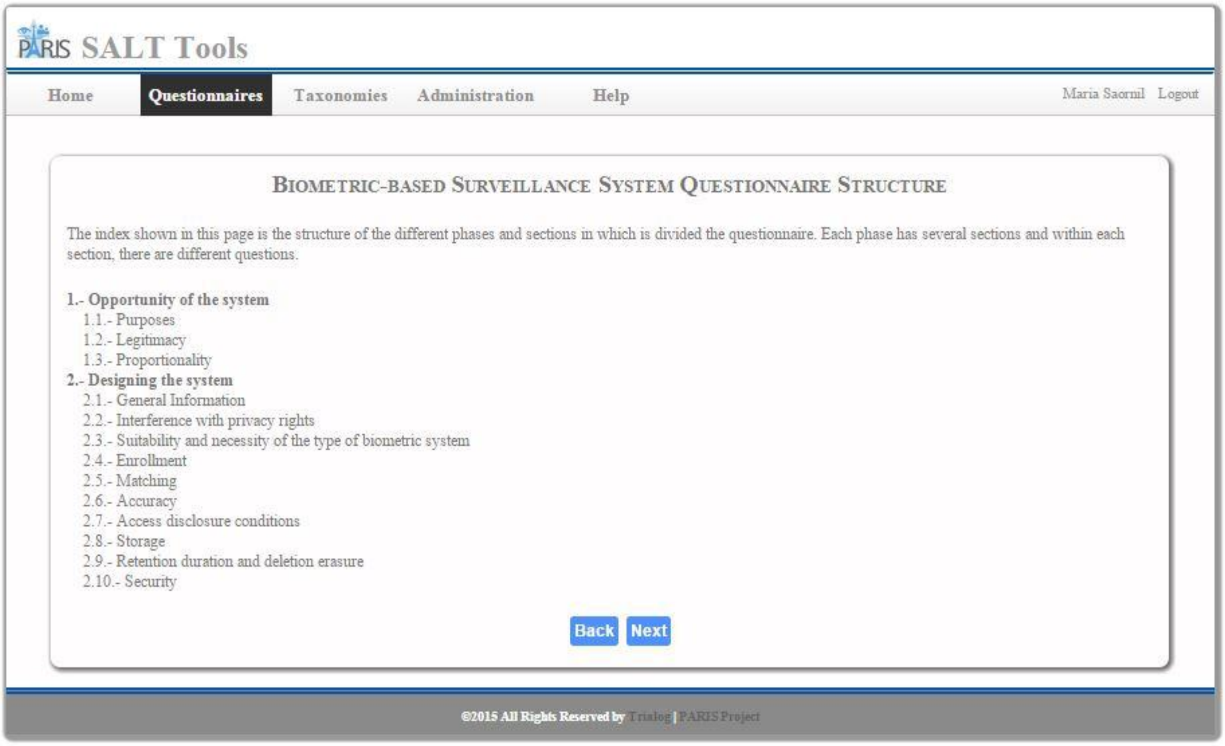
SCOPE OF THE OBJECTIVES

The Biometric-based Surveillance System use case is a good opportunity to test the SALT questionnaire in order to assess the impact of the biometric system on privacy and data protection rights.
Even if the SALT questionnaire tool is not yet fully ready, it is already possible to create and answer a questionnaire. We are preparing a first draft with KUL for the end of the year.

HOW TO USE IT

This questionnaire is divided in diferent phases, within them there are different sections and in each section there are several questions, some of them related between them. First, it will be shown to the user the structure of the questionnaire with his phases and sections, after it will begin the first phase with a little explanation of the objectives of that phase. Then it will begin the questions, question by question, at the left side you will see the structure of the questionnaire. And it will be highlighted the section in which the question, the user is answering, is. In blue color will be the sections that have some questions answered but not all and in green color will the sections that have all the questions answered by the user. When the user arrives to the end of the questionnaire, it will appear the button "Finish", by clicking on it it will redirect to the user to an evaluation of the answers with a report in pdf to be downloaded. You will see some words remarked in the description of the questions, on them it will appear a description and if you click on it, it shows you the taxonomy related to that word.

Figure 6: Biometric-based Surveillance System Questionnaire (II)



BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE STRUCTURE

The index shown in this page is the structure of the different phases and sections in which is divided the questionnaire. Each phase has several sections and within each section, there are different questions.

1.- Opportunity of the system
1.1.- Purposes
1.2.- Legitimacy
1.3.- Proportionality
2.- Designing the system
2.1.- General Information
2.2.- Interference with privacy rights
2.3.- Suitability and necessity of the type of biometric system
2.4.- Enrollment
2.5.- Matching
2.6.- Accuracy
2.7.- Access disclosure conditions
2.8.- Storage
2.9.- Retention duration and deletion erasure
2.10.- Security

Figure 7: Biometric-based Surveillance System Questionnaire (III)

Once the questionnaire is completed, the SALT Framework will provide a report including the responses provided, and thus an evidence of the reasoning followed to assess the concept of the system and the implementation selected. This report generation functionality is still under development, and will be finished during the last semester of the project.

3.2.2 References & Taxonomies

The knowledge in the SALT Repository is stored in the form of SALT references, as explained in D6.2. Each of these references contains information regarding one or several privacy and/or accountability concerns. It is important to remark that since SALT references are created by experts, their content fully depends on them.

On the other hand, it is possible to create taxonomies in the SALT Repository that help the SALT Framework users to understand the concepts included in the SALT references.

Both resources are explained in the following sub-sections.

3.2.2.1 Reference template

This is the template used for the creation of references in the SALT Repository, that is aligned with the work in other work packages of this project (WP2 to WP5):

Field	Type	Description
Reference name	Mandatory	Name that serves to identify the reference, that should be as descriptive as possible. In case the references correspond to a law, an article, a report or any other official document, the name should be the title of that document. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: *Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*
Original language	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum)* In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields).
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
System type	Mandatory	The system type to which the reference applies. *Possible values: Video surveillance systems / Biometric systems / All systems*
Geographical	Mandatory	A first layer of context information, which will define the territorial scope of

Scope		application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). There is also the option "Any" for the cases where this information is not relevant for the reference (e.g. technical information).
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (*e.g. specific cases/conditions where the reference is applicable).*
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)*
Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)*
List of concerns *(privacy and accountability related concerns for surveillance systems)*		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: Duty to inform - Deber de informar
Additional information	Optional	Extra information that helps readers find the concern in the source text.
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
Category	Mandatory	Category of the concern, that can be one or several among this options: *Legal, Socio-Ethical, Technical.*
SALT Topics	Optional	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks. The list of defined SALT legal topics, and its mapping with the privacy principles

		indicated in ISO Standard 29100, is available in Table 6
Stage	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder’s problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder’s needs; • **retirement**: shut down the system in a controlled manner.
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern.
Guidelines	Optional	Any guidance on how to include the concern in the stage of the system lifecycle in which the concern applies. This could be a concrete artifact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration.
OCL Rules	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design. OCL rules are only available for the design stage (in parallel with the UML profile).

Table 5: Template for the SALT References

SALT legal topic	ISO principle
Definitions	Terms and definitions, Actors and roles, recognizing PII
Fairness	n/a
Legal basis	Consent and choice; purpose legitimacy and specification
Purpose specification	Purpose legitimacy and specification
Data minimization	Collection limitation
Data Quality	Accuracy and quality
Data retention	Use, retention and disclosure limitation
Proportionality	n/a
Further use limitation	Data minimization; use, retention and disclosure limitation
Authorised disclosure	Data minimization
Sensitive data	
Data Subjects’ rights	Individual participation and access

Data security	Information security ; privacy compliance
Accountability	Accountability
Transparency	Consent and choice; purpose legitimacy and specification; openness, transparency and notice
Data protection risks	Privacy compliance

Table 6: Mapping of ISO principles and SALT legal topics

3.2.2.2 Reference list for WP6 use case

These are the main SALT References that have been used for the development of the biometric use case presented in WP6:

Id	Reference	Type(s)
WP6_REF_1	European Data Protection Directive 95/46/EC [1]: the Directive forms the legal framework for the processing of personal data, that has been transposed in all EU Member States.	Legal
WP6_REF_2	The General Data Protection Regulation [2]: on the 25th January 2012, the European Commission proposed a new legislative text that would repeal the 95/46/EC Directive.	Legal
WP6_REF_3	Spanish Organic Law 15/1999 on the Protection of Personal Data [5]: Legislative act transposing the 95/46/EC Directive.	Legal
WP6_REF_4	The Regulation developing the Data Protection Act 15/1999 of 13th of December [6], approved by Royal Decree 1720/2007 of 21st of December.	Legal
WP6_REF_5	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 [7].	Legal
WP6_REF_6	The "Guide on Video Surveillance" [8] developed by the Spanish Data Protection Agency providing practical criteria and directions for the application of the mentioned Spanish legislation to video surveillance systems.	Legal
WP6_REF_7	"End-to-end Privacy Accountability: Systematic Analysis of the General Data Protection Regulation Draft", elaborated by Inria [9].	Legal, Technical
WP6_REF_8	Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies [10].	Legal, Technical
WP6_REF_9	"Privacy by Design Solutions for Biometric One-to-Many Identification Systems" elaborated by the Information and Privacy Commissioner of Ontario [11].	Technical
WP6_REF_10	Julian Ashbourn, Biometrics Constitution. Guidelines for implementing biometric technology systems, v.1.30. Date Published: July 32, 2013.	Socio-ethical
WP6_REF_11	“Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems” [3].	Socio-ethical
WP6_REF_12	"Seven Types of Privacy" [4].	Socio-ethical

Table 7: SALT References used in the biometrics use case based on bodyprints

These references have been uploaded to the SALT Repository, and they are also described in the document *PARIS_WP6_Use_Case-SALT_References*.

3.2.2.3 Taxonomies

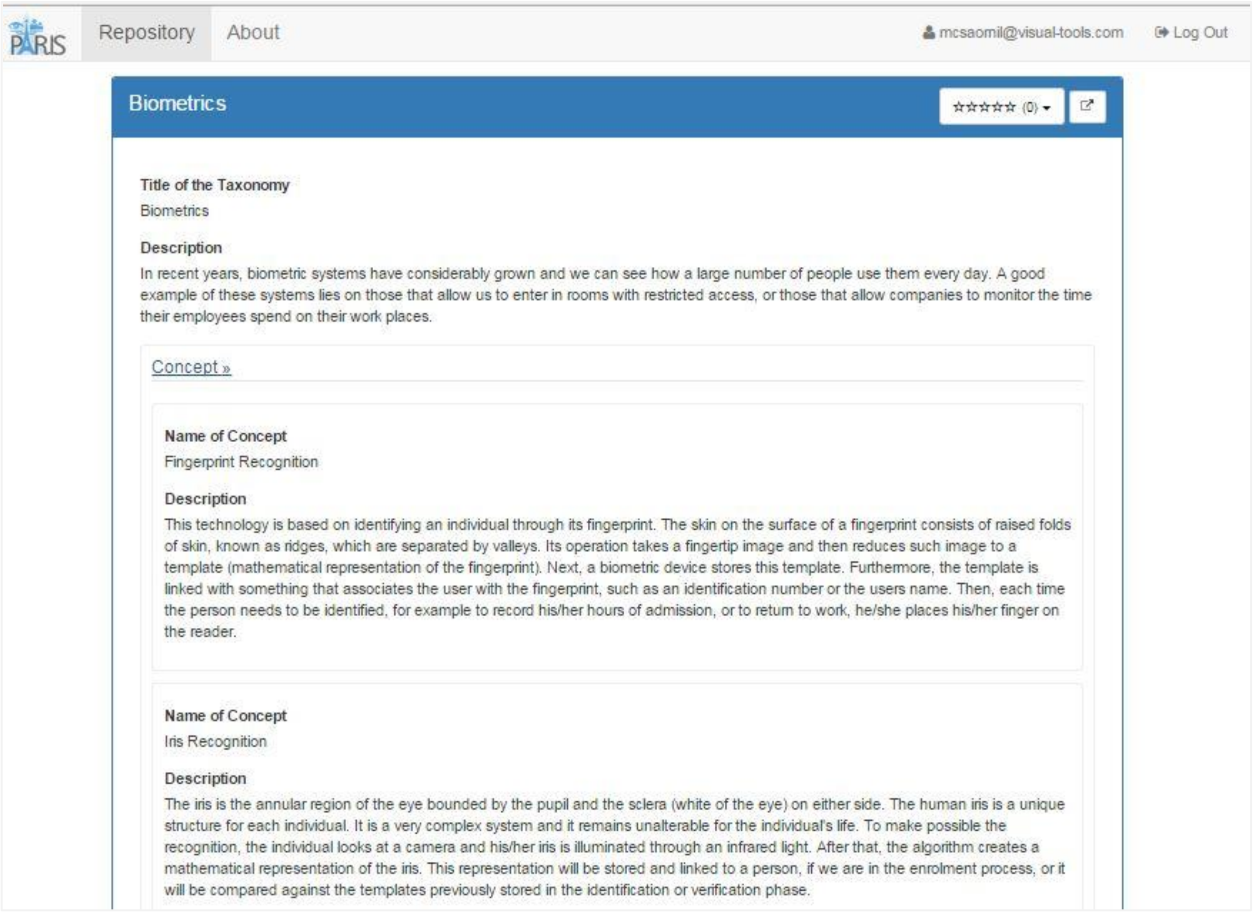
The goal of the taxonomies provided by the SALT Framework is to explain certain concepts related not only to privacy and accountability, but also to surveillance systems, in order to clarify the contents of the SALT References and to help understand when a given reference can be applied. Thus, taxonomies can be considered as sets of dictionaries containing terminology and definitions that are of importance in the development of surveillance systems under the SALT paradigm.

Taxonomies can be used at any moment independently from the stage of the development lifecycle of a system. They can be consulted just to learn about the existing terminology or concepts in a certain domain, or they can be used to understand better the contents of a SALT reference that can be applied to any of the stages of the lifecycle.

For biometric systems, these are the sources of information that have been identified so far for the extraction of taxonomies:

- ISO/IEC 2382:2015 [12], that provides a systematic description of the main concepts related to biometrics in order to clarify the use of terms in this subject field.
- European Data Protection Directive 95/46/EC [1], that is one of the SALT references that can be applied to the WP6 use case, and that contains definitions related to the processing of personal data (e.g. definition of data subject).
- Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies [10], that has also been included as a reference for the WP6 use case, and that contains definitions of terms related to biometrics (e.g. definition of biometric system).
- Deliverable 2.1 of the PARIS project, in which several concepts for biometrics are explained, including the main existing biometric technologies.

The different taxonomies stored in the SALT Repository can be consulted in the section "Taxonomies". As an example, Figure 8 shows the view of the taxonomy created for the last source of information mentioned.



Biometrics

Title of the Taxonomy
Biometrics

Description
In recent years, biometric systems have considerably grown and we can see how a large number of people use them every day. A good example of these systems lies on those that allow us to enter in rooms with restricted access, or those that allow companies to monitor the time their employees spend on their work places.

Concept »

Name of Concept
Fingerprint Recognition

Description
This technology is based on identifying an individual through its fingerprint. The skin on the surface of a fingerprint consists of raised folds of skin, known as ridges, which are separated by valleys. Its operation takes a fingertip image and then reduces such image to a template (mathematical representation of the fingerprint). Next, a biometric device stores this template. Furthermore, the template is linked with something that associates the user with the fingerprint, such as an identification number or the users name. Then, each time the person needs to be identified, for example to record his/her hours of admission, or to return to work, he/she places his/her finger on the reader.

Name of Concept
Iris Recognition

Description
The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The human iris is a unique structure for each individual. It is a very complex system and it remains unalterable for the individual's life. To make possible the recognition, the individual looks at a camera and his/her iris is illuminated through an infrared light. After that, the algorithm creates a mathematical representation of the iris. This representation will be stored and linked to a person, if we are in the enrolment process, or it will be compared against the templates previously stored in the identification or verification phase.

Figure 8: Example of taxonomy for biometric systems

3.2.3 Design validation tool

This section describes the design validation tool, initially called PAERIS (PrivAcy-by-design EngineeRIng aSsistant), from its usage point of view, i. e. how a user can make use of it and what behaviours and outputs are expected. A deeper insight of this tool is beyond the objective of this deliverable, since more detailed descriptions and implementations of the tools belong to Work Package 3, thus this information will be released in the next to come deliverable D3.4 (Guidelines for SALT Framework Management Tool).

The functioning mechanisms of the PAERIS tool are mainly transparent for users, typically system designers, since its use is limited to the design phase of the process. If the SALT methodology proposed by the PARIS project is followed, when creating a design for a given surveillance system, designers will use an UML profile specifically created to help them accomplish privacy and accountability constraints, together with functional requirements. The final output of this phase is an UML model of the system design (we call it a SALT compliant system design because the SALT methodology has been used for it to be obtained).

While using the UML profile, designers will access the SALT repository searching for the appropriate SALT references that may be applicable to the system under development. These references provide a series of concerns to be taken into account, which can be related to socio-ethical, legal or technological areas. Such concerns show a description to designers for them to know what constraints and why have to be fulfilled, but not only that. A set of guidelines describing possible ways to address such concerns is also available. These guidelines refer to UML artefacts and relations to be applied to the system design. It is obvious that there may be many possible implementations for each particular concern, which prevents from storing all of them (hundreds if not thousands). At least, thanks to these guidelines, designers can rely on one provided solution.

And here is when we start talking about the automatic validation. Together with the proposed guidelines, SALT references also offer a list of OCL rules. These rules are a formal way of describing the guidelines, which allows for an automatic validation in case the designer chooses to implement the solution suggested by the guidelines. Of course, if a designer implements another solution of his own, or if a given concern is not taken into account at all, then the automatic validation cannot be performed. Besides, it is also remarkable the fact that some concerns may not have OCL rules, which may happen sometimes due to the generality, ambiguity and wide field of application of some concerns, especially regarding socio-ethical and legal concerns. In such cases, the UML profile will continue aiding in the task of creating the system design, although the automatic validation will not be available (just for the afore mentioned concerns).

However, in general circumstances the SALT repository will provide full SALT references, whose concerns have guidelines and OCL rules. Then, how does the automatic validator help a system designer in these cases? As it has been previously stated, system designers access the SALT repository while using the UML profile. In this step, they retrieve the SALT references relevant to their systems, thus they have access to privacy and accountability concerns and also to guidelines for their implementation. They do not have to care about the OCL rules (in fact, the will commonly not be familiar with OCL language). However, in a background parallel procedure, the automatic validator will retrieve the OCL rules of the selected SALT references and will start to constantly check whether they are fulfilled by the current system design or not, showing an alert message for the last case. The criticality of this alert will depend on the type of concern, showing an error for those who are mandatory or just a warning (or info) for the rest.

We can see this type of validation like and on-the-fly checking, since the automatic validator continuously checks the UML model looking for inconsistencies with the stored OCL rules (in a similar way to nowadays software compilers, which show possible errors at the same time the software programmer is typing the code). In this way, system designers are always aware about those concerns that still need attention. Of course, the user can always deactivate the alert messages for those concerns whose guidelines have not been deliberately followed, avoiding the constant error/warning messages.

But the functionality of the automatic validator does not end here. As it is derived from this description, the behaviour of the validator is driven by the OCL rules. This means that we can enrich such rules in a way that allows for further functionality apart from the design checking. In particular, we can have the added value of a report generation. Yes, at the end of the validation process we can also have some documentation with important information regarding the newly created system design. The type of information will depend on each OCL rule, which in turn depends on the type of concern. Because of this, we can have very specific information regarding a concern and how its solution has been addressed in the UML model, but we can also have information indicating what parts of the system design have to be checked in order to verify a given concern. This comes very handy for those cases where an automatic validation is not possible and the presence of an external (human) auditor is required. The generated report will aid this auditor, telling him where and what to look for checking a given concern compliance.

The inclusion of concerns descriptions inside the report can also be considered, though this issue is still under consideration by the project partners due to the appearance of such information in the SALT references (i. e., the report would have redundant information, but it would avoid looking to SALT references). Figure 9 illustrates the relation of the automatic validator with the rest of elements. We can also appreciate how the automatic validator does not directly interact with the system designer, but it is limited to alerts delivery to the UML profile, which is the element the system designer interacts with.

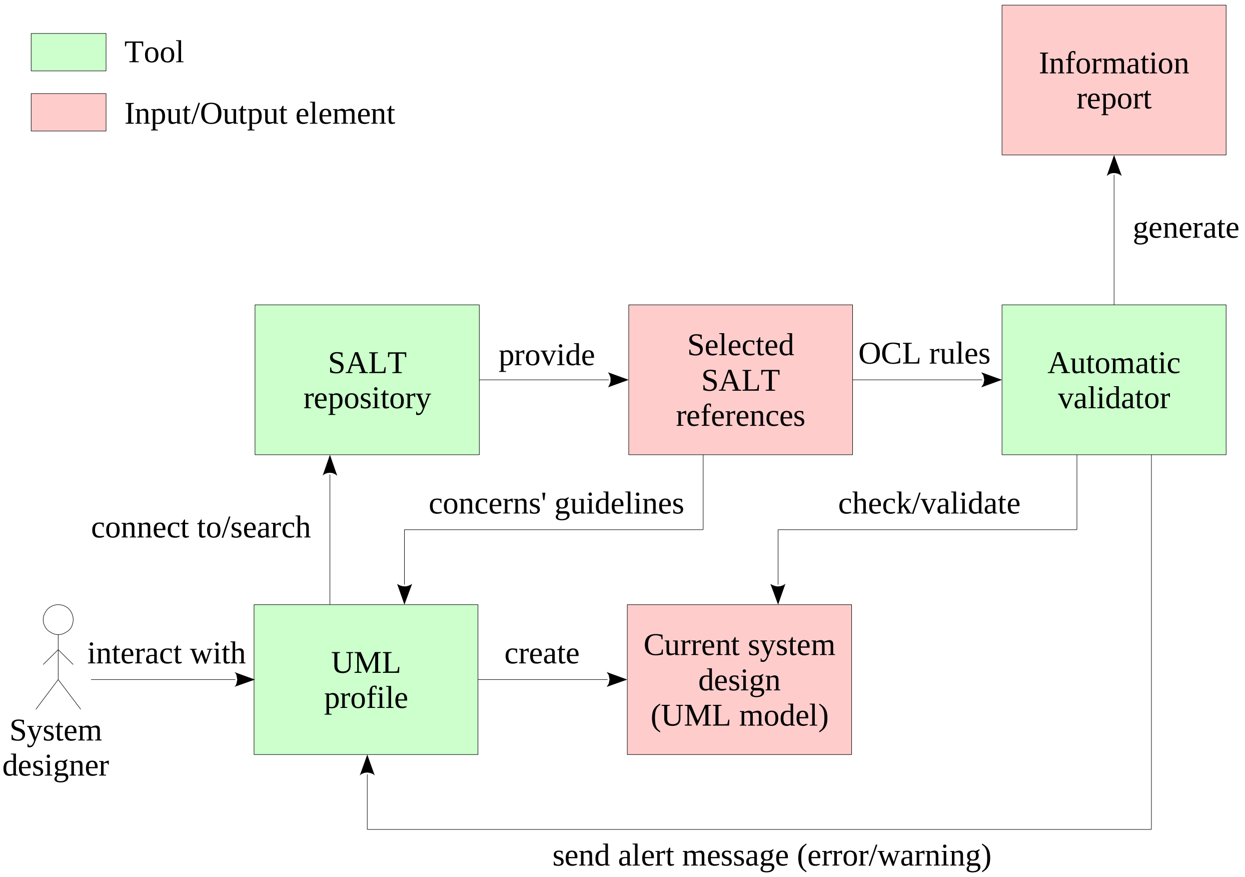


Figure 9: Interactions with the automatic validator

At this stage of the PARIS project, the automatic validator is still under development: OCL rules are locally stored within the UML profile, which allows for the creation of the rules and also testing whether the tool properly checks them or not. The connection between the automatic validator and the SALT repository (thus OCL rules can be retrieved from SALT references) is not yet implemented. This last functionality is planned to be finished in the next reporting period.

4 Use Case I: Designing the system

The goal of this use case is the demonstration of how the SALT Framework can be used to elaborate the design of a biometric system that takes into account privacy and accountability from socio-ethical, legal and technical perspectives.

This use case covers the first stages of the system lifecycle, from the concept phase, where the problems of the stakeholder are analysed and the purpose of the system is defined, until the end of the design stage. As a result of this use case, a system design that addresses the SALT concerns is obtained.

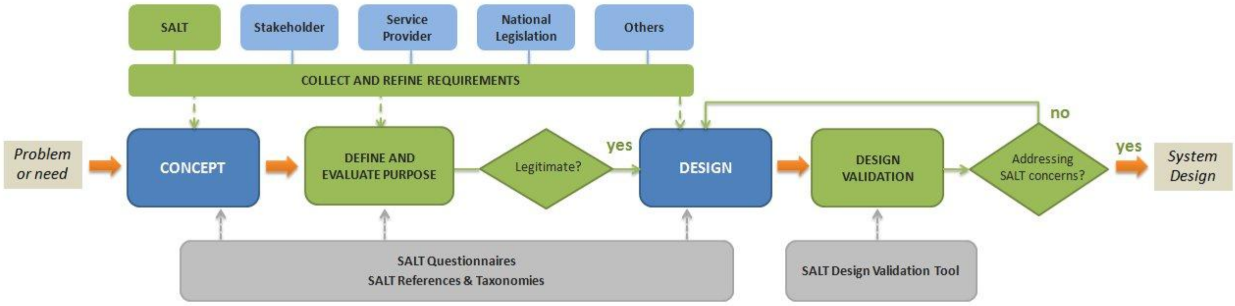


Figure 10: Stages of the system lifecycle covered by Use Case I

The specific process followed to design the biometric system developed in WP6 is described in this section.

4.1 Concept stage

In this first phase, the problems of the stakeholder are analyzed in order to select the most suitable solution. The concept or intention phase covers the *Concept* stage, the initial collection of requirements that impose a set of constraints for the system to be designed, and the evaluation of the proportionality and legitimacy of the proposed solution.

4.1.1 Concept stage

This use case starts with the stakeholder company (Visual Tools) requiring a solution to protect the material stored in the office located in Madrid during the night period. As this company will be the one using the system once deployed, it has the role of the *Data Controller*.

To deal with this problem, the stakeholder entrusts the task of finding a solution that meets their needs to the *System Proposer*, that in this case is an engineer, currently employed in Visual Tools, experienced in the design of surveillance solutions, with a certain degree of legal knowledge and practical expertise in the deployment of surveillance systems.

Identification and analysis of stakeholder's needs

The first task of the *System Proposer* is the identification of the stakeholder's needs and the collection of requirements and constraints for a possible solution. This is an iterative process, as several interviews with the stakeholder are normally required to obtain all the information needed and to evaluate the viability and adequacy of the possible solutions.

In a first iteration, the *System Proposer* obtained the following requirements from the Data Controller:

Goal	• Surveillance of the office during the night period (from 9PM to 7AM).
Location	• Visual Tools' office in Madrid (Spain), thus the system shall comply with the Spanish legislation for surveillance systems in private spaces.
Others	• Valuable hardware equipment and software applications subject to intellectual rights protection are stored in many places throughout the office (not just in one storeroom). • During the night period, there are maintenance employees working at the office. They wear uniforms and have their own front door key. • The office already has a PIR alarm system installed but it has to be switched off at night while the maintenance employees are working to avoid false alarms. • False alarms can cost a lot of money in fees, so the number of false alarms should be reduced as much as possible. • The office also has a video surveillance system installed but it is very difficult for system operators to monitor or review many hours of video from multiple cameras and react quickly to an incident. • The solution shall make use of the existing infrastructure whenever possible. • Low cost • Privacy-aware solution

Table 8: Summary of the initial requirements from the stakeholder

Taking into account this initial set of requirements, the *System Proposer* drafts one or several proposals for a solution, including at least an idea of the technologies that can be used and of the system architecture in each case.

In this case, the *System Proposer* evaluated the following solutions:

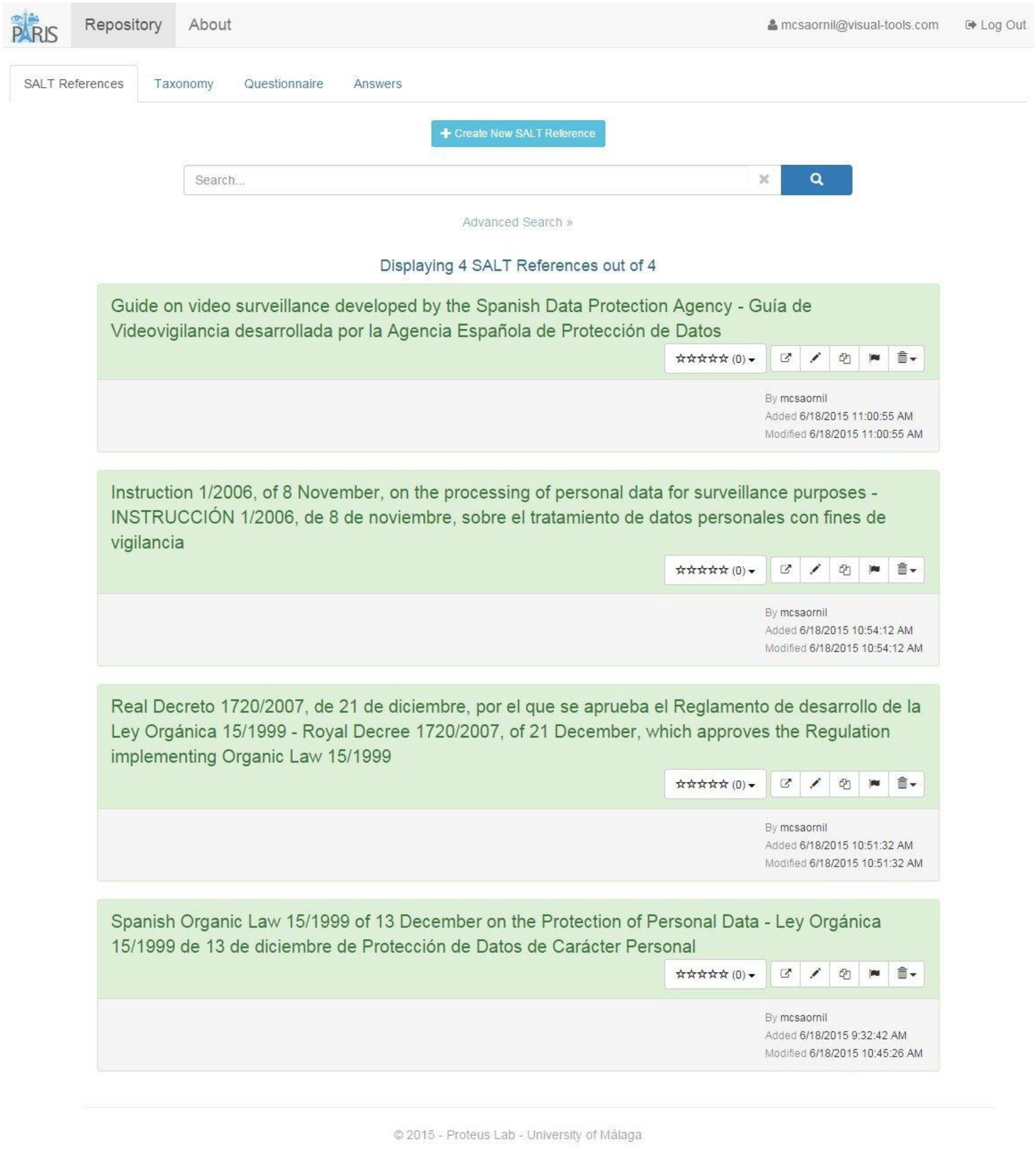
- Hire a security guard to monitor the offices during the night period (non-technical solution);
- An access control system located at the front door based on ID cards;
- System based on biometrics, allowing to detect automatically any person entering the office.

Collection of requirements from the SALT Framework

With all this information in mind, the *System Proposer* makes use of the SALT Framework Tools to complete the list of requirements with a set of privacy and accountability concerns for the use case.

Using the SALT Framework, it is possible to consult the main recommendations in terms of privacy and accountability that can be applied to the use case in the form of SALT References.

Mainly, at this initial stage, legal references are consulted in order to obtain legal requirements that have to be applied to the use case. In this case, the *System Proposer* started looking for legal references that can be applied to a system deployed in Spain, therefore the first references consulted where extracted from the Spanish legal framework (WP6_REF_3-6). Examples of requirements extracted from this references can be found in Table 1 (e.g. REQ_LEG_*, REQ_VSS_*).



Displaying 4 SALT References out of 4

Guide on video surveillance developed by the Spanish Data Protection Agency - Guía de Videovigilancia desarrollada por la Agencia Española de Protección de Datos

☆☆☆☆☆ (0)

By mcsaornil
Added 6/18/2015 11:00:55 AM
Modified 6/18/2015 11:00:55 AM

Instruction 1/2006, of 8 November, on the processing of personal data for surveillance purposes - INSTRUCCIÓN 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia

☆☆☆☆☆ (0)

By mcsaornil
Added 6/18/2015 10:54:12 AM
Modified 6/18/2015 10:54:12 AM

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 - Royal Decree 1720/2007, of 21 December, which approves the Regulation implementing Organic Law 15/1999

☆☆☆☆☆ (0)

By mcsaornil
Added 6/18/2015 10:51:32 AM
Modified 6/18/2015 10:51:32 AM

Spanish Organic Law 15/1999 of 13 December on the Protection of Personal Data - Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal

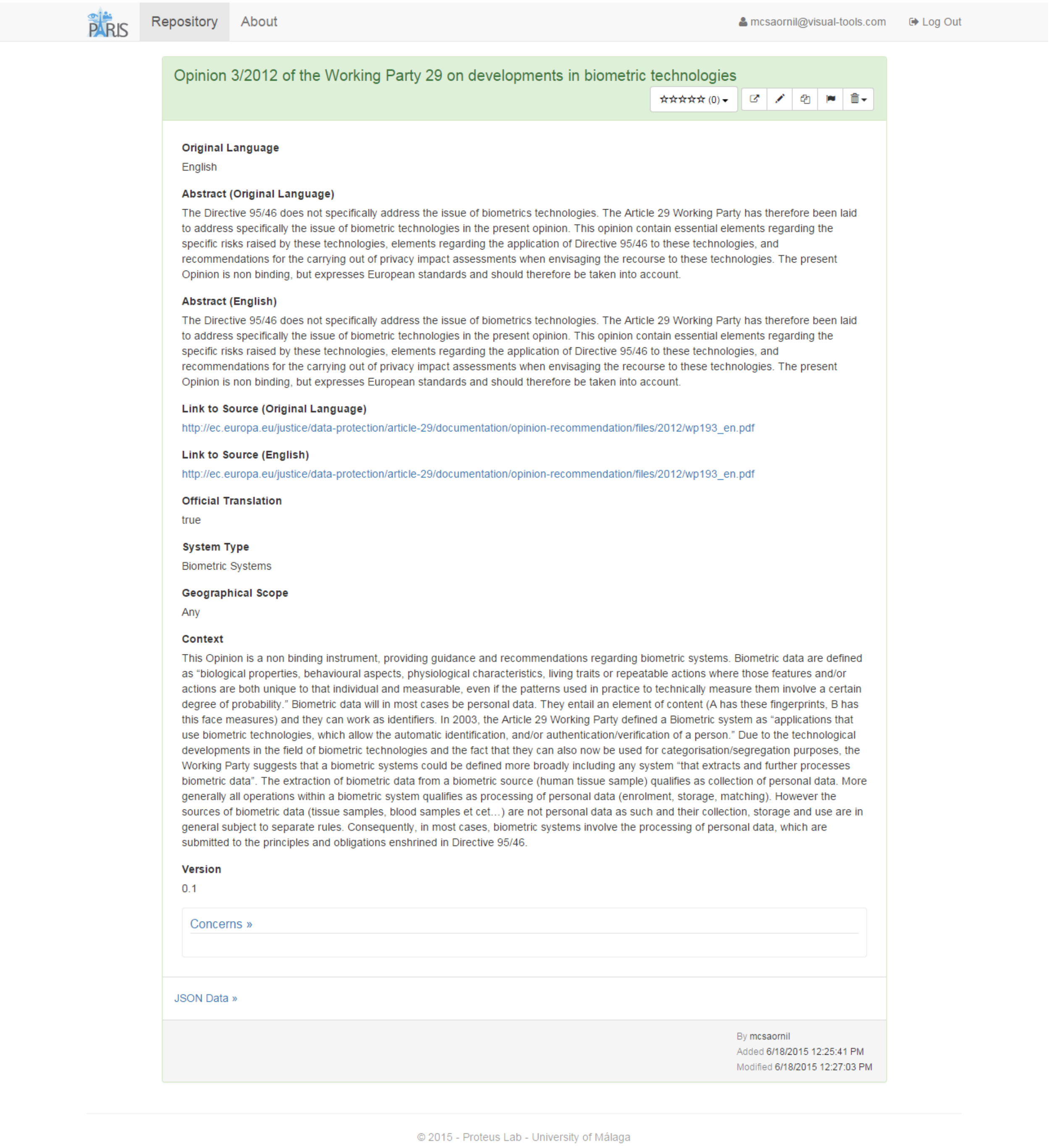
☆☆☆☆☆ (0)

By mcsaornil
Added 6/18/2015 9:32:42 AM
Modified 6/18/2015 10:45:26 AM

© 2015 - Proteus Lab - University of Málaga

Figure 11: SALT Repository - Searching references from the Spanish legal framework

Technical references could also be looked up to get information about the available technologies that can be used and the data protection risks associated to each of them, such as WP6_REF_8 that includes concerns about the use of biometric technologies, or WP6_REF_5-6 that are specific for video surveillance. This information can help the System Proposer in the process of selection of the most suitable solution to solve the stakeholder's problems.



Opinion 3/2012 of the Working Party 29 on developments in biometric technologies

Original Language

English

Abstract (Original Language)

The Directive 95/46 does not specifically address the issue of biometrics technologies. The Article 29 Working Party has therefore been laid to address specifically the issue of biometric technologies in the present opinion. This opinion contain essential elements regarding the specific risks raised by these technologies, elements regarding the application of Directive 95/46 to these technologies, and recommendations for the carrying out of privacy impact assessments when envisaging the recourse to these technologies. The present Opinion is non binding, but expresses European standards and should therefore be taken into account.

Abstract (English)

The Directive 95/46 does not specifically address the issue of biometrics technologies. The Article 29 Working Party has therefore been laid to address specifically the issue of biometric technologies in the present opinion. This opinion contain essential elements regarding the specific risks raised by these technologies, elements regarding the application of Directive 95/46 to these technologies, and recommendations for the carrying out of privacy impact assessments when envisaging the recourse to these technologies. The present Opinion is non binding, but expresses European standards and should therefore be taken into account.

Link to Source (Original Language)

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Link to Source (English)

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Official Translation

true

System Type

Biometric Systems

Geographical Scope

Any

Context

This Opinion is a non binding instrument, providing guidance and recommendations regarding biometric systems. Biometric data are defined as "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability." Biometric data will in most cases be personal data. They entail an element of content (A has these fingerprints, B has this face measures) and they can work as identifiers. In 2003, the Article 29 Working Party defined a Biometric system as "applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person." Due to the technological developments in the field of biometric technologies and the fact that they can also now be used for categorisation/segregation purposes, the Working Party suggests that a biometric systems could be defined more broadly including any system "that extracts and further processes biometric data". The extraction of biometric data from a biometric source (human tissue sample) qualifies as collection of personal data. More generally all operations within a biometric system qualifies as processing of personal data (enrolment, storage, matching). However the sources of biometric data (tissue samples, blood samples et cet…) are not personal data as such and their collection, storage and use are in general subject to separate rules. Consequently, in most cases, biometric systems involve the processing of personal data, which are submitted to the principles and obligations enshrined in Directive 95/46.

Version

0.1

Concerns »

JSON Data »

By mcsaornil
Added 6/18/2015 12:25:41 PM
Modified 6/18/2015 12:27:03 PM

© 2015 - Proteus Lab - University of Málaga

Figure 12: SALT Repository - Example of SALT References applicable to biometrics

Analysis of possible solutions and viability

Once the requirements are clear, it is time to analyze the available solutions in terms of viability. For this task, given a set of solutions to the stakeholder problem, the selection of the most suitable approach is normally based on the performance expected from the system, the ease of use, the user acceptance, the security level required and other type of non-technical constraints that have been already explained in D6.1 (section *2.1.4.2 Selection of biometric technologies*).

In this particular case, these are the main factors that have been considered:

- *Cost of the solution:*

  The stakeholder requires a solution at the lowest possible cost. In the case of hiring one or two security guards five days a week for the night period, to monitor all the cameras and to carry out several patrols, the cost is too expensive for the company in the long run.

- *Environmental constraints:*

  The characteristics of the Visual Tools premises in Madrid imply several limitations. For example, the building has two entrances from the street, which complicates the implementation of a typical access control system.

  Besides, the company offices are spread through 3 floors with a total area of 1000 m^2. The current video surveillance system cannot capture all area and it is limited, because the cameras on the ground floor are positioned in a way they do not capture the street view which is visible through glass windows, thus an incident could happen without being captured by the cameras.

  Finally, as there are going to be maintenance employees working during the night period, it is important to define a solution that is not affected by this, avoiding the generation of false alarms produced by the access or movement of the people that is expected to be working at the office at night.

- *Ease of integration with current procedures and operations:*

  The solution should adjust as much as possible to the operations already carried out to monitor the office. Right now, there are system operators in charge of monitoring remotely the office and verifying any alarm fired by the PIR system before reporting any incident to the local authorities. On the one hand, the selected solution should facilitate as much as possible the tasks of detection of unauthorized accesses and the discard of false alarms. On the other hand, the new system can take advantage of the existence of a human verification to accept a lower system accuracy.

Considering all the factors, the most suitable solution should be able to detect any person accessing the office, and to send an alert to the system operator only when that person is not allowed to be there during the night period. This is why the *System Proposer* presented a solution combining detection and matching of people against a database of authorized personnel. This can be achieved through the use of biometric technologies that allow to identify the people accessing to the office.

Normally, the *System Proposer* is responsible for evaluating several solutions and technologies from different service providers in order to select the best option at the right cost, but this case is different, as the stakeholder company is also a provider of solutions for surveillance. In this case, the *System Proposer* evaluates the use of the biometric algorithms developed by the stakeholder company: an algorithm for face recognition and an algorithm to extract bodyprints. As the bodyprints are apparently more privacy-friendly, as they do not reveal by themselves any personal information, the *System Proposer* prefers that option.

Although the bodyprints technology is quite new, the results of the algorithm tests showed a good performance for the recognition of people wearing uniforms under conditions similar to the scenario where the system will be deployed.

A bodyprints system is similar to other video surveillance systems, as it uses cameras to capture information from data subjects, the only difference is that it has the capability of extracting biometric features of an individual from the images collected. These features, stored in the form of biometric templates or bodyprints, are sufficiently distinctive to discriminate people, even with similar clothes. In this type of system, no interaction from data subjects is required, and the system can be configured to send alerts to the operators monitoring the office remotely, which fits perfectly with the current surveillance operations carried out at the office. This makes the solution based on bodyprints, by now, a suitable approach.

4.1.2 Definition of purpose and initial evaluation

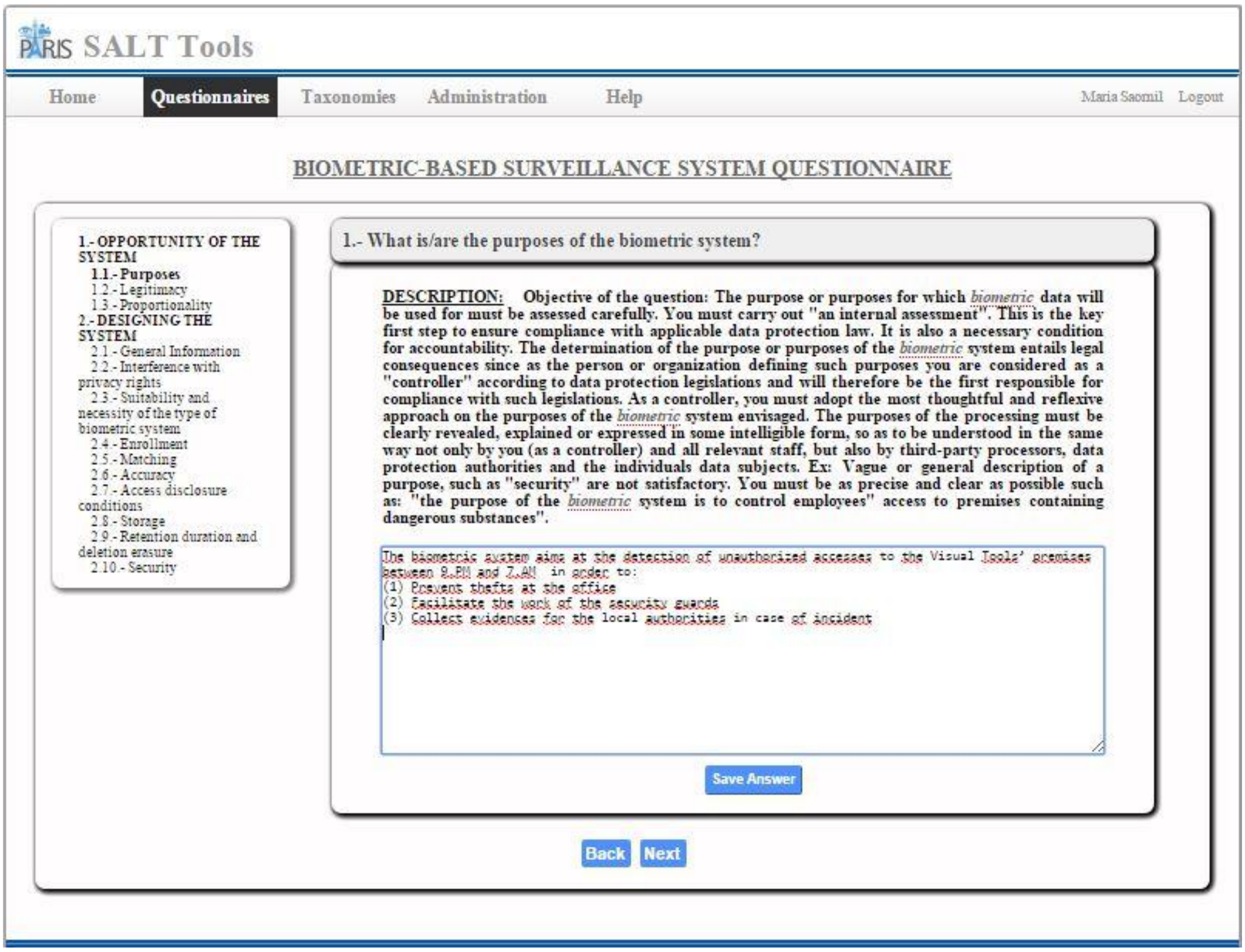
After understanding the customer needs, the *System Proposer* uses the SALT Framework to assess the solution drafted.

As the solution is based on biometric technologies, the bodyprints, the *System Proposer* can use the questionnaire for biometrics included in the framework. The questionnaire, for this *Concept phase*, allows to evaluate the opportunity of the system in terms of legitimacy and proportionality. In addition, the questions addressed to the design of the system, can be also reviewed at this initial stage to identify the privacy risks associated to the different approaches, which can be useful to reconsider the solution selected.

Purpose definition

First of all, it is required to define the purpose of the system, for which it is necessary to analyze in depth the stakeholder's needs and the concrete problems that have to be solved, starting with the most relevant.

Taking into account all the information provided by the stakeholder, we can state that the main purpose of the system is theft prevention at the office. Moreover, the system should cover other secondary uses: facilitate the work of system operators and collect evidences in case of intrusion for law enforcement.



BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

1.- What is/are the purposes of the biometric system?

DESCRIPTION: Objective of the question: The purpose or purposes for which biometric data will be used for must be assessed carefully. You must carry out "an internal assessment". This is the key first step to ensure compliance with applicable data protection law. It is also a necessary condition for accountability. The determination of the purpose or purposes of the biometric system entails legal consequences since as the person or organization defining such purposes you are considered as a "controller" according to data protection legislations and will therefore be the first responsible for compliance with such legislations. As a controller, you must adopt the most thoughtful and reflexive approach on the purposes of the biometric system envisaged. The purposes of the processing must be clearly revealed, explained or expressed in some intelligible form, so as to be understood in the same way not only by you (as a controller) and all relevant staff, but also by third-party processors, data protection authorities and the individuals data subjects. Ex: Vague or general description of a purpose, such as "security" are not satisfactory. You must be as precise and clear as possible such as: "the purpose of the biometric system is to control employees" access to premises containing dangerous substances".

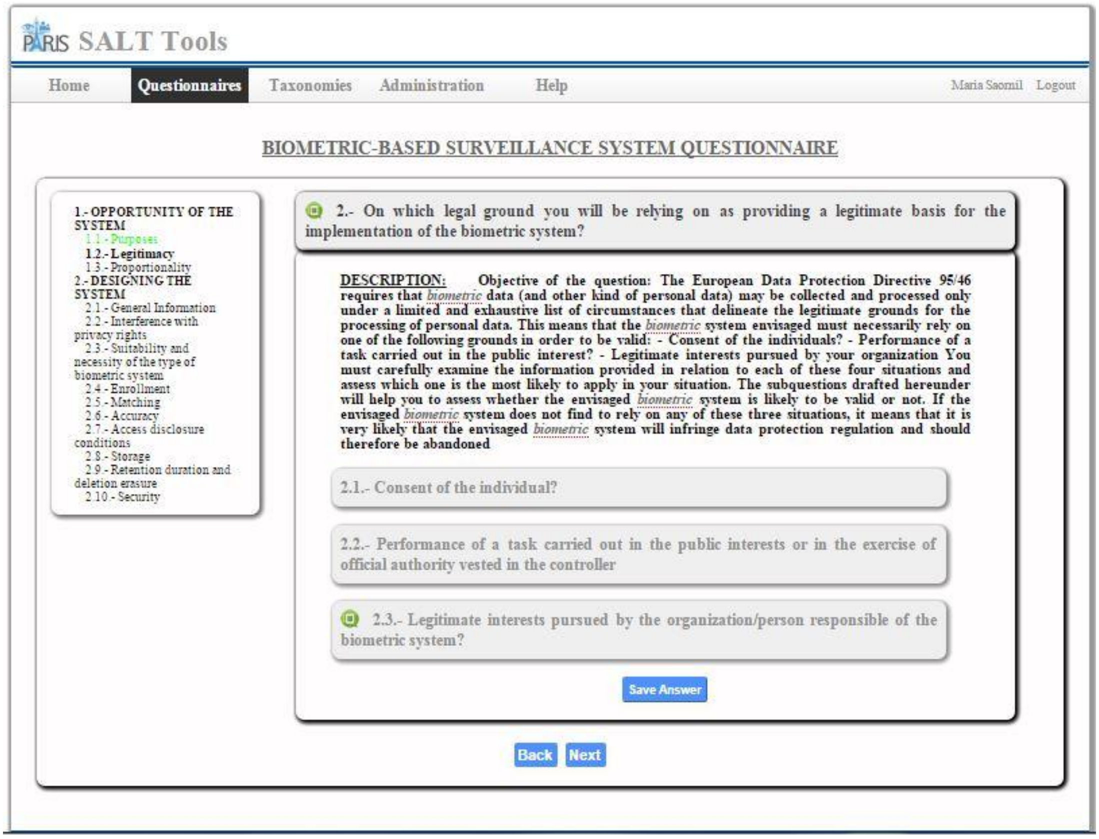
```
The biometric system aims at the detection of unauthorized accesses to the Visual Tools' premises
between 9.PM and 7.AM  in order to:
(1) Prevent thefts at the office
(2) Facilitate the work of the security guards
(3) Collect evidences for the local authorities in case of incident
```

Figure 13: SALT Repository - Questionnaire for biometrics: purpose definition

The purpose definition is addressed in requirements *REQ_QUE_1, REQ_LEG_1 and REQ_ACC_1.*

Legitimacy

The questionnaire points out that *the European Data Protection Directive 95/46 requires that biometric data (and other kind of personal data) may be collected and processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data*. To justify the legitimacy of the system, the questionnaire provides three options of legal ground in which the system shall rely in order to be valid.



BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

2.- On which legal ground you will be relying on as providing a legitimate basis for the implementation of the biometric system?

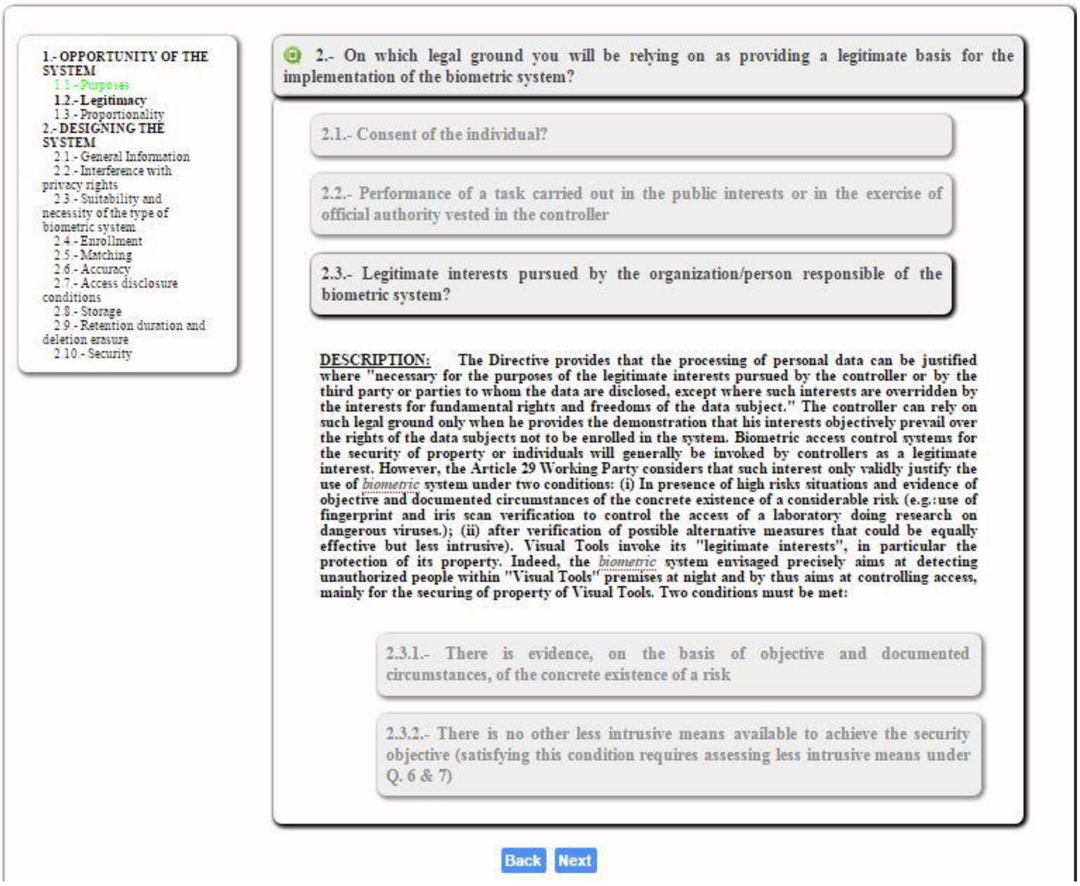
DESCRIPTION: Objective of the question: The European Data Protection Directive 95/46 requires that biometric data (and other kind of personal data) may be collected and processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data. This means that the biometric system envisaged must necessarily rely on one of the following grounds in order to be valid: - Consent of the individuals? - Performance of a task carried out in the public interest? - Legitimate interests pursued by your organization You must carefully examine the information provided in relation to each of these four situations and assess which one is the most likely to apply in your situation. The subquestions drafted hereunder will help you to assess whether the envisaged biometric system is likely to be valid or not. If the envisaged biometric system does not find to rely on any of these three situations, it means that it is very likely that the envisaged biometric system will infringe data protection regulation and should therefore be abandoned

2.1.- Consent of the individual?

2.2.- Performance of a task carried out in the public interests or in the exercise of official authority vested in the controller

2.3.- Legitimate interests pursued by the organization/person responsible of the biometric system?

Figure 14: SALT Repository - Questionnaire for biometrics: legitimacy (I)


1.- OPPORTUNITY OF THE SYSTEM
1.1 - Purposes
1.2.- Legitimacy
1.3 - Proportionality
2.- DESIGNING THE SYSTEM
2.1 - General Information
2.2 - Interference with privacy rights
2.3 - Suitability and necessity of the type of biometric system
2.4 - Enrollment
2.5 - Matching
2.6 - Accuracy
2.7 - Access disclosure conditions
2.8 - Storage
2.9 - Retention duration and deletion erasure
2.10 - Security
Back
Next

2.- On which legal ground you will be relying on as providing a legitimate basis for the implementation of the biometric system?

2.1.- Consent of the individual?

2.2.- Performance of a task carried out in the public interests or in the exercise of official authority vested in the controller

2.3.- Legitimate interests pursued by the organization/person responsible of the biometric system?

DESCRIPTION: The Directive provides that the processing of personal data can be justified where "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject." The controller can rely on such legal ground only when he provides the demonstration that his interests objectively prevail over the rights of the data subjects not to be enrolled in the system. Biometric access control systems for the security of property or individuals will generally be invoked by controllers as a legitimate interest. However, the Article 29 Working Party considers that such interest only validly justify the use of biometric system under two conditions: (i) In presence of high risks situations and evidence of objective and documented circumstances of the concrete existence of a considerable risk (e.g.:use of fingerprint and iris scan verification to control the access of a laboratory doing research on dangerous viruses.); (ii) after verification of possible alternative measures that could be equally effective but less intrusive). Visual Tools invoke its "legitimate interests", in particular the protection of its property. Indeed, the biometric system envisaged precisely aims at detecting unauthorized people within "Visual Tools" premises at night and by thus aims at controlling access, mainly for the securing of property of Visual Tools. Two conditions must be met:

2.3.1.- There is evidence, on the basis of objective and documented circumstances, of the concrete existence of a risk

2.3.2.- There is no other less intrusive means available to achieve the security objective (satisfying this condition requires assessing less intrusive means under Q. 6 & 7)

Figure 15: SALT Repository - Questionnaire for biometrics: legitimacy (II)

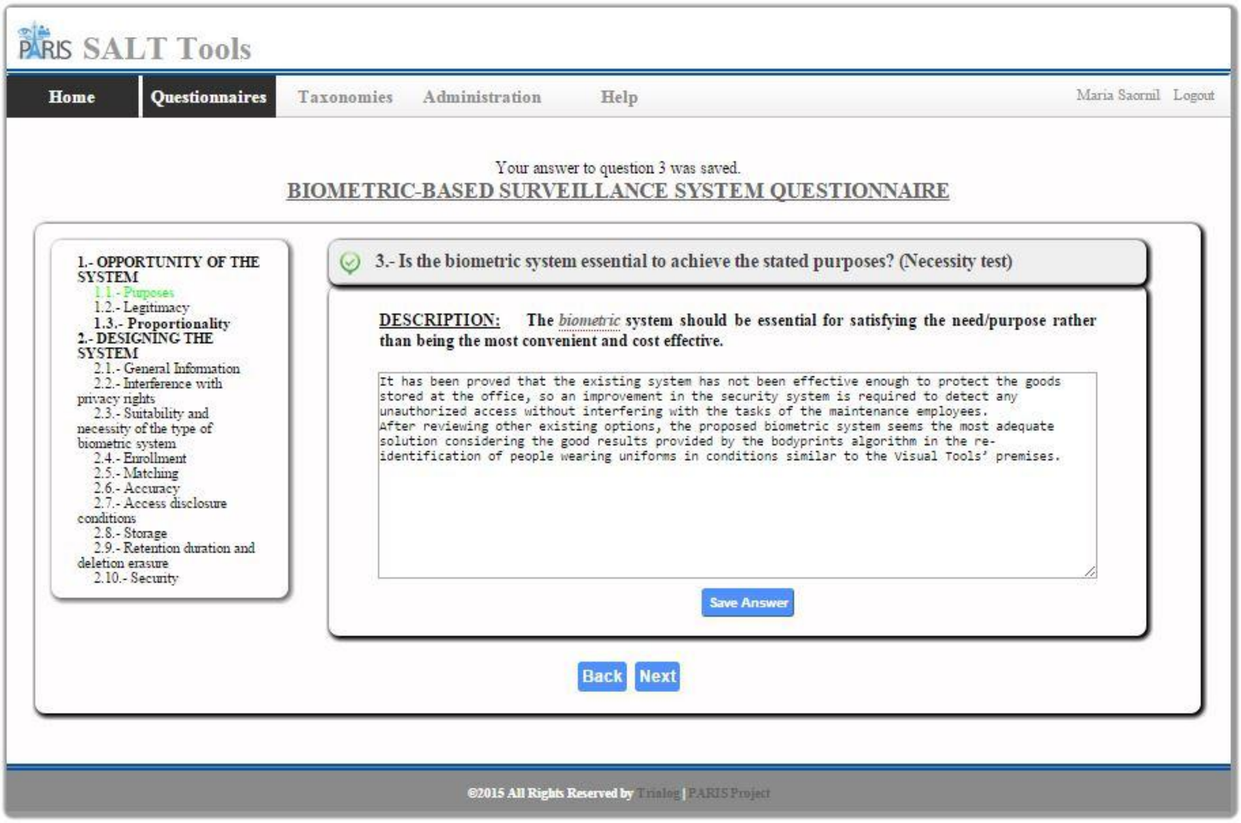
In the scenario described in this document, the *Data Controller* (Visual Tools) wants to improve the existing security mechanisms implemented in the office, as they have proved to be insufficient, because some material has disappeared during the night period without anyone noticing and without firing any alarm. Taking into account the solution provided by the *System Proposer*, the processing of biometric data is required to prevent thefts at the office, controlling who accesses for the security of property. Therefore, in this case the *Data Controller* invokes its "legitimate interests".

As explained in this section, the *System Proposer* has also considered other solutions, even non-technical solutions such as hiring security guards, but they have all been discarded because they do not solve completely the problem or do not comply with the main stakeholder's requirements (e.g. budget).

The legitimacy of the system is addressed in requirements *REQ_QUE_2, REQ_LEG_1 and REQ_ACC_1.*

Proportionality

The questionnaire also stresses the importance of justifying the necessity and suitability of the system and the selected technologies for the defined purpose. This is not only a requirement of the European Data Protection Directive 95/46/EC, but also a requirement of the Spanish legislation, which is particularly critical when processing biometric data: a project based on biometrics can be disapproved by the *Data Protection Authorities* if it doesn't provide a fair balance of its purposes in terms of proportionality and beneficence.



Your answer to question 3 was saved.

BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

3.- Is the biometric system essential to achieve the stated purposes? (Necessity test)

DESCRIPTION: The *biometric* system should be essential for satisfying the need/purpose rather than being the most convenient and cost effective.

```
It has been proved that the existing system has not been effective enough to protect the goods
stored at the office, so an improvement in the security system is required to detect any
unauthorized access without interfering with the tasks of the maintenance employees.
After reviewing other existing options, the proposed biometric system seems the most adequate
solution considering the good results provided by the bodyprints algorithm in the re-
identification of people wearing uniforms in conditions similar to the Visual Tools’ premises.
```

©2015 All Rights Reserved by Trialog | PARIS Project

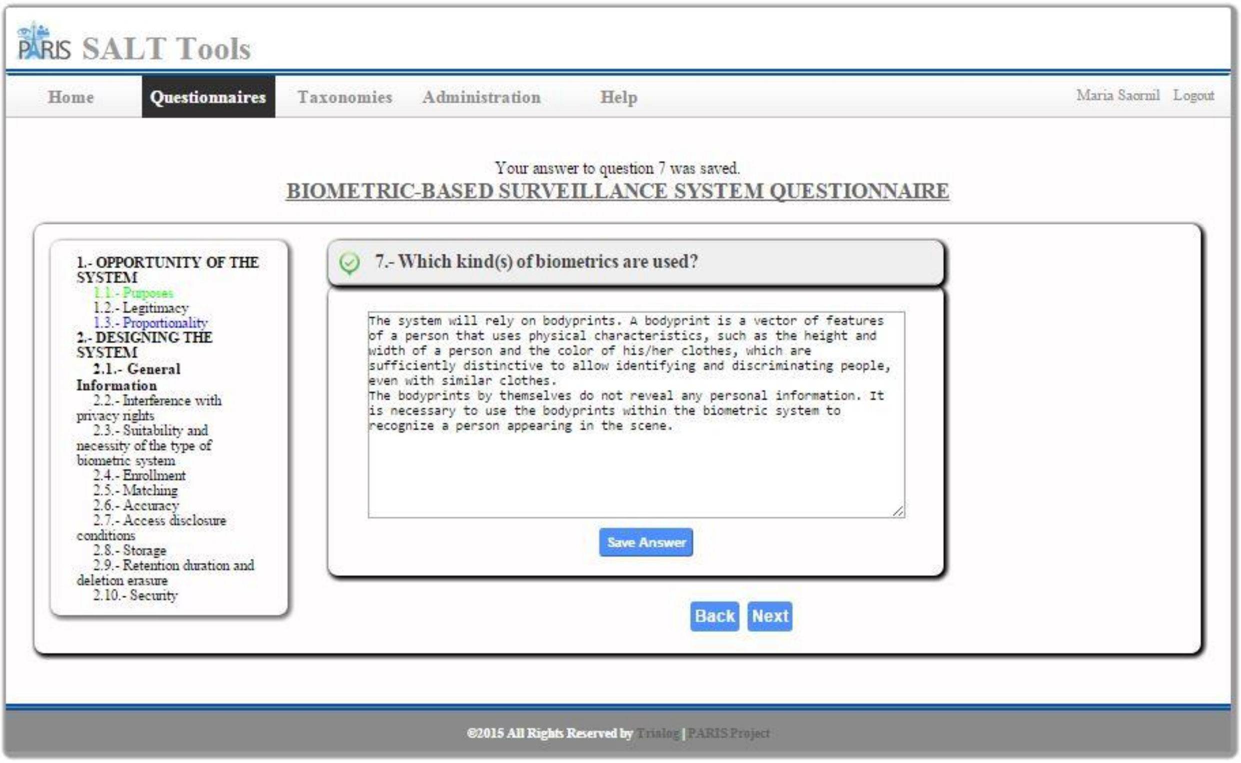
Figure 16: SALT Repository - Questionnaire for biometrics: proportionality

In the scenario described in this document, it has been proved that the existing system has not been effective enough to protect the goods stored at the office, so an improvement in the security system is required to detect any unauthorized access without interfering with the tasks of the maintenance employees. After reviewing other existing options, even non-technological options, the proposed biometric system seems the most adequate solution considering the good results provided by the bodyprints algorithm in the re-identification of people wearing uniforms in conditions similar to the Visual Tools' premises, and all the stakeholder requirements.

The proportionality of the system purpose is addressed in requirements *REQ_QUE_3, REQ_LEG_1 and REQ_ACC_1.*

Other questions applicable to the *Concept* stage

In the *Concept* stage, it is also advisable to review the questions addressed to the design stage to have in mind the main privacy and accountability concerns related to the technologies selected and to the design decisions that can be taken during the viability analysis.



Your answer to question 7 was saved.

BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

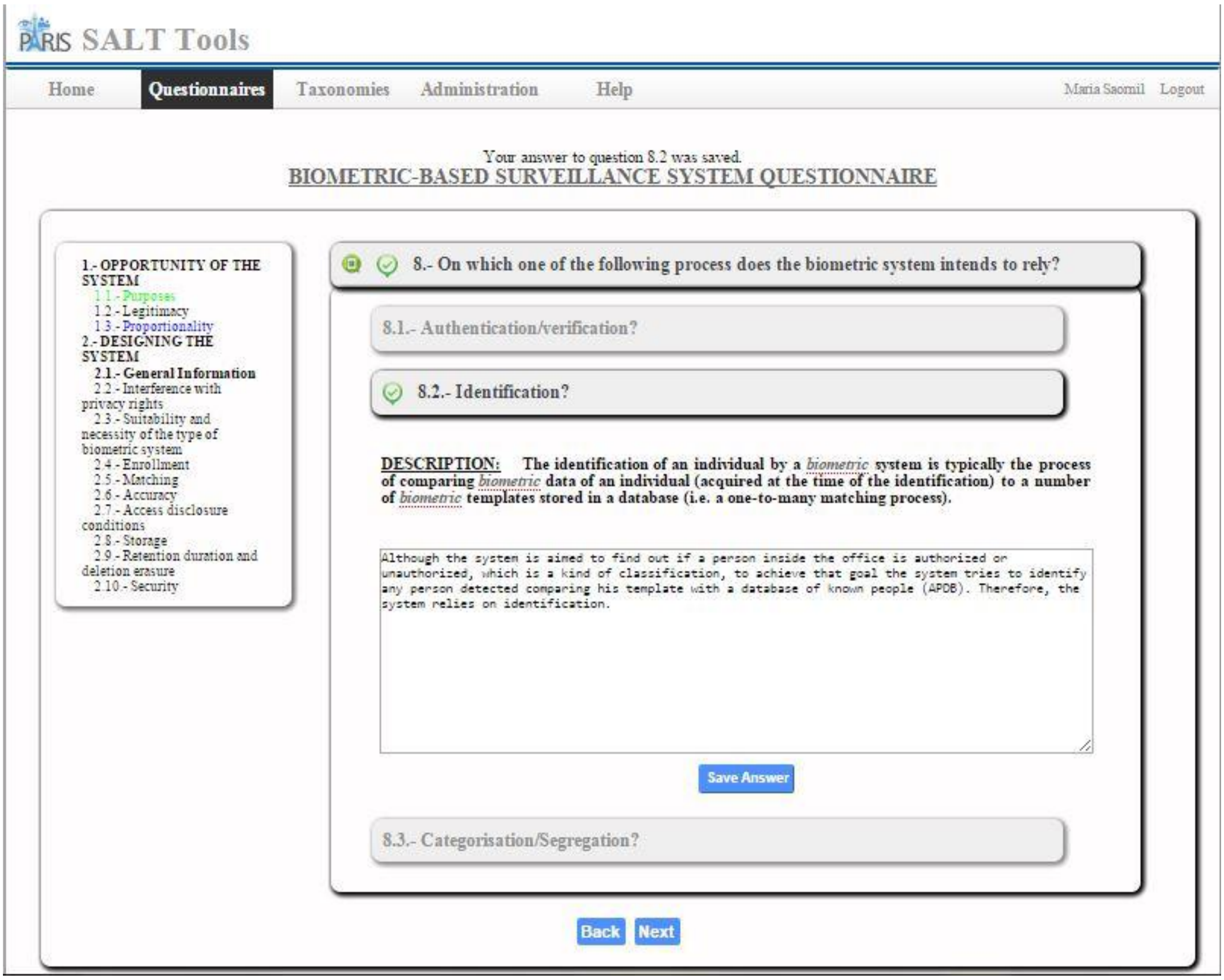
1.- OPPORTUNITY OF THE SYSTEM
- 1.1.- Purposes
- 1.2.- Legitimacy
- 1.3.- Proportionality

2.- DESIGNING THE SYSTEM
- **2.1.- General Information**
- 2.2.- Interference with privacy rights
- 2.3.- Suitability and necessity of the type of biometric system
- 2.4.- Enrollment
- 2.5.- Matching
- 2.6.- Accuracy
- 2.7.- Access disclosure conditions
- 2.8.- Storage
- 2.9.- Retention duration and deletion erasure
- 2.10.- Security

7.- Which kind(s) of biometrics are used?

```
The system will rely on 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.
The bodyprints by themselves do not reveal any personal information. It
is necessary to use the bodyprints within the biometric system to
recognize a person appearing in the scene.
```

Figure 17: SALT Repository - Questionnaire for biometrics: designing the system (I)



Your answer to question 8.2 was saved.

BIOMETRIC-BASED SURVEILLANCE SYSTEM QUESTIONNAIRE

1.- OPPORTUNITY OF THE SYSTEM
1.1.- Purposes
1.2.- Legitimacy
1.3.- Proportionality
2.- DESIGNING THE SYSTEM
2.1.- General Information
2.2.- Interference with privacy rights
2.3.- Suitability and necessity of the type of biometric system
2.4.- Enrollment
2.5.- Matching
2.6.- Accuracy
2.7.- Access disclosure conditions
2.8.- Storage
2.9.- Retention duration and deletion erasure
2.10.- Security

8.- On which one of the following process does the biometric system intends to rely?

8.1.- Authentication/verification?

8.2.- Identification?

DESCRIPTION: The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

Although the system is aimed to find out if a person inside the office is authorized or unauthorized, which is a kind of classification, to achieve that goal the system tries to identify any person detected comparing his template with a database of known people (APDB). Therefore, the system relies on identification.

8.3.- Categorisation/Segregation?

Figure 18: SALT Repository - Questionnaire for biometrics: designing the system (II)

These are some of the privacy and accountability issues considered of particular relevance by the *System Proposer* for the use case at this initial stage, before the elaboration of the system design:

- Level of risk associated to the type of recognition process performed in terms of privacy (identification, verification or categorization).
- Need to analyze the data protection risks associated to the technologies selected, especially taking into account the risks related to identity theft, the misuse of data and the consequences of an error in the matching process.
- Need to involve data subjects in the enrolment and matching processes whenever possible.
- Whenever it is permitted to process biometric data, it is preferred to avoid the centralized storage of the personal biometric information.

At the end of the *Concept Stage*, the main technologies to use are selected, and the *System Proposer* has a general idea about how the solution can be implemented taking privacy and accountability into account. With this idea, the *System Proposer* elaborates the requirements specification for the system.

At this initial stage of the development process, the questionnaire for biometrics is used as an artifact to perform a privacy impact assessment of the different solutions being considered to solve the stakeholder's problem.

Artifacts used	
A1	SALT Framework questionnaire for biometrics

Table 9: Artifacts used at the Concept stage

Although it is not included in the list of artifacts, it is also recommended to consult the stakeholders and the data subjects potentially targeted by the system whenever possible to get feedback about how intrusive they perceive the different solutions. In this case, this consultation was not carried out at this initial stage, but we plan to get feedback from data subjects (Visual Tools' employees) during the deployment stage.

4.2 Elaborating the system design

The design of the system is delegated to an engineer, or a team of engineers, that takes the role of the *System Designer*. In this case, the *System Designer* is an employee of the *Surveillance Service Provider* (Visual Tools).

System Designers may have at least an overall idea of the implementation of the system, and normally the technologies used for the creation of the different system components are selected during the development phase. Therefore, the system specification elaborated during this stage should include as much information as possible about the hardware/software to use, the system architecture, programming languages, communication technologies, security mechanisms, etc. Besides, the specification should also describe the main procedures required for the interaction of the different users with the system.

The following sections describe the process followed to obtain a system design addressing the main privacy and accountability concerns for this particular use case.

4.2.1 Design stage

The *System Designer* elaborates a design of the system following the specification given by the *System Proposer* and the business constraints imposed by the *Surveillance Service Provider*. This process can be iterative, as new issues and requirements can arise during the design process.

Initial system design

In a first attempt to draft the system, this was the design elaborated:

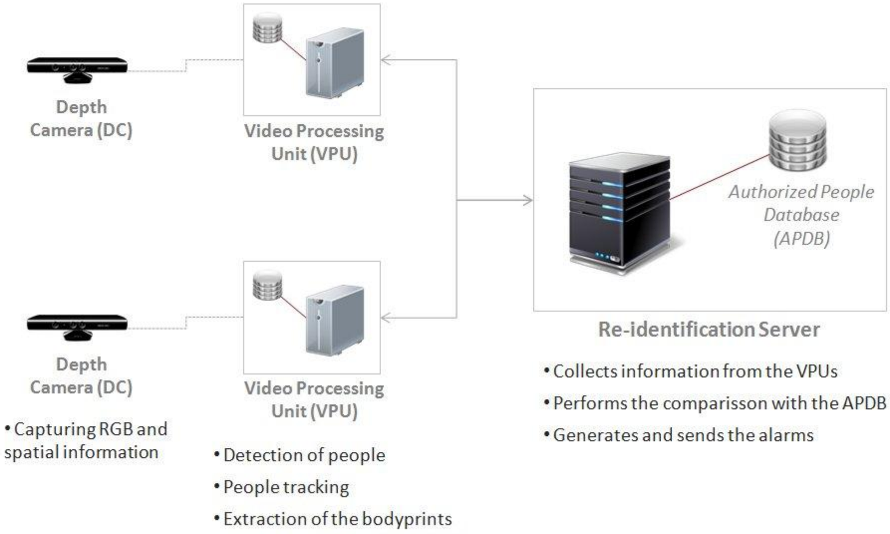
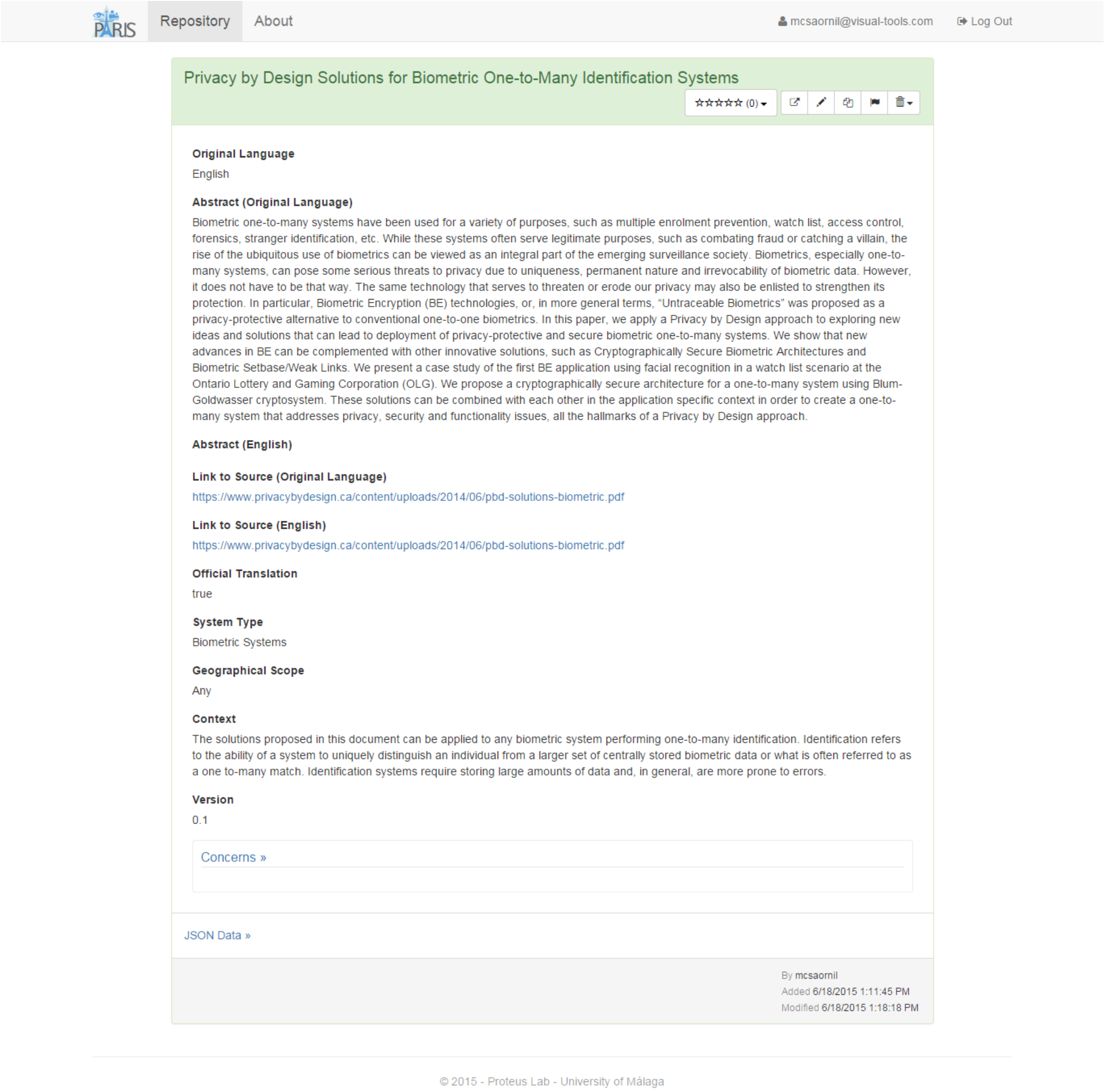

Depth
Camera (DC)
Video Processing
Unit (VPU)
Authorized People
Database
(APDB)
Depth
Camera (DC)
Video Processing
Unit (VPU)
Re-identification Server
• Capturing RGB and spatial information
• Detection of people
• People tracking
• Extraction of the bodyprints
• Collects information from the VPUs
• Performs the comparisson with the APDB
• Generates and sends the alarms

Figure 19: Initial system design

The system is basically composed of three components: depth cameras that capture RGB and spatial information, video processing units (VPU) processing that information and obtaining the bodyprints for each person detected, and a re-identification server comparing the bodyprints against a database of authorized people in order to detect intrusions. This first draft of the system architecture was already detailed in deliverable D6.1.

Consulting the SALT Repository

In order to evaluate the privacy concerns associated to the design drafted, the *System Designer* can consult the SALT Framework, that provides recommendations and guidelines also from a technical perspective in the form of SALT References.



Privacy by Design Solutions for Biometric One-to-Many Identification Systems

Original Language

English

Abstract (Original Language)

Biometric one-to-many systems have been used for a variety of purposes, such as multiple enrolment prevention, watch list, access control, forensics, stranger identification, etc. While these systems often serve legitimate purposes, such as combating fraud or catching a villain, the rise of the ubiquitous use of biometrics can be viewed as an integral part of the emerging surveillance society. Biometrics, especially one-to-many systems, can pose some serious threats to privacy due to uniqueness, permanent nature and irrevocability of biometric data. However, it does not have to be that way. The same technology that serves to threaten or erode our privacy may also be enlisted to strengthen its protection. In particular, Biometric Encryption (BE) technologies, or, in more general terms, "Untraceable Biometrics" was proposed as a privacy-protective alternative to conventional one-to-one biometrics. In this paper, we apply a Privacy by Design approach to exploring new ideas and solutions that can lead to deployment of privacy-protective and secure biometric one-to-many systems. We show that new advances in BE can be complemented with other innovative solutions, such as Cryptographically Secure Biometric Architectures and Biometric Setbase/Weak Links. We present a case study of the first BE application using facial recognition in a watch list scenario at the Ontario Lottery and Gaming Corporation (OLG). We propose a cryptographically secure architecture for a one-to-many system using Blum-Goldwasser cryptosystem. These solutions can be combined with each other in the application specific context in order to create a one-to-many system that addresses privacy, security and functionality issues, all the hallmarks of a Privacy by Design approach.

Abstract (English)

Link to Source (Original Language)

https://www.privacybydesign.ca/content/uploads/2014/06/pbd-solutions-biometric.pdf

Link to Source (English)

https://www.privacybydesign.ca/content/uploads/2014/06/pbd-solutions-biometric.pdf

Official Translation

true

System Type

Biometric Systems

Geographical Scope

Any

Context

The solutions proposed in this document can be applied to any biometric system performing one-to-many identification. Identification refers to the ability of a system to uniquely distinguish an individual from a larger set of centrally stored biometric data or what is often referred to as a one to-many match. Identification systems require storing large amounts of data and, in general, are more prone to errors.

Version

0.1

Concerns »

JSON Data »

By mcsaornil
Added 6/18/2015 1:11:45 PM
Modified 6/18/2015 1:18:18 PM

© 2015 - Proteus Lab - University of Málaga

Figure 20: SALT Repository - Example of technical reference applicable to biometrics

In particular, references WP6_REF_7-9 were consulted by the *System Designer* and considered to take the following design decisions:

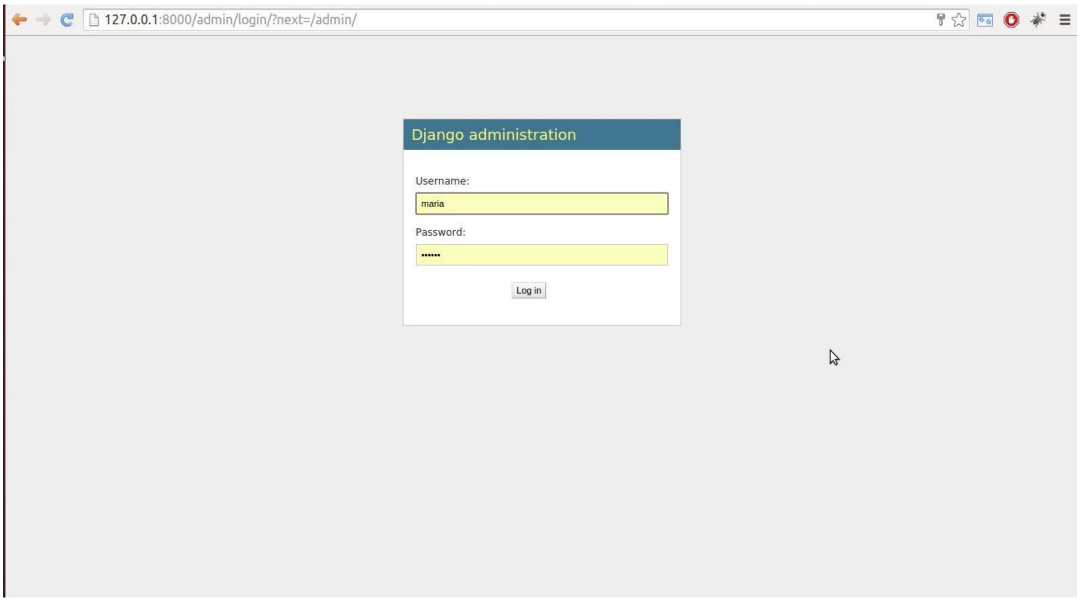
- **Data storage**: Although WP6_REF_8 recommends to use distributed storage for the biometric information, in cases like this where it is required to perform one-to-many comparisons for the identification of data subjects the use of a centralized database is necessary. To protect privacy in this type of systems, WP6_REF_9 recommends to store the data containing personal information separately from the database of biometric templates. Considering this, the *System Designer* decided that it was better to store the key frames separately from the bodyprints and just link the information using alphanumeric identifiers. A key frame, as explained in D6.2, is just an image extracted from the video used to get the bodyprint that serves as a reference to check to whom the bodyprint belongs, and as it can be used to identify a person accessing the office, it should be properly protected.

- **Separate the matching process from the alarm management**: also WP6_REF_9 recommends to separate the "Service Provider" application displaying the results to end users (in this case the *System Operator*) from the components performing the matching and the database of biometric templates. Thus, the *System Designer* decided to limit the tasks performed by the RIS to the collection and comparison of bodyprints, and create a new component to show the results to the *System Operator*, which is the RMS. This way, the end user *(System Operator)* does not have access to the devices storing the biometric data.
- **Encryption of bodyprints**: Both WP6_REF_8 and WP6_REF_9 advise to protect the biometric templates as a measure to prevent the misuse of the biometric information. Even in cases where it is not possible to retrieve the raw biometric data from the template, if there are risks of theft or misuse of the biometric templates, these should be properly protected. Thus, the bodyprints composing the APDB should be stored in an encrypted form. Although the mentioned references recommend the technique of biometric encryption, the *System Designer* decided to protect the whole bodyprint using AES encryption, that provides sufficient security and it is easier to implement and faster to process.
- **Control of unattended operations**: for data collection, usage and storage accountability, WP6_REF_7 recommends to register evidences about data handling in the form of system logs. Although the use of logs was already foreseen, the reference made the *System Designer* refine the information that should be included in the different logs and the process and operations to be traced. The reference also proposes to use log analyzers that can automatically verify the compliance of the system operation with the privacy policies defined, however, the *System Designer* decided to perform this task manually if necessary due to resource restrictions.
- **Access control mechanisms**: in order to register who has access to the information stored in the system (WP6_REF_7), the main resources of each component implement access control mechanisms (e.g. interfaces, web services, databases). Besides, these user profiles were defined at the design stage with different permissions to access the system resources:

User Profile	Permissions
System Administrator	Access to all the information stored in the system Access to all the system applications (configuration, enrolment, etc.)
System Operator	Limited access to the information stored in the system (alarms) Access only to the Surveillance User Interface (alarms)
Supervisor	Access to the information stored in the system related to an incident (access authorized and supervised by the System Administrator)
Data Subject	Access only to his/her personal information stored in the system (access authorized and supervised by the System Administrator)

Table 10: User Profiles defined

Every component (VPU, RIS & RMS) include an administrator panel that can be used by the System Administrator to create system users with different profiles and authorize access (or not) to the different interfaces and resources.



127.0.0.1:8000/admin/login/?next=/admin/

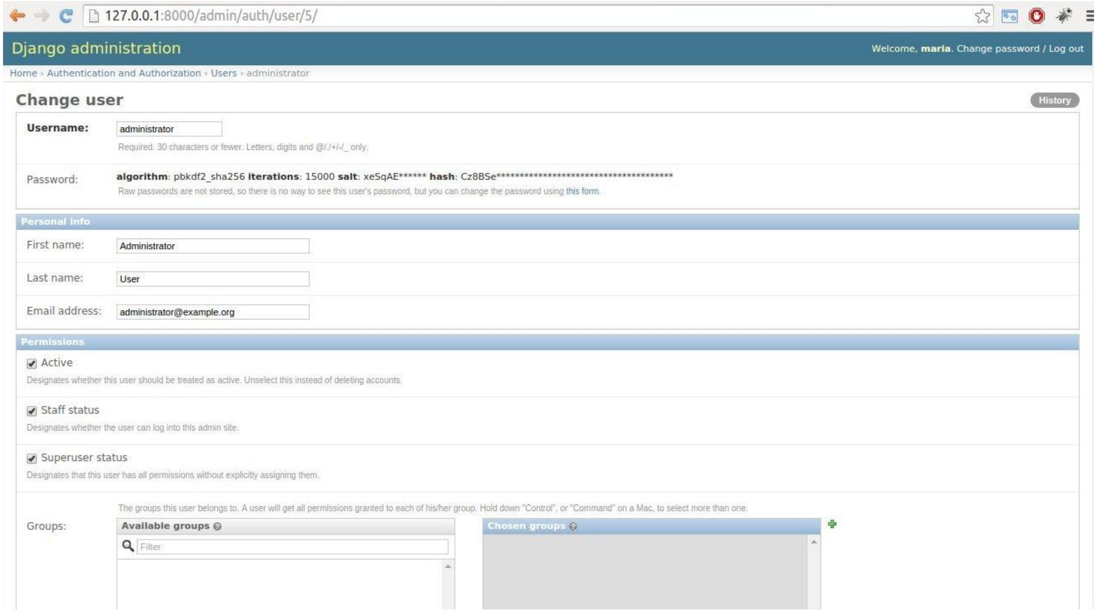
Django administration

Username: maria

Password: ••••••

Log in

Figure 21: Administration panel: Login



127.0.0.1:8000/admin/auth/user/5/

Django administration

Welcome, **maria**. Change password / Log out

Home › Authentication and Authorization › Users › administrator

Change user

History

Username: administrator

Required. 30 characters or fewer. Letters, digits and @/./+/-/_ only.

Password: **algorithm**: pbkdf2_sha256 **iterations**: 15000 **salt**: xeSqAE****** **hash**: Cz8BSe**

Raw passwords are not stored, so there is no way to see this user's password, but you can change the password using this form.

Personal info

First name: Administrator

Last name: User

Email address: administrator@example.org

Permissions

☑ Active

Designates whether this user should be treated as active. Unselect this instead of deleting accounts.

☑ Staff status

Designates whether the user can log into this admin site.

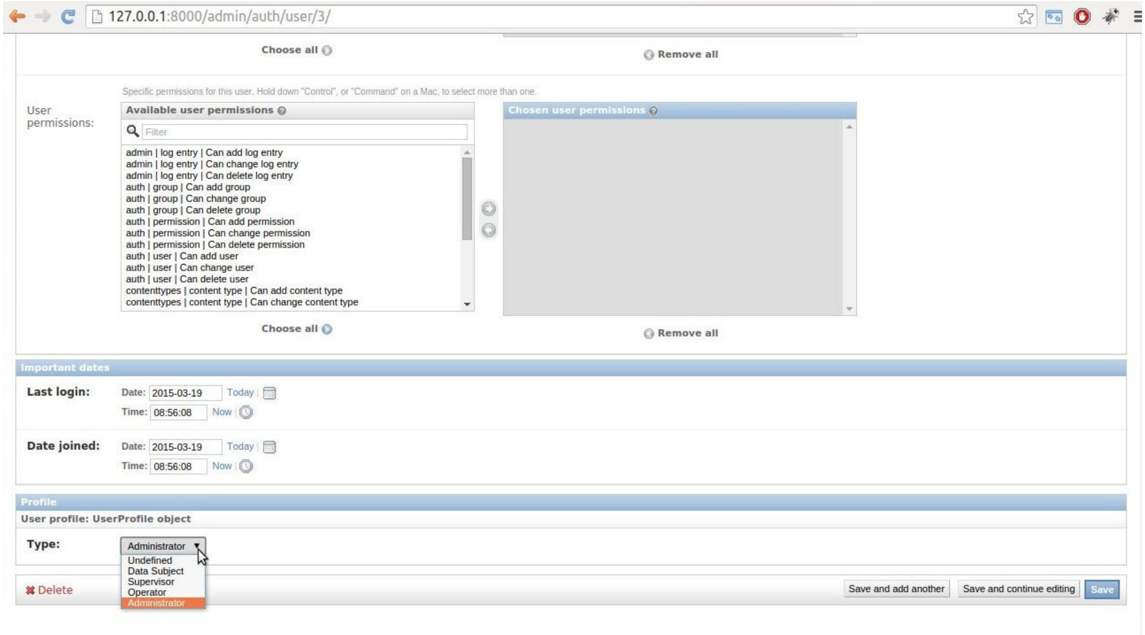
☑ Superuser status

Designates that this user has all permissions without explicitly assigning them.

Groups:

The groups this user belongs to. A user will get all permissions granted to each of his/her group. Hold down "Control", or "Command" on a Mac, to select more than one.

Figure 22: Administration panel: User management (I)



127.0.0.1:8000/admin/auth/user/3/

Specific permissions for this user. Hold down "Control", or "Command" on a Mac, to select more than one.

User permissions:

Available user permissions

admin | log entry | Can add log entry
admin | log entry | Can change log entry
admin | log entry | Can delete log entry
auth | group | Can add group
auth | group | Can change group
auth | group | Can delete group
auth | permission | Can add permission
auth | permission | Can change permission
auth | permission | Can delete permission
auth | user | Can add user
auth | user | Can change user
auth | user | Can delete user
contenttypes | content type | Can add content type
contenttypes | content type | Can change content type

Chosen user permissions

Important dates

Last login: Date: 2015-03-19 Time: 08:56:08

Date joined: Date: 2015-03-19 Time: 08:56:08

Profile

User profile: UserProfile object

Type: Administrator

Figure 23: Administration panel: User management (II)

- **Automated data erasure mechanisms**: the *System Designer*, according to WP6_REF_8, added to the different components mechanisms for the automatic erasure of the bodyprints stored in the system once they are no longer necessary.

Design refinement

After several revisions, and taking into account the information obtained from the SALT References, the system was slightly modified. In the latest version, the system designed is comprised of the following components:

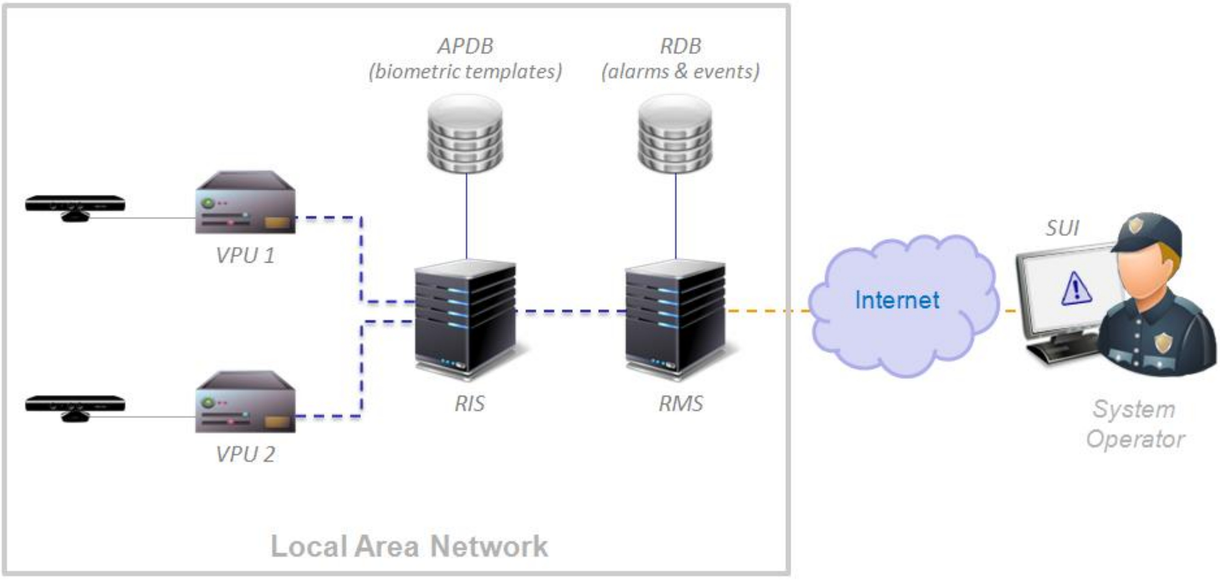


Figure 24: System overview

- **Depth Cameras** (DCAM): Providing RGB and spatial information of the area under surveillance.

- **Video Processing Unit** (VPU). This device is continuously analyzing the images from the depth cameras connected to it to extract the bodyprints of the people appearing in the scene. For each depth camera used, a VPU is required.
- **Re-Identification Server** (RIS), which periodically requests the new bodyprints from each VPU unit installed in the system. Anytime a new bodyprint is obtained, the RIS performs the matching with the template database. The results are temporary stored in the RIS and copied to a directory of the RMS. This server does not have connection to the Internet.
- **Results Management Server** (RMS), which is responsible for managing the alarms and displaying the results to the system operator through a Web UI accessible from a remote location.
- **Authorized People Database** (APDB): template database containing the bodyprints of the people that are authorized to be inside the office at the defined period.
- **Results Database** (RDB): database containing the results of the matching process and the alarms generated.
- **Surveillance User Interface** (SUI): Web user interface displaying the results of the recognition process and allowing to validate or discard the alarms generated. This tool also provides system information for maintenance purposes.

Design specification

As a result of this stage, the specification of the system design is obtained. This specification includes technical information, such as the functional architecture of each component (modules, utilities, etc.) or the main technologies to use in the system implementation, and also the procedures that have to be carried out in order to use the system and fulfill the requirements collected.

System architecture

Regarding the system architecture, this was the main information provided in the system specification:

1. **Video Processing Unit**

These are the modules composing the VPU:

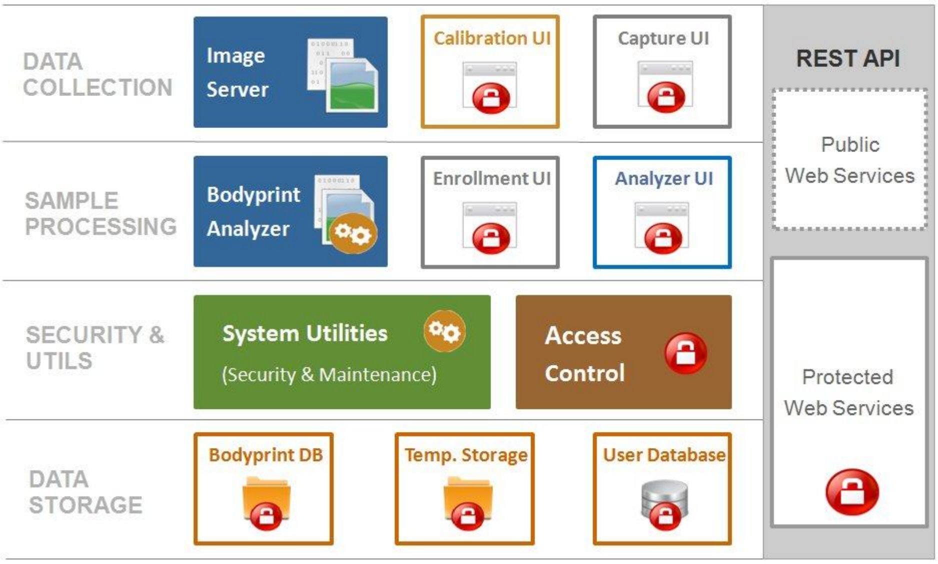


Figure 25: Modules of the Video Processing Unit

Module	Description
Image server	Set of programs allowing to capture data from the depth cameras for enrolment or detection.
Calibration User Interface	Setup assistant facilitating the calibration of the depth cameras. This interface can be used in the deployment stage and also during the maintenance stage.
Capture User Interface	Application that allows to record video sequences for the enrolment of people in the system.
Bodyprint Analyzer	This module processes the RGB and depth information captured by the cameras.
Enrolment User Interface	Application in form of wizard that facilitates the enrolment of people in the system database (enrolment mode).
Analyzer User Interface	Program that allows to start the processing of data for detection (detection mode). This program launches the Bodyprint Analyzer, the Web Server that enables the REST API, and the processes performing the different system monitoring and maintenance tasks in the VPU.
System Utilities: **Data Compression**	Module allowing to compact data files and folders in a compressed file. It is used to optimize the storage of bodyprints, as well as their transmission to the Re-Identification Server.
System Utilities: **Data Encryption**	Module for the protection of data. It is used to protect the bodyprints stored in the system and sent to the RIS, and also for the protection of video sequences during the enrolment phase.
System Utilities: **Bodyprint Manager**	This module is responsible for the management of bodyprints. This task covers the search and provision of the bodyprints requested by the RIS, and also the deletion of bodyprints according to the retention period defined.
System Utilities: **System Monitoring**	Module responsible for the maintenance of the system, that checks periodically that the Video Processing Unit works as expected.
Access Control	This module is used for the authentication and authorization of the users that require access to the different resources provided by the VPU. This module is used, for example, to control the access to the different user interfaces and also to the Web services.

Bodyprint Database	The bodyprints extracted by the VPU are stored in the Bodyprint Database until they are collected by the RIS for enrolment or detection. The bodyprint database contains a folder for each person detected that includes the corresponding bodyprint, the results of the detection/tracking processes, a key frame and also the detection timestamp. All the information in the Bodyprint Database is stored compressed and encrypted.
Temporary Storage	The data captured by the depth cameras is temporary stored in the VPU for a defined period of time (retention period).
User Database	It contains the system users that are able to access to the different resources of the VPU.
REST API	Set of Web Services providing information obtained and stored in the Video Processing Unit: • *Public Web Services*: the service providing a description of the Video Processing Unit is public. • *Protected Web Services*: the set of web services for the collection of data of the VPU are protected by authentication and authorization mechanisms.

Table 11: Modules of the Video Processing Unit

During the **enrolment**, the VPU is used for the extraction of the bodyprints of the people to be enrolled in the system database as authorized. The bodyprints in this case are obtained from videos recorded with the *Capture UI*.

On the other hand, when the system works in **detection mode**, the VPU is continuously analysing the data provided by the depths cameras, that is processed on the fly to obtain in almost real time the bodyprints of the people appearing in the area under surveillance.

2. **Re-Identification Server** & **Authorized People Database**

The RIS uses the following modules:

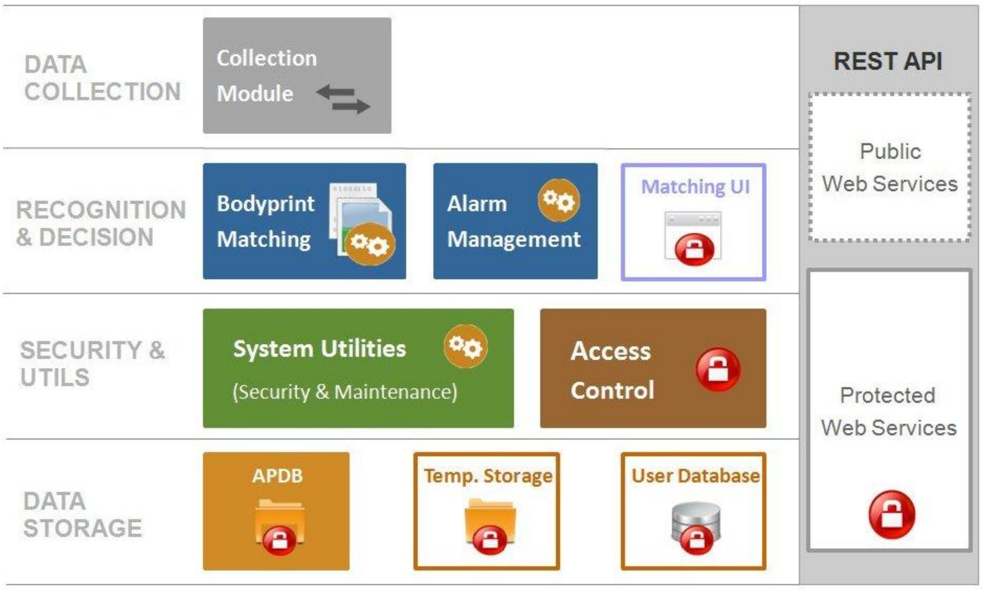


Figure 26: Modules of the Re-Identification Server

Module	Description
Collection Module	This module is used to request new bodyprints to the VPUs installed in the system.
Bodyprint Matching	Program responsible for comparing the bodyprints collected from the VPUs with the bodyprints stored in the APDB.
Results Management	Program in charge of filtering the results of the decision process according to a defined policy, to decide if the match is accepted (authorized person) or rejected (unauthorized person), and generate an alarm if necessary. In case an unauthorized access is detected, an alarm is generated and sent to the RMS to be displayed to the System Operator.
Matching User Interface	Application that allows to configure and run the matching process (Bodyprint Matching), and also the Web Server to enable the REST API.
System Utilities: **Data Compression**	Module allowing to compact data files and folders in a compressed file. It is used to optimize the storage of bodyprints.
System Utilities: **Data Encryption**	Module for the protection of data. It is used to protect the bodyprints and the images stored in the RIS.
System Utilities: **Bodyprint Manager**	This module is responsible for the management of bodyprints. This task covers the search and provision of the bodyprints requested for the matching process, and also the deletion of bodyprints according to the retention period defined.
System Utilities: **System Monitoring**	Module responsible for the maintenance of the system, that checks periodically that the Re-Identification Server works as expected, and that allows to send alarms to the RMS.
Access Control	This module is used for the authentication and authorization of the users that require access to the different resources provided by the RIS. This module is used, for example, to control the access to the different user interfaces.
Authorized People Database	This database contains the bodyprints of the people enrolled in the system, which are protected by encryption. For each person enrolled several bodyprints may be stored in order to improve the results of the matching process. Each bodyprint is stored in the APDB with a key frame that facilitates the validation process, that is also protected.
Temporary Storage	The bodyprints obtained from the VPUs are temporary stored in the system until they are compared with the APDB and the results are validated by the System Operator. Besides, the results of the comparison performed in the RIS are also stored there, including all the parameters obtained in the matching process (e.g.: level of confidence of the results), which will serve to detect incorrect configurations of the re-identification module.
User Database	It contains the system users that are able to access to the different resources of the RIS.
REST API	Set of Web Services providing information obtained and stored in the RIS. • *Public Web Services*: the service providing a description of the Re-Identification Server is public. • *Protected Web Services*: the set of web services for the collection of data stored in the RIS are protected by authentication and authorization mechanisms.

Table 12: Modules of the Re-Identification Server

In the **enrolment** phase, the RIS is just used to store the bodyprints of the authorized people in the APDB.

During the **matching phase** *(detection mode)*, the RIS periodically requests information from the VPUs, collecting any new bodyprint extracted. Then, the RIS compares the new bodyprints with the APDB and decides if the corresponding person is authorized or not. The results of this process and the detection timestamp are copied to the RDB (RMS) to be displayed to the *System Operator* through the *Surveillance User Interface*. After this, the RIS requests from the RMS the results of the validation process, and analyses them in order to detect inaccurate bodyprints. In addition, the results validated as authorized accesses will be marked by the RIS as "ready for deletion". Otherwise, if the access has been validated as unauthorized, the related information will be stored in the system in case it is necessary for law enforcement.

3. **Results Management Server** & **Results Database**

The RMS uses the following modules:

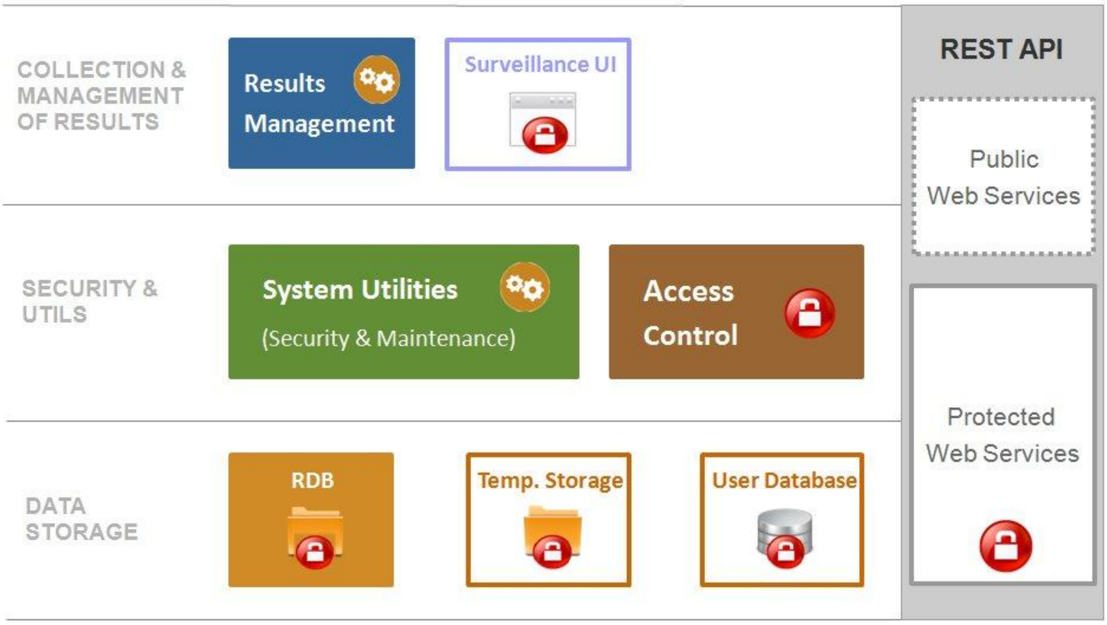


Figure 27: Modules of the Results Management Server

Module	Description
Results Management	Program in charge of processing the information received from the RIS and the VPU that has to be shown to the System Operator.
Surveillance User Interface	Application that allows to review and validate the results of the detection process.
System Utilities: **Data Compression**	Module allowing to compact data files and folders in a compressed file. It is used to optimize the storage of data received from the RIS.
System Utilities: **Data Encryption**	Module for the protection of data. It is used to protect the data received from the RIS.
Access Control	This module is used for the authentication and authorization of the users that require access to the different resources provided by the RMS. This module is used, for example, to control the access to the Surveillance UI.
Results Database	This database contains a history of the accesses detected, and the results of the comparison and the validation processes. For each access detected, this database stores the detection timestamp, a key frame, the

	identifier of the device that captured the event and the results of the validation.
Temporary Storage	The information collected from other devices is stored temporary in the RMS until it is reviewed or no longer required.
User Database	It contains the system users that are able to access to the different resources of the RMS.
REST API	Set of Web Services providing information obtained and stored in the RMS. • *Public Web Services*: the service providing a description of the RMS is public. • *Protected Web Services*: the set of web services for the collection of results and the provision of data stored in the RMS are protected by authentication and authorization mechanisms.

Table 13: Modules of the Results Management Server

As the goal of the RMS is the management and validation of results of the process of detection of unauthorized accesses, it only works during the matching phase *(detection mode)*.

Anytime an access is detected in the area under surveillance, the results of the corresponding recognition process are sent to the RDB by using the REST API of the RMS. That information is displayed through the *Surveillance UI* to the *System Operator*, who has to validate the information. The results of this validation process are stored in the RDB, until they are reviewed by the RIS and marked as "ready for deletion".

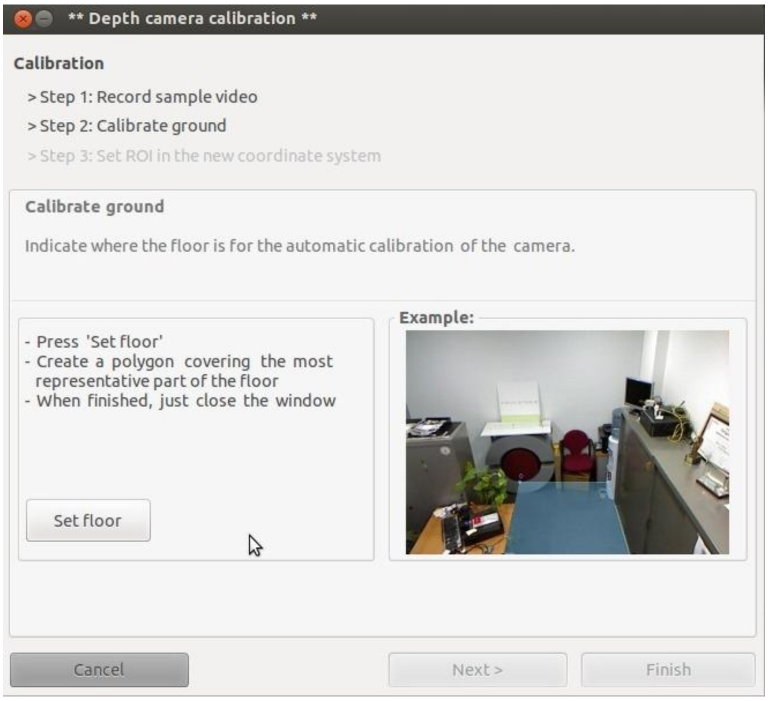
The implementation and use of the different system components are deeply described in the system documentation.

Procedures

The system specification also includes a description of the procedures that have to be carried out to operate and maintain the system. These are the most relevant procedures in terms of privacy and accountability:

- **System configuration:**

  The *System Administrator* is responsible for the system configuration and setup. This task requires to calibrate the depth cameras, to set up the system databases, to create the system users, to configure the VPUs and the RIS to start the extraction and matching of bodyprints at the beginning of the detection period defined, and to launch the RMS so the Surveillance UI can be available for *System Operators*. The different processes to be followed to configure the system are detailed in the system documentation. Training sessions will be scheduled for System Administrators and Operators to help them set up and use the system (artifact A7).



** Depth camera calibration **

Calibration

> Step 1: Record sample video

> Step 2: Calibrate ground

> Step 3: Set ROI in the new coordinate system

Calibrate ground

Indicate where the floor is for the automatic calibration of the camera.

- Press 'Set floor'
- Create a polygon covering the most representative part of the floor
- When finished, just close the window

Figure 28: Calibration User Interface

- **Enrolment process**:

The *System Administrator* is also in charge of the enrolment process, that consists of extracting the bodyprints of the people that are allowed to access the Visual Tools premises during the detection period and storing them in the APDB so the system can be able to decide if a detected person is authorized or not. This process is detailed in section *6.1: Enrolment* (artifact A5).

- **Action plan in case of unauthorized access:**

The procedure to follow in case an unauthorized access is detected, once it is checked by the *System Operator*, is detailed in the system documentation and briefly described in section *6.2: Matching* (artifact A24).

- **Access to the data stored in the system:**

Also in the system documentation, the protocol to follow in case someone requires access to the data stored in the system is explained, for example, in case a *Data Subject* requires access to his personal data (artifact A19), or if the local authorities want to investigate an incident (artifact A24). Any access to the data stored in the system shall be authorized and monitored by the *System Administrator*.

- **Maintenance operations:**

Several operations will be carried out during the operation & maintenance stage of the system to ensure that it works as expected, and that it addresses the identified privacy and accountability requirements. Examples of this type of operations are: the periodic renewal of bodyprints stored in the APDB (artifact A15), the revision of policies and procedures every two years (artifact A17), and also the periodic revision of the need of the system (artifact A22).

To get guidelines for the definition of the different procedures, *System Designers* can used the following tools provided by the SALT Framework:

- *Questionnaire for biometrics*: although the *System Designer* is not in charge of answering the questionnaire, it is recommended that he reviews the different questions, with their related privacy and accountability concerns, and the answers provided by the *System Proposer*, in order to have in mind the most important privacy and accountability requirements.
- *SALT References*: the *System Proposer* should inform the *System Designer* about the most important references that apply to the use case, or at least, those used during the concept phase, just in case the *System Designer* requires to consult details of a certain concern. Besides, the *System Designer* may require to search for other references that can be useful during the design phase. In this case, for example, WP6_REF_7, WP6_REF_8 and WP6_REF_9 resulted very useful for the *System Designer*.
- *Taxonomies*: they were used to understand certain terms included in the SALT References.

4.2.2 Design validation

Once the design is created, the *System Designer* can use the SALT Framework to validate the design according to the associated concerns.

On the one hand, there is a specific tool in the SALT Framework for the validation of designs (PAERIS), that has been already explained in *3.2.3 Design validation tool*. Using this tool together with the UML profile (especially created to work in parallel with the validation tool), the *System Designer* will create an UML model of the system design and will be automatically informed about the concerns not fulfilled, if there are any.

As the design validation tool is still under development, we have not tested yet this functionality. This task will be carried out during the next semester, in which we plan to evaluate the different SALT Framework tools. Anyway, as a reminder, Figure 29 shows the most relevant elements that can be used for the creation of the UML model of a biometric system.

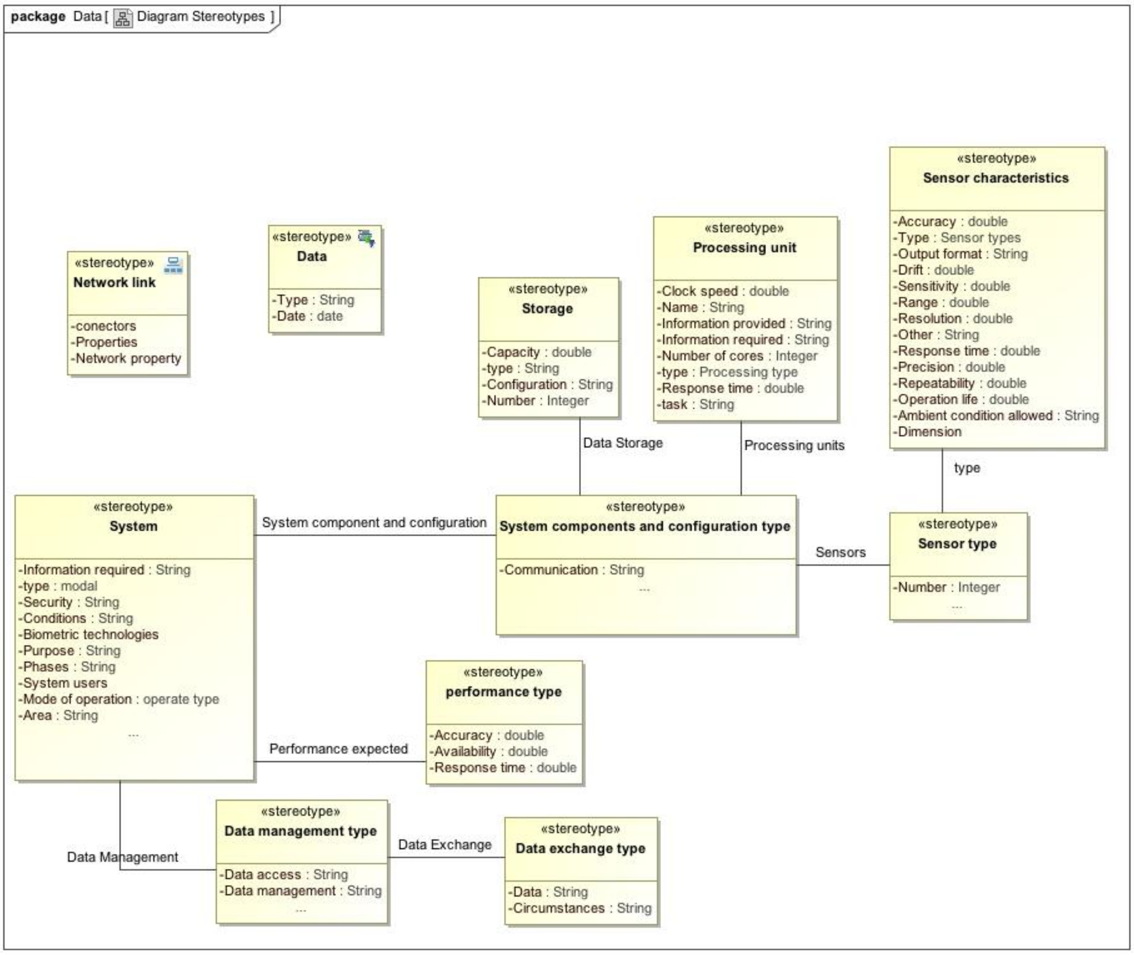


Figure 29: Stereotype Diagram for biometric systems

On the other hand, it is possible to assess the privacy risks associated to several design decisions using the *Questionnaire for biometrics*, that at least points to the most relevant privacy and accountability concerns related to biometric systems. This assessment should be carried out by a person with certain legal and technical expertise, to apply correctly the different recommendations and evaluate their enforceability and adequacy for the use case.

In this particular use case presented in WP6, the questionnaire was just reviewed at the end of the stage to check that all the technical questions had been taken into account (e.g. data retention periods, erasure mechanisms, different risks associated to the bodyprints, etc.).

4.2.3 Results of the design stage

Following the SALT process defined, and using all the mentioned tools provided by the SALT methodology, at the end of the design stage the following documents are obtained:

- **Report with the results of the questionnaire**, that contains the responses provided and the reasoning followed to define the system purpose and evaluate its legitimacy and proportionality. Also a risk assessment of the system drafted will be provided.

This report is still under development, therefore we cannot provide an example yet, but this work will be done during the next semester.

- **Report with the results of the design validation**, that is produced at the end of the design validation process using the corresponding SALT tool, and which will highlight the concerns not fulfilled based in the existing OCL rules as explained in *3.2.3 Design validation tool*. We are still considering to include other type of guidelines and recommendations in this report extracted from the SALT references that can be applied to a certain system.

This report is also under development, therefore we cannot provide an example yet, but this work will be done during the next semester.

- **UML model of the system design**, that is also an output of the design validation tool.

- **System specification**, containing technical details about how to implement the system and also the definition of the different operational procedures (e.g. *Procedures*).

5 Use Case II: Deploying the system

This use case is aimed at demonstrating how the SALT Framework can also be used for the implementation of the system designed considering privacy and accountability during all the process. It covers the stages of development and deployment.

At the end of this phase, the system designed is installed in the *Data Controller's* facilities (Visual Tools premises) and it is ready to be used for the detection of unauthorized accesses.

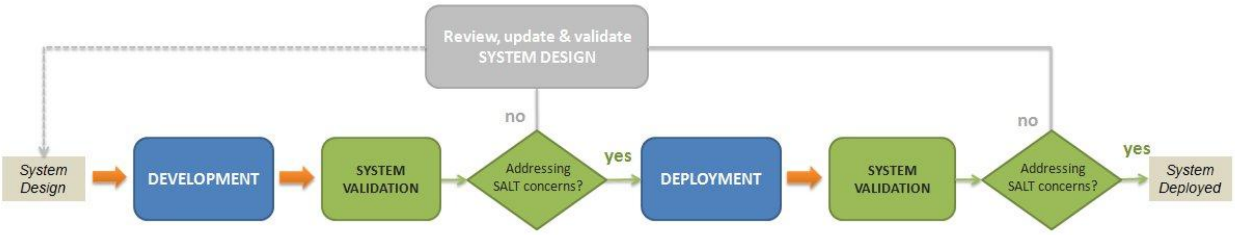


Figure 30: Stages of the system lifecycle covered by Use Case II

Because of resource reasons, the system has not been fully developed yet. During the last semester we have also been working on refining and improving the SALT Framework Tools (questionnaires, references, etc.), which made us re-evaluate the use case in terms of privacy and accountability, and new concerns were raised which made necessary to slightly modify the system design.

By now, the components developed have only been set up in the Visual Tools' lab for testing purposes. We plan to install a first prototype of the system in the Visual Tools headquarters in Madrid during the next semester, with at least the minimal functionalities that let us evaluate the system.

5.1 Development

The development stage starts with the specification of the system, that should take into consideration privacy and accountability if it had been elaborated following the SALT approach.

The *Surveillance Service Provider* entrusts the task of implementing the system according to the given specification to the *System Developer*, who can be a single person or a team. In this case, the role of the *System Developer* is taken by the R&D Department of Visual Tools.

As a result of this stage, a system is developed meeting the stakeholder's requirements and addressing the main privacy and accountability concerns identified in the previous stages.

Tasks performed during the development stage

These are the main activities carried out during this stage:

- *Build the system*: the different system components are constructed according to the design specification. This work includes the programming of the modules and interfaces composing each system component (VPU, RIS & RMS), and the creation of the system databases (RDB, APDB and User databases).

- *Unit testing*: the different modules and components are first tested independently from the rest of the system, to validate that they work as expected.
- *Integration of components and system testing*: all the modules are tested together, to check the functionality, interoperability and performance of the system.
- *Revisions of the design of the system*: in some cases, to correct bugs or improve the system functionalities it is necessary to review the design of the system.

Decisions made at the development stage

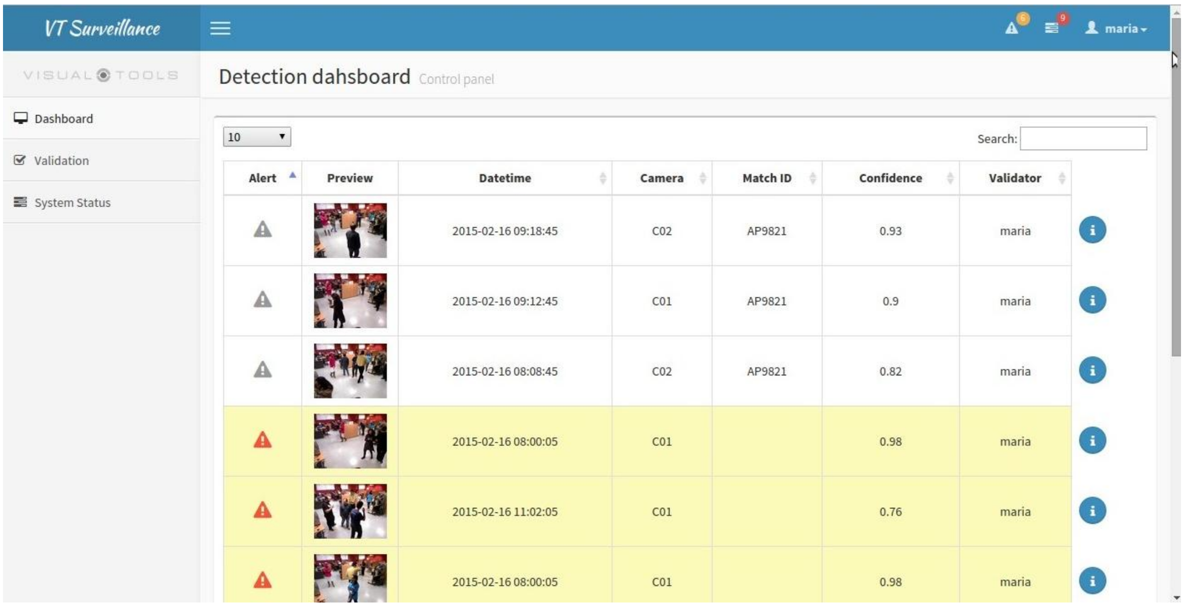
The development phase is one of the most critical stages, as the results of this phase affects profoundly the operation & maintenance tasks of the system.

In terms of programming, a well written code reduces the effort to be spent in testing and maintenance. It is also important to point out, that an error detected during an early stage is easier to be solved and at a lower cost. Thus, it is important during the development stage to focus on developing system components and modules that are easy to test and maintain. For the biometrics system presented in WP6, the modular design chosen for the different system components provides more flexibility for developers, and facilitates the system re-design and also its maintenance in the long term.

Although the main technologies to be used in the system implementation are selected during the design stage, some of the technological decisions can be taken by the *System Developer*, such as the programming language to code the components or the libraries or frameworks to use. Besides, after the different tests carried out during this stage, the system may need to be redesigned, therefore the *System Developer* and the *System Designer* should work together (if they are not actually in the same team).

In the case of the systems developed by Visual Tools, there are normally many iterations between the design and development stages. The company prefers to follow customer-driven development methodologies, trying to involve end users in the development process whenever possible. This allows to test the system usability at an early-stage and to check if the solution produced solves adequately the problem proposed and it is a product that the customers will be willing to pay for.

In this case, we tested the initial version of the Web User Interface showing the alarms with the employee from Visual Tools that will be responsible for administrating the system, who has also experience as an operator.



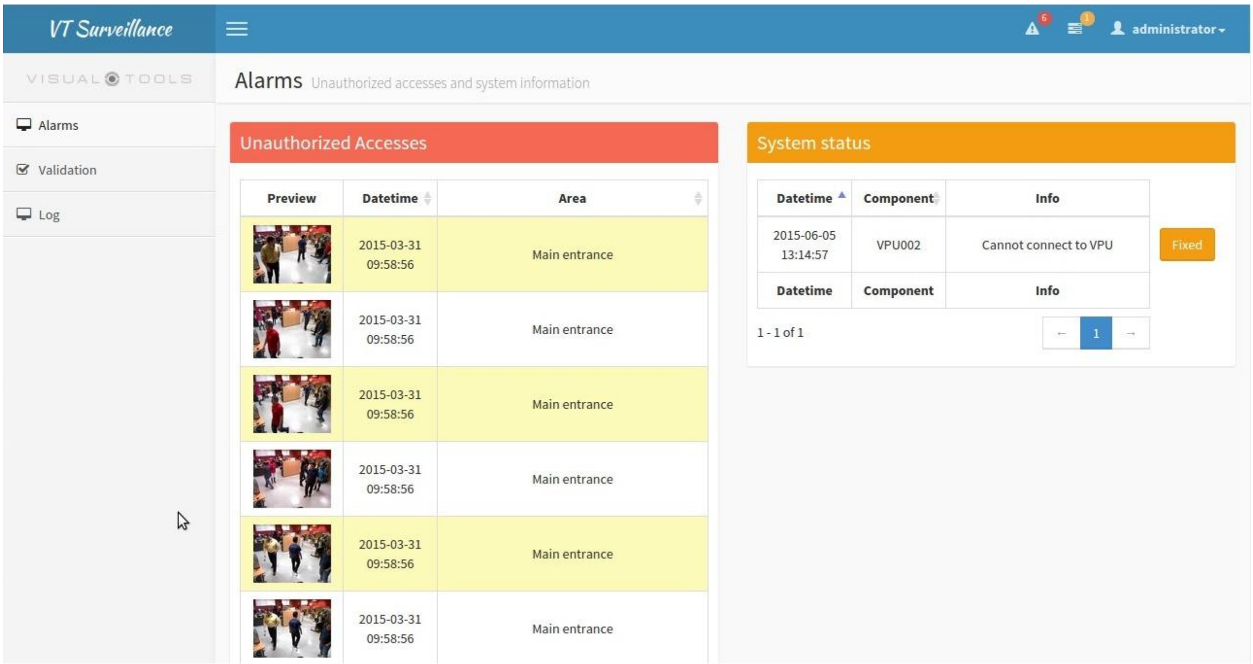
Detection dahsboard Control panel

Alert	Preview	Datetime	Camera	Match ID	Confidence	Validator	
⚠		2015-02-16 09:18:45	C02	AP9821	0.93	maria	i
⚠		2015-02-16 09:12:45	C01	AP9821	0.9	maria	i
⚠		2015-02-16 08:08:45	C02	AP9821	0.82	maria	i
⚠		2015-02-16 08:00:05	C01		0.98	maria	i
⚠		2015-02-16 11:02:05	C01		0.76	maria	i
⚠		2015-02-16 08:00:05	C01		0.98	maria	i

Figure 31: Initial version of the Web User Interface

This initial version displayed in the main panel a list with all the detection events, and a lot of information related to the results of the comparison process. Taking the feedback of the end user into account, we decided to simplify the tool: on the one hand, we cannot expect *System Operators* to understand the comparison process, therefore the parameters obtained from the matching operations are stored in the system (RIS) but not shown in the Web User Interface; on the other hand, normally System Operators work in a control centre and are in charge of monitoring several places at the same time, and we cannot expect them to be looking for the interface during long periods of time, thus they should only be warned in case of unauthorized access.

Taking all this into account, we developed a new version of the User Interface that shows in the main panel just the alarms produced by an unauthorized access or an error in the system. It is possible to see a log with all events in a secondary panel, but the lust only includes the datetime and area where the event was detected, and the ID of the event/bodyprint in case it is necessary to look for more information (RIS).



Alarms Unauthorized accesses and system information

Unauthorized Accesses

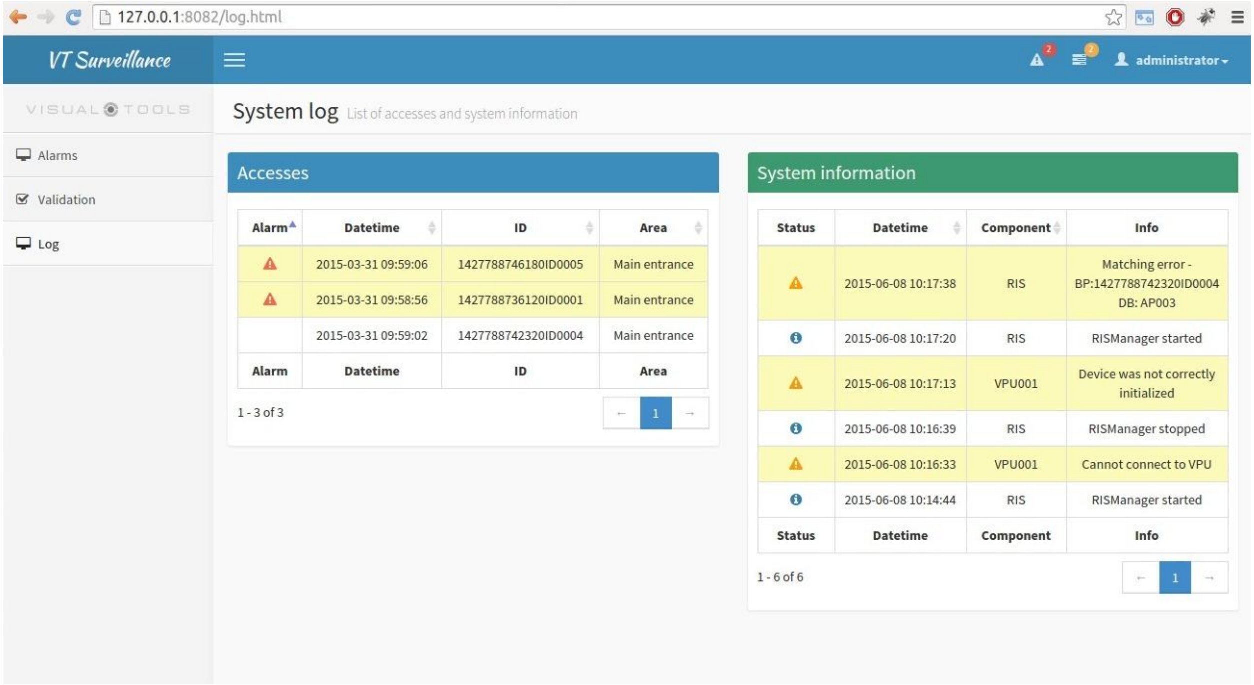
Preview	Datetime	Area
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance

System status

Datetime	Component	Info
2015-06-05 13:14:57	VPU002	Cannot connect to VPU
Datetime	Component	Info

1 - 1 of 1

Figure 32: Last version of the Web User Interface - Main panel



System log List of accesses and system information

Accesses

Alarm	Datetime	ID	Area
⚠	2015-03-31 09:59:06	1427788746180ID0005	Main entrance
⚠	2015-03-31 09:58:56	1427788736120ID0001	Main entrance
	2015-03-31 09:59:02	1427788742320ID0004	Main entrance
Alarm	Datetime	ID	Area

1 - 3 of 3

System information

Status	Datetime	Component	Info
⚠	2015-06-08 10:17:38	RIS	Matching error - BP:1427788742320ID0004 DB: AP003
ℹ	2015-06-08 10:17:20	RIS	RISManager started
⚠	2015-06-08 10:17:13	VPU001	Device was not correctly initialized
ℹ	2015-06-08 10:16:39	RIS	RISManager stopped
⚠	2015-06-08 10:16:33	VPU001	Cannot connect to VPU
ℹ	2015-06-08 10:14:44	RIS	RISManager started
Status	Datetime	Component	Info

1 - 6 of 6

Figure 33: Last version of the Web User Interface - Log panel

Use of the SALT Framework during the development stage

The references stored in the SALT Repository can also provide guidelines for *System Developers*, for example, recommendations for the evaluation of the system once developed, the technologies to use, or concerns related to the integration of components (e.g. protection of data communications).

For this use case, the System Developer consulted the same references used by the System Designer, to be aware about the main privacy and accountability concerns (WP6_REF_7, WP6_REF_8 and WP6_REF_9).

Requirements at the development stage

It is essential at the end of this stage to verify that the system addresses all the stakeholder's requirements, as well as the different privacy and accountability concerns identified during the concept and design stages.

In Table 3 it is possible to see the requirements that can be checked at the end of the development stage in the case of the biometrics system developed. The technical requirements have been extracted from the list initially presented in D6.1, while the concerns about privacy and accountability are extracted from the list of Table 1. Due to the mentioned resource limitations, only a few of the technical requirements have not been fulfilled yet:

Id	Fulfilled	Technical requirements - Details
TR_2 - TR_15	*Yes*	• The system has been configured as planned • The alarm management has been separated from the matching process • The communications between the different components is protected by encryption • The personal data and the biometric templates are stored encrypted • Access control mechanisms have been implemented to access to the different system resources • Logs are used to control the unattended operations
Id	**Fulfilled**	**Operational requirements - Details**
OR_1 - OR_4, OR_8, OR_10, OR_12, OR_16-18, OR_23	*Yes*	• The system is able to perform all the operations listed • The SA can manage the system users from the administration panel of the different components • The enrolment process can be initiated manually and only by the SA • The SA can have access and modify or delete the data stored in the system • The SO is able to receive alarms of unauthorized accesses and validate them from the Web UI located in the RMS • Monitoring tasks are performed automatically to ensure that the system works as expected, or at least to warn the SO in case there is an error
OR_11	*No*	• By now, it is not possible to configure the detection period in which the system shall work: the SA has to start/stop the system manually. This requirement is left as a future improvement of the system.
Id	**Fulfilled**	**Functional requirements - Details**
FR_1 - FR_5, FR_8-FR_11, FR_13, FR_6, FR_7, FR_12-18, FR_19-20	*Yes*	• The system includes all the functionalities required for the extraction (VPU) and comparison (RIS) of bodyprints, and also to generate alarms and show them to System Operators (RMS) • Thanks to the validation of results, it is possible to detect and discard inaccurate templates: a warning is generated each time an error is detected in the matching process. The SO then is able to review it and request the update of a bodyprint to the SA. • The system stores the datetime and an image anytime a person is detected • The system stores information of the system users (User DB of each component) • The system allows users with administration permissions to configure the different components, and to initiate manually the enrolment process • The system performs several maintenance operations automatically, for

		example, to remove certain data after a defined period of time
FR_12	*No*	• By now, the system has to be started and stopped manually. It does not accept yet the configuration of the detection period.
Id		**Environment requirements - Details**
ER_1- ER_6	*Yes*	Tests have been performed in the Visual Tools' lab in an environment similar to the Visual Tools headquarters in Madrid, and the system is able to work as expected.

Table 14: Summary of the technical requirements fulfilled at the development stage

5.2 Deployment

Once the system is developed and tested, the next step consists of setting up the system at the *Data Controller*'s facilities (Visual Tools) and get it ready to be used for the detection of unauthorized accesses.

In this phase, the main actors are the *Installer* and the *System Administrator*.

Tasks performed during the deployment stage

These are some of the activities that will be carried out for the deployment of the system:

- *Installation of hardware and software at the stakeholder facilities*: at least the RIS, the RMS and two VPUs will be installed at the Visual Tools premises covering the main transit areas. The *Installer* is responsible for this task.

  During the installation of the system, it is important to fulfill REQ_VSS_4, that refers to the location of the cameras, and also REQ_SOC_* in which it is recommended to provide "surveillance breaks" to reduce the intrusive impact of the system. Artifact A13 is also related to this task and shall be implemented.

  Once finished, for accountability purposes, the *Installer* shall sign a document including details of the installation conducted (artifact A23).

- *User training* (artifact A7): first, the *Installer* shall train the *System Administrator* so he can manage all the system properly; after that, the *Installer* or the *System Administrator* shall provide guidance to *System Operators* so they can use the Surveillance UI and know the procedures defined in case of intrusion.

  After this training, system users should be clear about their responsibilities and the different operational and organizational procedures (e.g. what to do in case there is a system failure, what to do in case of intrusion, what to do in case a DS requests access to his personal data...).

- *Fulfillment of legal requirements prior to the use of the system*, that in this case are mainly covered by requirements REQ_VSS_*, such as the inscription of the system in the General Register (artifact A3), the installation of informative signs in the areas under surveillance (artifact A4) or the elaboration of the different documents (artifacts A4 and A11). The *System Administrator* is registered as responsible for the system, and thus is in charge of verifying that these tasks are carried out.

- *Configuration of the system for the detection of unauthorized accesses*, that includes the deployment of the system databases, the creation of the system users and the definition of the detection period. Normally, the System Administrator performs these tasks.

Documents generated at the deployment stage

Normally, two technical documents are elaborated for any system:

- *Documentation for System Operators* [A11], explaining how to use the Surveillance UI, the procedures to follow in case of system failure or in case of unauthorized access, and also how to handle the main errors that may occur during the operation of the system.
- *System documentation* [A11], that contains details of the system design, system requirements, how to configure the system, security mechanisms implemented, etc. This document helps to understand how the system works and has been implemented so they can be easily maintained or updated with new functionalities.

Besides, as extracted from the different legal requirements, this other documentation should be prepared:

- Privacy Management Program (internal privacy policy) [A11]
- Public Privacy Policy (for people to be enrolled in the system) [A2]
- Public Privacy Policy summarized (handout for any DS requesting information) [A2]
- The Security Document, that is mandatory according to the Spanish legislation, and that shall include all the technical and organizational measures implemented to guarantee the security of the data processed and stored by the system [6], as well as the obligations of the personnel involved in data processing.

> We are still working on the first draft of the system documentation, that contains all the technical information required to use and maintain the system, and also defines the security obligations of the different system users *(Security Document)*.
>
> Regarding the privacy policies, due to resource reasons, in the last semester of the project we just plan to elaborate a draft with the main contents and a handout to be provided to any DS requesting the information.

Use of the SALT Framework during the deployment stage

Again, some of the references stored in the SALT Repository may include concerns that have to be applied during this stage.

For this use case, both the *Installer* and the *System Administrator* took into account references WP6_REF_3, WP6_REF_4, WP6_REF_5 and WP6_REF_6 that inform about the legal issues required by the Spanish legislation.

Requirements at the deployment stage

The following table summarizes the main requirements that should be checked at the end of the deployment stage:

Id	Technical requirement	Status
TR_1	• The cameras used shall cover the main transit areas of the office	*To be checked after deployment*
Id	**Operational requirement**	**Stage**
OR_5-6, OR_9	• The system documentation under development will provide information about how to configure and use the system, and also the different procedures for data access or to maintain the system	*To be checked after deployment*
OR_7-8	• The SA will be trained properly to manage the system and its users	
Id	**Environment requirement**	**Stage**
ER_5-6	• Each depth camera shall cover a maximum area of 5 x 3 meters • Each depth camera shall be placed at a minimum of 0.8 meters of the objects	*To be checked after deployment*

Table 15: Summary of the technical requirements to be fulfilled at the deployment stage

5.3 Auditing the system

According to the Spanish legislation, privacy audits have to be executed every two years for those systems that have to implement high or medium level security measures [6], or any time a substantial modification of the system is made, to check the adequacy and efficiency of the security measures implemented.

Although that does not apply to the WP6 use case *(low level security* [6]*)*, we want to describe in this section the steps to follow in case the *Spanish Data Protection Agency* requires the verification of the compliance of the system with the current regulations, to show how the different SALT resources can be used in this process.

The Spanish Data Protection Agency (AEPD), has elaborated a document detailing how an audit of this type works, and the procedure that should be followed by the auditors [13].

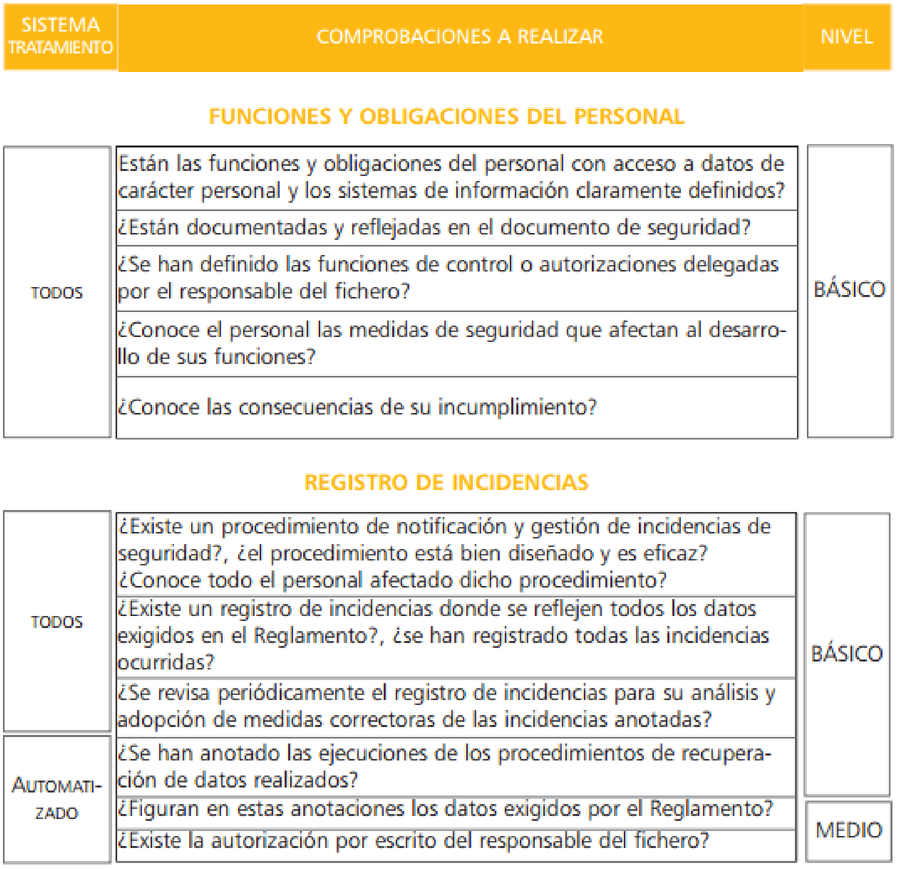
The *Data Protection Officer* (DPO) is in charge of auditing the system in order to check if the security measures indicated in Title VIII of the Royal Decree 1720/2007 [6] have been implemented correctly.

These are the main steps to follow by the DPO:

- Determine the extent of the audit, establishing which are the files that should be audited, the data processing systems, procedures, etc.;
- Determine the resources needed to carry out the audit;
- Collection of data:
    - List of files, structure and contents
    - Security policies and procedures (register of incidents, system logs, backups, etc.)
    - Security document and previous audits
    - System documentation

- List of system users, authorized accesses and their responsibilities
- Inventory of the existing media, and the recording of any entry and exit of media
- Data access logs and reports of their periodic revision
- Interviews with system users, and also with any person responsible for the system
- Visual inspection

- Evaluation of the evidences collected, for which the Spanish Data Protection Agency provides a set of verifications that have to be reviewed to check the compliance with the legislation. This appears in the documentation as a list of questions grouped by the security level to be applied, that should be answered at the end of the auditing process. Figure 34 shows an example of the mentioned verifications (in the original language).



SISTEMA TRATAMIENTO	COMPROBACIONES A REALIZAR	NIVEL
	FUNCIONES Y OBLIGACIONES DEL PERSONAL	
TODOS	Están las funciones y obligaciones del personal con acceso a datos de carácter personal y los sistemas de información claramente definidos?	BÁSICO
	¿Están documentadas y reflejadas en el documento de seguridad?	
	¿Se han definido las funciones de control o autorizaciones delegadas por el responsable del fichero?	
	¿Conoce el personal las medidas de seguridad que afectan al desarrollo de sus funciones?	
	¿Conoce las consecuencias de su incumplimiento?	
	REGISTRO DE INCIDENCIAS	
TODOS	¿Existe un procedimiento de notificación y gestión de incidencias de seguridad?, ¿el procedimiento está bien diseñado y es eficaz? ¿Conoce todo el personal afectado dicho procedimiento?	BÁSICO
	¿Existe un registro de incidencias donde se reflejen todos los datos exigidos en el Reglamento?, ¿se han registrado todas las incidencias ocurridas?	
	¿Se revisa periódicamente el registro de incidencias para su análisis y adopción de medidas correctoras de las incidencias anotadas?	
AUTOMATIZADO	¿Se han anotado las ejecuciones de los procedimientos de recuperación de datos realizados?	
	¿Figuran en estas anotaciones los datos exigidos por el Reglamento?	MEDIO
	¿Existe la autorización por escrito del responsable del fichero?	

Figure 34: Example of verifications to carry out in a privacy audit

During all this process, the *System Administrator* and also the *Data Controller* can assist the DPO in the collection of all the information or resources required, monitoring and registering any access to the data stored in the system.

Besides, *System Operators* or any other technical person involved in the design, development or deployment of the system, may be contacted by the DPO for an interview.

If the system has been developed following the SALT process and using the SALT Tools, the documentation required by the DPO, the system logs and traces of any data access should be available and adequate to the current legislation. Furthermore, at this point the *Data Controller* can provide the following reports to the DPO, in order to facilitate the assessment of the whole system in terms of privacy and accountability:

- **Report with the results of the questionnaire** that, as explained before, contains the results of the initial privacy risk assessment of the concept of the system.
- **Report with the results of the design validation**, indicating some concerns that apply to the system designed and that have (probably) been taken into consideration.
- **List of SALT References and taxonomies used during the different stages of the system lifecycle**, and that may support some of the decisions made for the design, development or deployment of the system.

6 Use Case III: Using the system

This use case serves to demonstrate how the system is used once it is operational, and particularly how the surveillance service is provided according to the SALT guidelines.

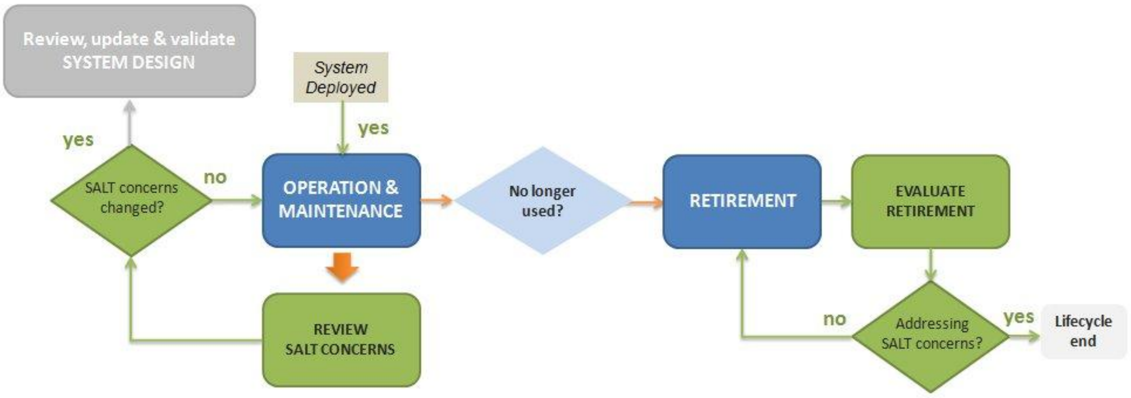


Figure 35: Stages of the system lifecycle covered by Use Case III

6.1 Enrolment

Once the system is properly configured for the detection of unauthorized accesses at the defined period, it is time to enroll in the system the people that are allowed to be at the office during the mentioned period, who are the maintenance employees in this case. The *System Administrator* is responsible for this task.

It is recommended that *System Administrator* is aware during all the enrolment process about the related concerns on privacy and accountability, thus, if needed, the *System Administrator* can consult the reports provided by the SALT Tools in the previous stages, and also the SALT References used by the *System Proposer* and the *System Designer*. Besides, the SALT Repository could contain specific references about good practices on the enrolment process.

For this use case, in order to be transparent and address the identified concerns on privacy and accountability, the *Data Subject* to be enrolled in the system is involved in the enrolment procedure, that is comprised of the following tasks:

- Inform the people to be enrolled in the system (from now on: *Authorized Person*) about the existence of the system, its purpose, how the data is collected and processed, and their rights over their personal data.
- Enroll the *Authorized Persons* in the system, that in this case consists of extracting their bodyprints and storing them in the *Authorized People Database* (APDB).

Below, the tasks are detailed.

6.1.1 Information of Data Subjects

Although the consent of *Data Subjects* is not mandatory in this case, as the *Authorized Persons* are employees of Visual Tools and therefore the consent cannot be considered "freely given", it is a good practice in terms of privacy and accountability to inform adequately the person who is going to be enrolled in the system. This concern is pointed out by the legal references that mention the existing concerns about transparency in the processing of personal data, particularly by WP6_REF_8, that is specific to biometric systems. This issue is also addressed by the questionnaire for biometrics, which states that "*any biometric system that would not require the active participation of the individual during the enrolment phase should be avoided*". These two resources, if used by the *System Proposer* and the *System Designer* during the concept and design stages, will let them identify the need to involve *Data Subjects* in the enrolment so they can take it into consideration while drafting the system.

As mentioned in D6.2, to address this concern about transparency in the enrolment process (mainly by REQ_QUE_5, REQ_ACC_18-20 and REQ_LEG_3), an information notice is going to be elaborated including the following information:

- Purpose of the collection and processing of their personal data (REQ_QUE_1)
- Area covered by the surveillance systems and availability of surveillance breaks (*REQ_VSS_4,* REQ_SOC_*)
- Description of the matching procedure (*REQ_QUE_6*)
- The period for which the personal data will be stored (*REQ_QUE_14*)
- Explanation of their rights over their personal data (access, rectification, erasure and repudiation) (*REQ_LEG_8*)
- Security measures implemented for the protection of data (*REQ_QUE_13, REQ_VSS_6*)

This notice will be provided to the *Authorized Persons*, and the *Data Controller* (Visual Tools) will also arrange an informative session to explain them directly the contents of the notice and to clarify any doubt about it.

Artifacts used (prior to enrolment)	
A2	Information notice for Authorized Persons
A25	Informative session to explain the details of the system and clarify doubts

Table 16: Artifacts used before enrolling the Authorized Persons

6.1.2 Enrolment of Data Subjects

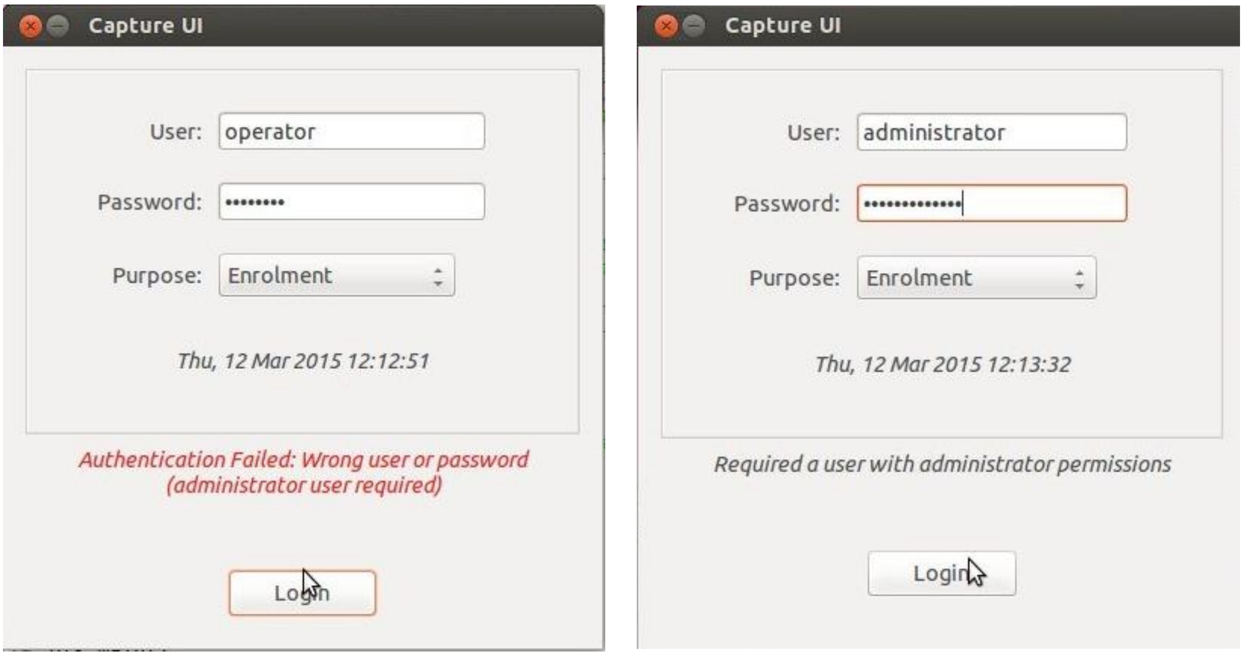
The enrolment phase is at the core of the biometric system. During this phase biometric data of a particular data subject is captured and aligned with an identity. Requirements REQ_ACC_8-12 are related to this phase of the enrolment process.

In this case the enrolment is performed offline, which means that the collection of data from *Data Subjects* and the extraction of biometric templates from that data are carried out at different moments. The whole process is managed by the *System Administrator* and requires the collaboration of the *Data Subjects* for the first part.

These are the steps to follow for the enrolment of *Authorized Persons* in the biometric system implemented:

1. **Collection of data:**

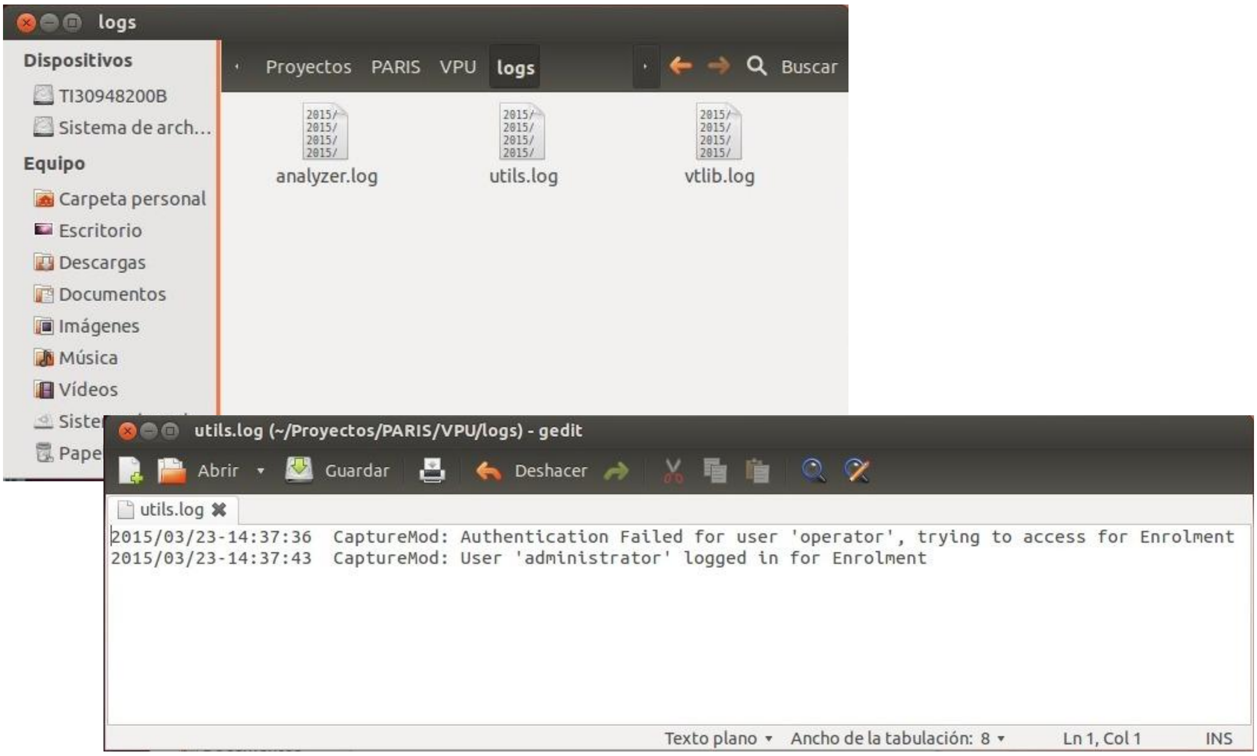
- The *System Administrator* uses the Capture User Interface of one of the VPUs to record a video of the *Data Subject* to be enrolled. Only the system users with "administrator" profile can have access to this interface. For logging in it is also necessary to indicate the purpose of data collection.
- The *Data Subject* is asked to walk crossing the area monitored by the VPU in different ways to capture the whole body from different angles (e.g. from the front and side) wearing the working clothes. One minute of video is normally sufficient, the most important thing recording the video is to capture several views of the person to be enrolled.
- The video collected is automatically encrypted by the Capture User Interface and stored in the VPU.



User: operator
Password: ••••••••
Purpose: Enrolment
Thu, 12 Mar 2015 12:12:51
Authentication Failed: Wrong user or password (administrator user required)

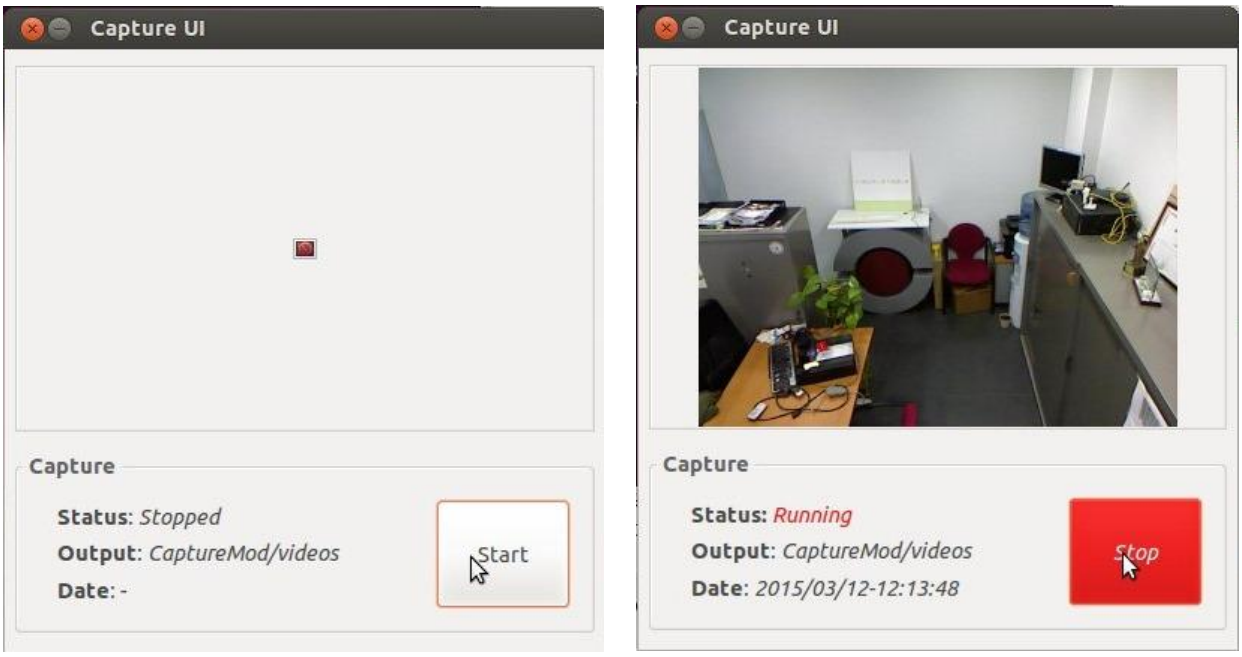
User: administrator
Password: •••••••••••••
Purpose: Enrolment
Thu, 12 Mar 2015 12:13:32
Required a user with administrator permissions

Figure 36: Capture User Interface - Log in with different profiles



```
2015/03/23-14:37:36  CaptureMod: Authentication Failed for user 'operator', trying to access for Enrolment
2015/03/23-14:37:43  CaptureMod: User 'administrator' logged in for Enrolment
```

Figure 37: Capture User Interface - extract of the log (utils.log)



Status: *Stopped*
Output: *CaptureMod/videos*
Date: -

Status: *Running*
Output: *CaptureMod/videos*
Date: *2015/03/12-12:13:48*

Figure 38: Capture User Interface - Recording video sequence

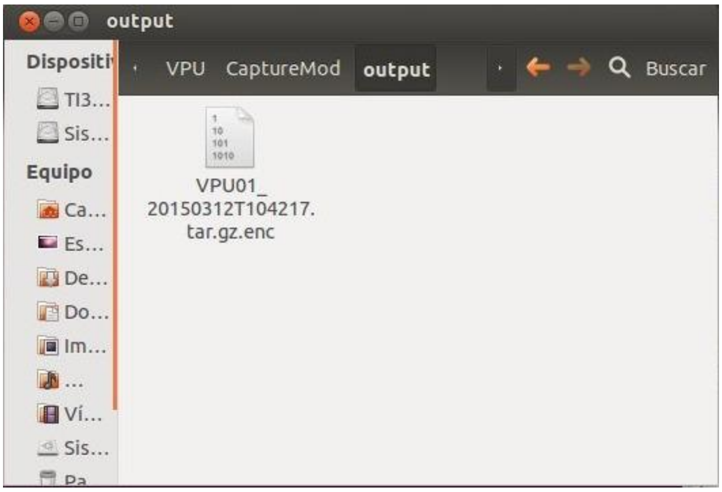
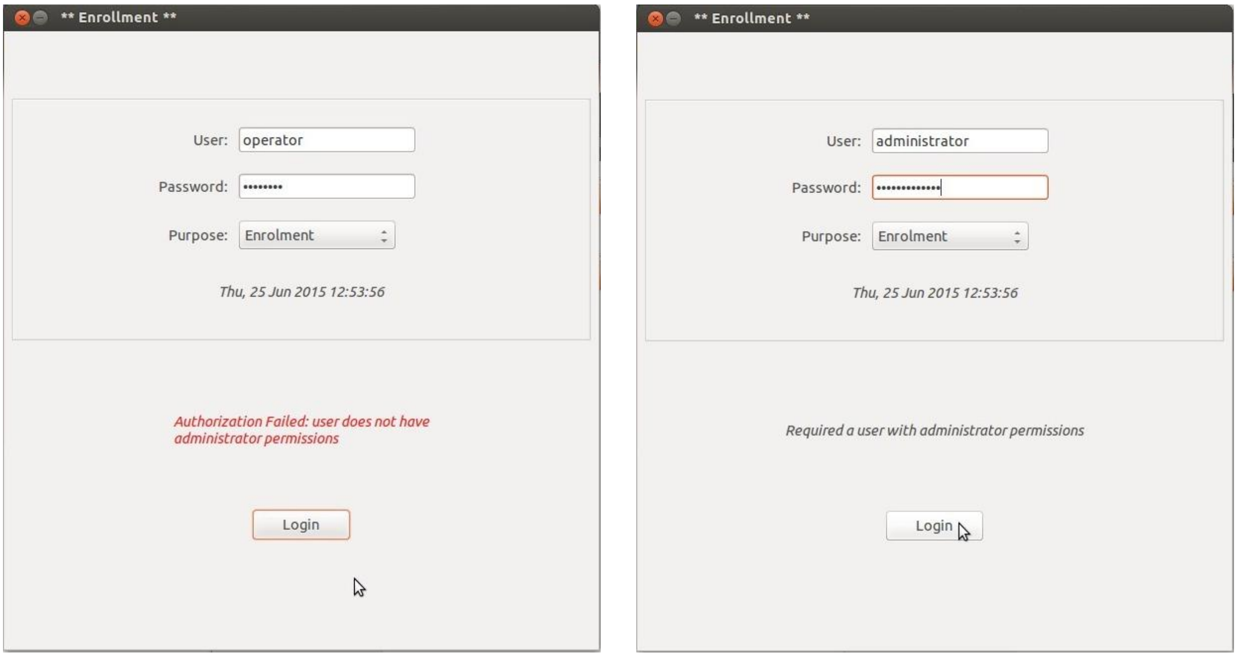


Figure 39: Capture User Interface - File generated

Extraction and storage of bodyprints:

- The *System Administrator* then uses the Enrolment User Interface in order to extract the bodyprints from the video collected. Again, it is required to log in with "administrator" profile and to indicate the purpose of the use of the Enrolment UI.
- Using the Enrolment UI, the *System Administrator* loads and processes the encrypted video sequence generated in the previous phase, obtaining one or several bodyprints.
- Then, it is possible to review the bodyprints generated and filter only those belonging to the person to be enrolled (in case another person appears in the sequence).



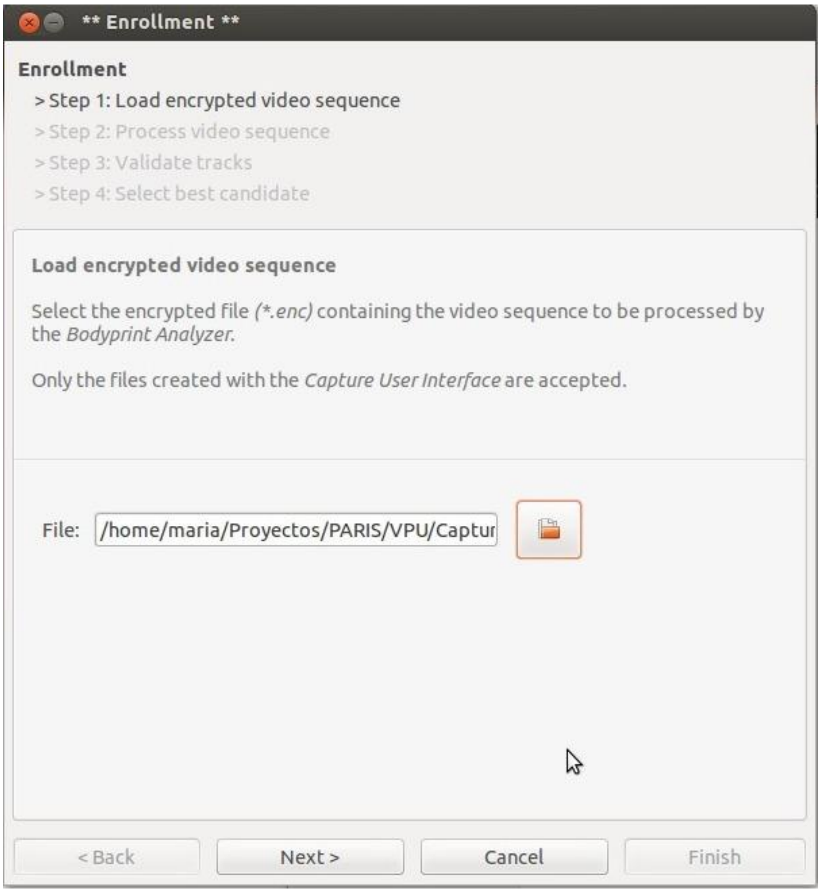
User: operator
Password: ••••••••
Purpose: Enrolment
Thu, 25 Jun 2015 12:53:56

Authorization Failed: user does not have administrator permissions

User: administrator
Password: ••••••••••••••
Purpose: Enrolment
Thu, 25 Jun 2015 12:53:56

Required a user with administrator permissions

Figure 40: Enrolment User Interface - Log in with different profiles



** Enrollment **

Enrollment

> Step 1: Load encrypted video sequence

> Step 2: Process video sequence

> Step 3: Validate tracks

> Step 4: Select best candidate

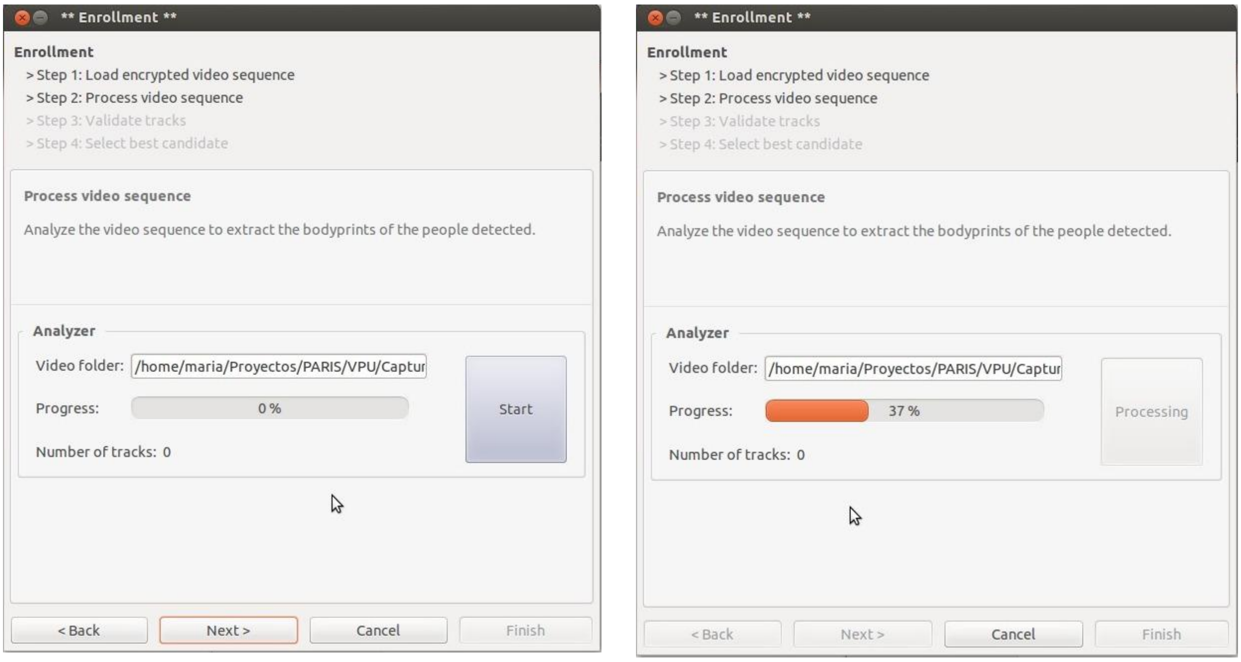
Load encrypted video sequence

Select the encrypted file *(*.enc)* containing the video sequence to be processed by the *Bodyprint Analyzer.*

Only the files created with the *Capture User Interface* are accepted.

File: /home/maria/Proyectos/PARIS/VPU/Captur

Figure 41: Enrolment User Interface - Loading a video sequence



** Enrollment **

Enrollment

> Step 1: Load encrypted video sequence

> Step 2: Process video sequence

> Step 3: Validate tracks

> Step 4: Select best candidate

Process video sequence

Analyze the video sequence to extract the bodyprints of the people detected.

Analyzer

Video folder: /home/maria/Proyectos/PARIS/VPU/Captur

Progress: 0 %

Number of tracks: 0

** Enrollment **

Enrollment

> Step 1: Load encrypted video sequence

> Step 2: Process video sequence

> Step 3: Validate tracks

> Step 4: Select best candidate

Process video sequence

Analyze the video sequence to extract the bodyprints of the people detected.

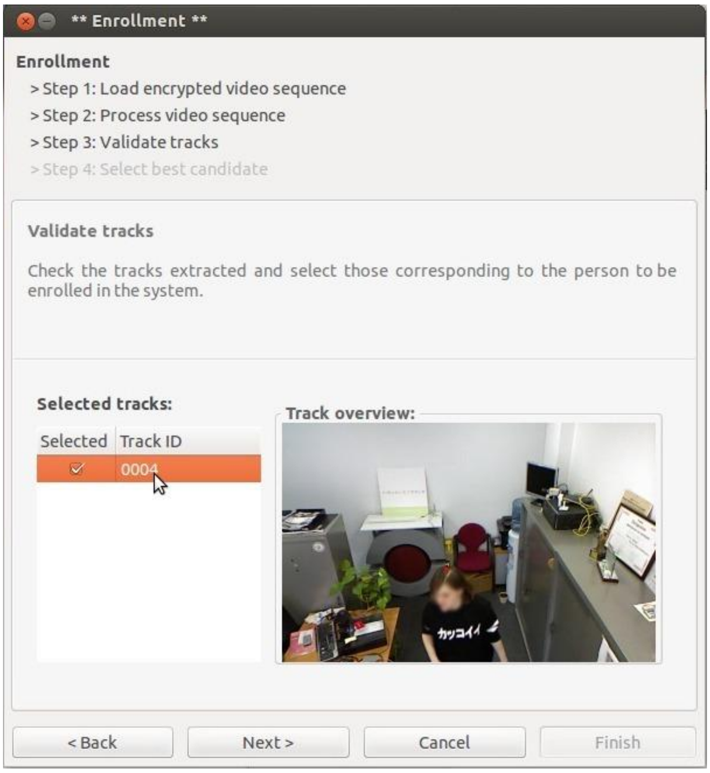
Analyzer

Video folder: /home/maria/Proyectos/PARIS/VPU/Captur

Progress: 37 %

Number of tracks: 0

Figure 42: Enrolment User Interface - Processing video sequence



** Enrollment **

Enrollment

> Step 1: Load encrypted video sequence

> Step 2: Process video sequence

> Step 3: Validate tracks

> Step 4: Select best candidate

Validate tracks

Check the tracks extracted and select those corresponding to the person to be enrolled in the system.

Selected tracks:

Selected	Track ID
☑	0004

Track overview:

Figure 43: Enrolment User Interface - Validation of bodyprints

- Finally, the *System Administrator* selects the most adequate bodyprints to be included in the APDB. For this, the initial idea was to implement a function in this Enrolment User Interface that compares all the bodyprints generated and allows to group those providing better results, but this capability has not been developed yet, so, by now, the SA has to select manually the best candidates for the APDB. In case of doubt, all the bodyprints belonging to the Authorized Person can be included in the APDB.
- Once selected, the SA copies the selected bodyprints to the APDB located in the RIS, using for this a portable storage device. After this, the SA is responsible for deleting the bodyprints from the VPU and also from the portable storage device.
- There is no need to involve the Data Subject in this part of the process.

Moreover, the Data Controller has defined the following activities in regards to the enrolment of Data Subjects:

- The enrolment will be repeated every 6 months and anytime an error is detected in one of the bodyprints of the APDB.
- Didactic sessions about how to enroll a DS and how to protect the data collected will be carried out to train the *System Administrator* before starting the operation & maintenance stage.

Artifacts used	
A5	Definition of a procedure for enrolment in which the collaboration of the data subject is required
A7	Training sessions for the System Administrator
A8-A10	Use of logs to trace the main operations performed by the Capture UI and the Enrolment UI
A12	Encryption of videos and bodyprints
A21	Access control mechanisms for the User Interfaces

Table 17: Artifacts for the enrolment of Data Subjects

At the end of the enrolment phase, the APDB contains the bodyprints of the Authorized Persons and thus, the system is ready to detect unauthorized accesses.

6.2 Matching

The system is now ready to work for the detection of unauthorized accesses during the defined detection period.

The main actor interacting with the system during the matching phase is the *System Operator*, that is normally working in a remote control centre, and that is responsible for monitoring several buildings at the same time. The SO in this case uses the Surveillance UI located in the RMS to monitor the accesses to the office and also the system status.

For the demonstration of the use case, and to validate the correct functioning of the system, we have developed a set of interfaces that allow to run the different system components. The *System Administrator* is responsible for setting up the system, so he is the only person allowed to use these interfaces.

> As a future improvement, we plan to configure the system so that the Bodyprint Analyzer (VPUs) and the Re-Identification Server are automatically launched at the defined detection period.

Again, it is recommended that the system users involved in this phase (SO and SA) are aware about the privacy risks related to the operation stage. Following the SALT recommendations, a didactic session should have been carried out during the deployment stage explaining the most relevant concerns. Besides, the SALT Repository could contain specific references about good practices on the matching process (e.g. recommendations for transparency).

As explained in D6.2, one of the most important issues in terms of privacy at this stage is the transparency of the process. As the active participation of the *Data Subjects* is not possible in this case, adequate measures have been implemented to inform about the surveillance operations carried out at the Visual Tools premises: on the one hand informative signs will be installed in the areas under surveillance before the operation stage (*REQ_QUE_6, REQ_VSS_1, REQ_ACC_34*); and on the other hand, an informative handout will be elaborated to be provided and explained to any Data Subject that requests it (*REQ_QUE_*, REQ_LEG_2, REQ_ACC_4-5, REQ_VSS_2*) containing information about the data processing. Further information about how the matching process is carried out can be found in the system documentation as well as in the internal privacy policy (REQ_ACC_23-33, REQ_QUE_9).

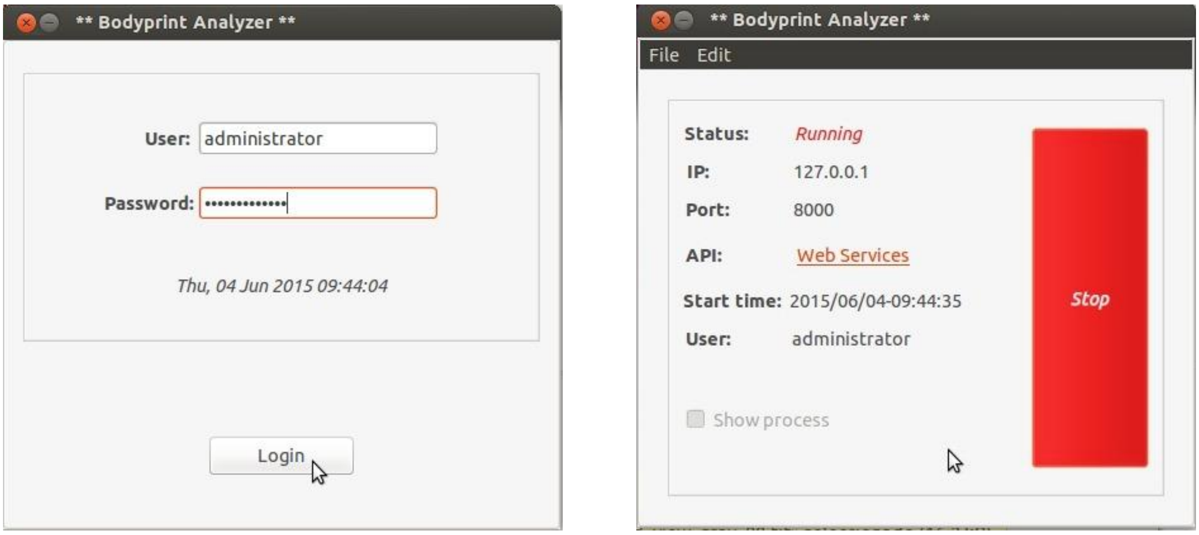
Artifacts used	
A2	Public privacy policy for any Data Subject
A4	Use of informative signs
A11	System documentation
A19	Procedure to let data subjects access their personal information
A25	Didactic sessions for data subjects

Table 18: Artifacts for the matching phase (I)

Regarding the system operations during the matching phase, they are described in the following subsections, and also the action plan defined in case an intrusion is detected.

6.2.1 System operation

If the system is properly deployed, any time a *Data Subject* accesses to the Visual Tools' premises he is detected by the system. This means that one of the VPUs that is continuously processing the data provided by the depth camera connected to it, is able to detect the DS and extracts the corresponding bodyprint.



** Bodyprint Analyzer **

User: administrator

Password: •••••••••••••

Thu, 04 Jun 2015 09:44:04

** Bodyprint Analyzer **

Status: Running

IP: 127.0.0.1

Port: 8000

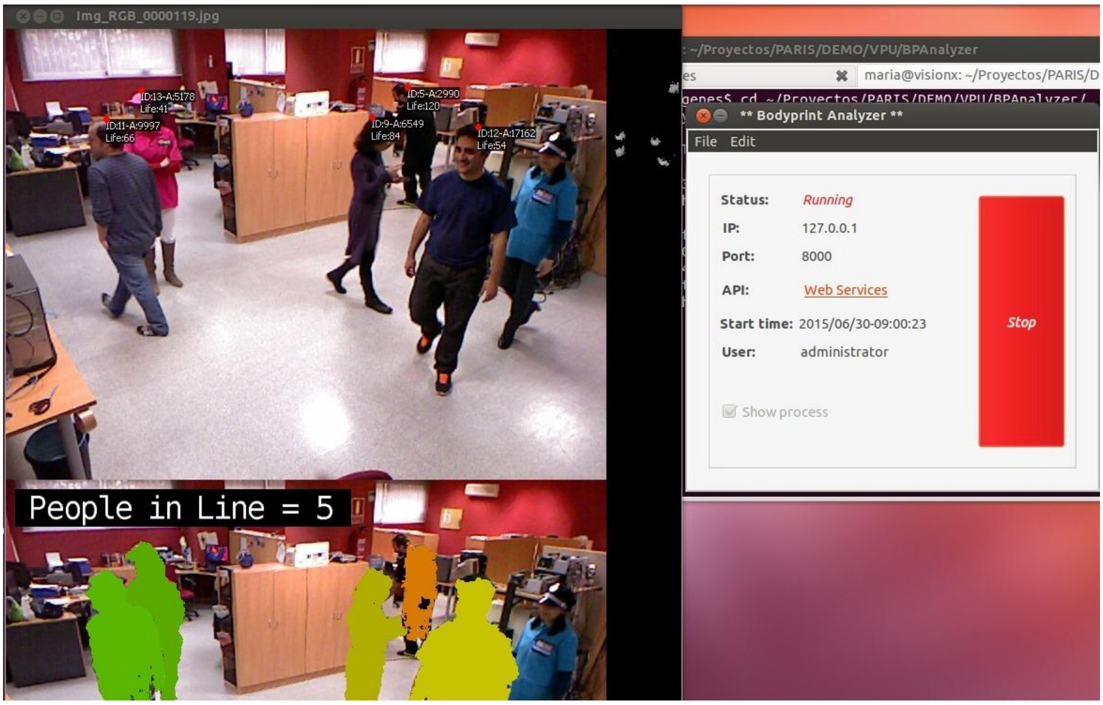
API: Web Services

Start time: 2015/06/04-09:44:35

User: administrator

□ Show process

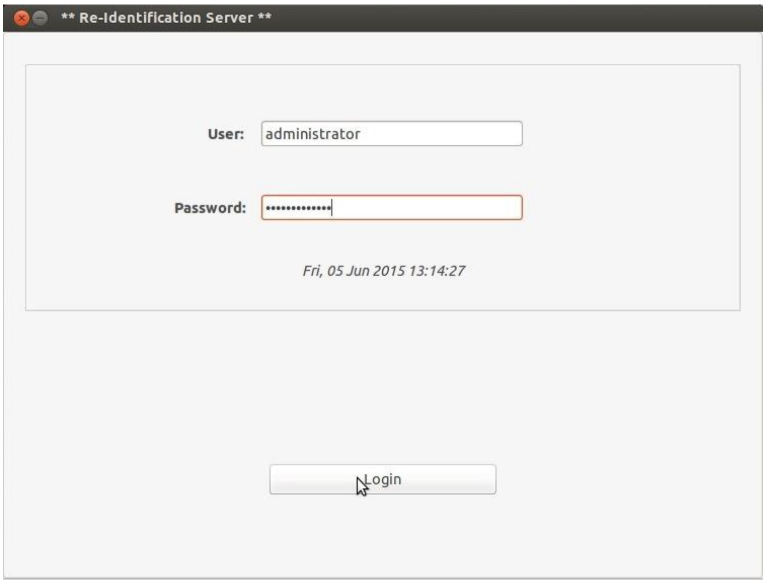
Figure 44: Analyzer User Interface (VPU)



Status: Running
IP: 127.0.0.1
Port: 8000
API: Web Services
Start time: 2015/06/30-09:00:23
User: administrator
☑ Show process

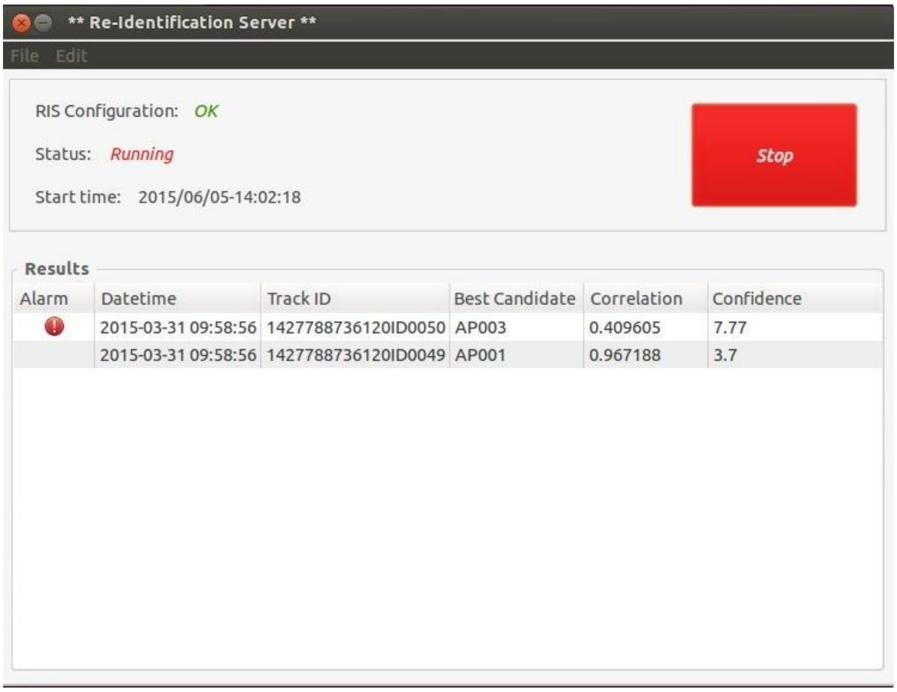
Figure 45: Analyzer User Interface (VPU): Showing the process of detection

In the mean time, the RIS is periodically requesting new bodyprints from each of the VPUs of the system (every 30s). Thus, with only a few seconds of delay, the RIS gets the bodyprint obtained from the DS, and compares it with the APDB to find out if the detected DS is an authorized person.



User: administrator
Password: ••••••••••••
Fri, 05 Jun 2015 13:14:27

Figure 46: Matching User Interface (RIS)(I)



RIS Configuration: OK

Status: Running

Start time: 2015/06/05-14:02:18

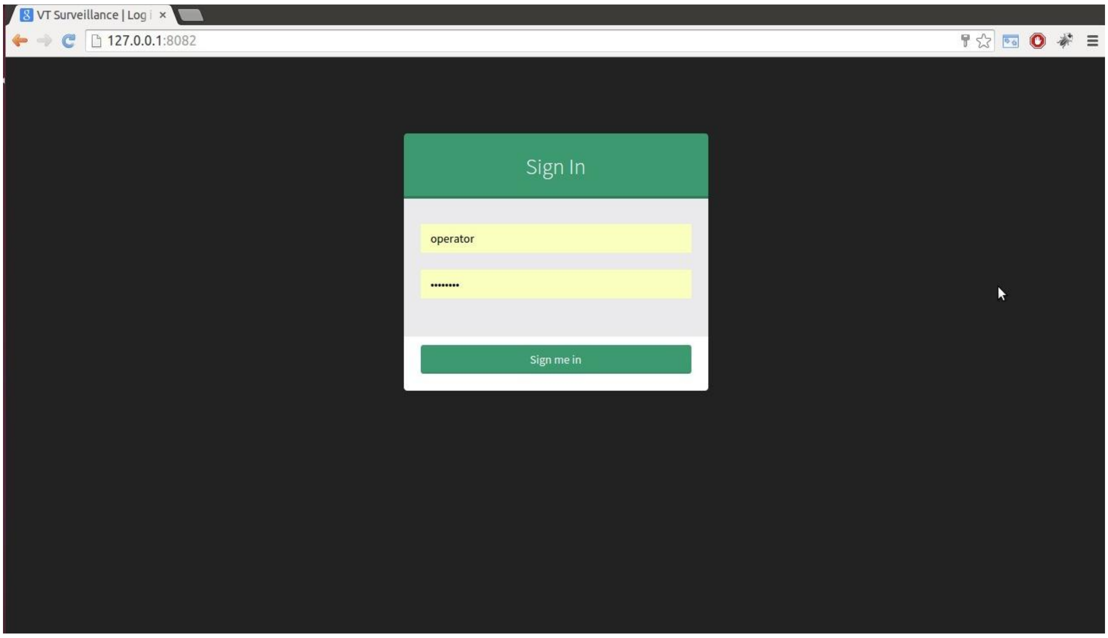
Results

Alarm	Datetime	Track ID	Best Candidate	Correlation	Confidence
●	2015-03-31 09:58:56	1427788736120ID0050	AP003	0.409605	7.77
	2015-03-31 09:58:56	1427788736120ID0049	AP001	0.967188	3.7

Figure 47: Matching User Interface (RIS)(II)

The results of the comparison are then sent to the RMS: an alarm is generated if an intrusion is detected to facilitate its visualization and validation in the Surveillance UI; on the contrary, if the person detected is recognized as one of the authorized persons, juts the information of the event is sent to the RMS.

The *System Operator* can connect to the Surveillance UI through any Web browser. It is just necessary to log in the application with Operator or Administrator profile.

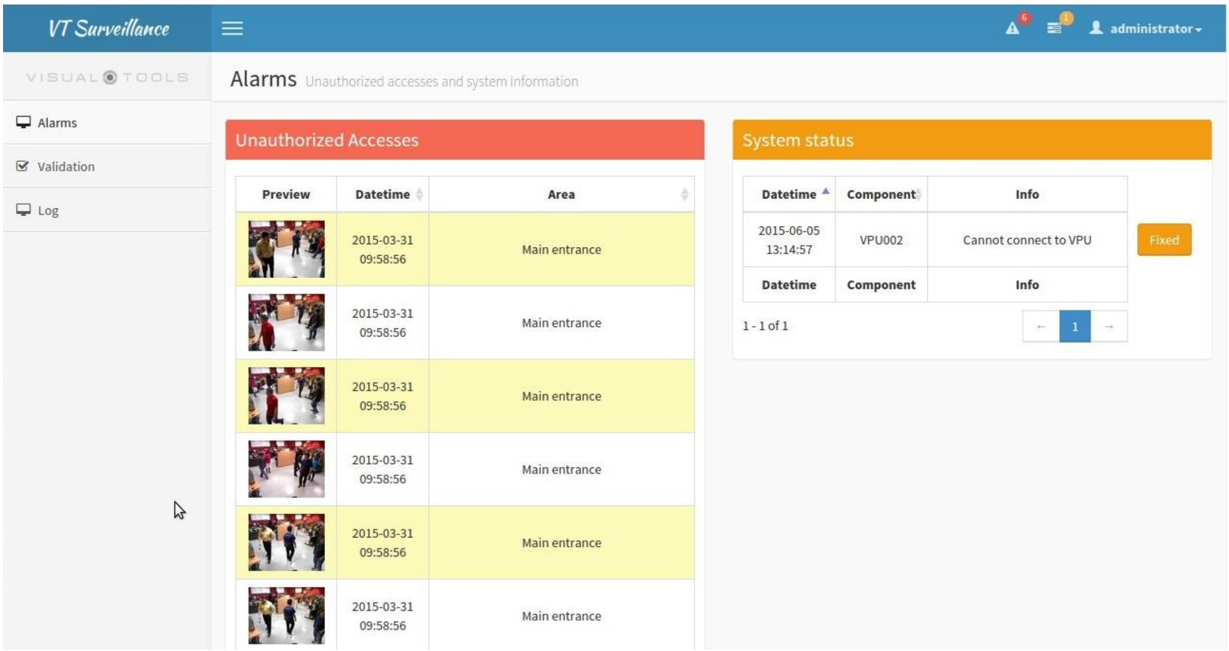


operator

••••••••

Figure 48: Surveillance UI - Login panel

In the main panel of the Surveillance UI, the unauthorized accesses and the system alarms informing of a malfunctioning of the system are displayed. The alarms are ordered by datetime, so the *System Operator* can see first the most recent events.



Alarms Unauthorized accesses and system information

Unauthorized Accesses

Preview	Datetime	Area
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance

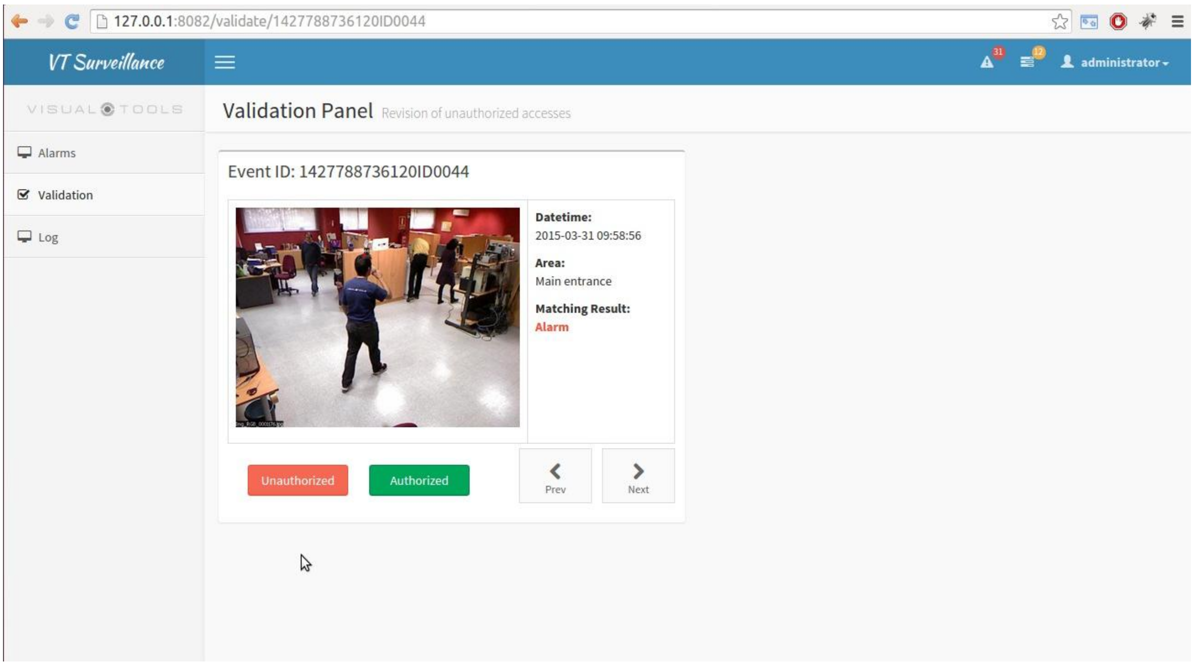
System status

Datetime	Component	Info
2015-06-05 13:14:57	VPU002	Cannot connect to VPU
Datetime	Component	Info

1 - 1 of 1

Figure 49: Surveillance UI: Main panel

Clicking in an alarm, the *System Operator* can see more details of the related event. It is also possible to access to the details of all the alarms that are pending to be validated, one by one, by navigating to the "Validation" panel through the left menu.



Validation Panel Revision of unauthorized accesses

Event ID: 1427788736120ID0044

Datetime:
2015-03-31 09:58:56

Area:
Main entrance

Matching Result:
Alarm

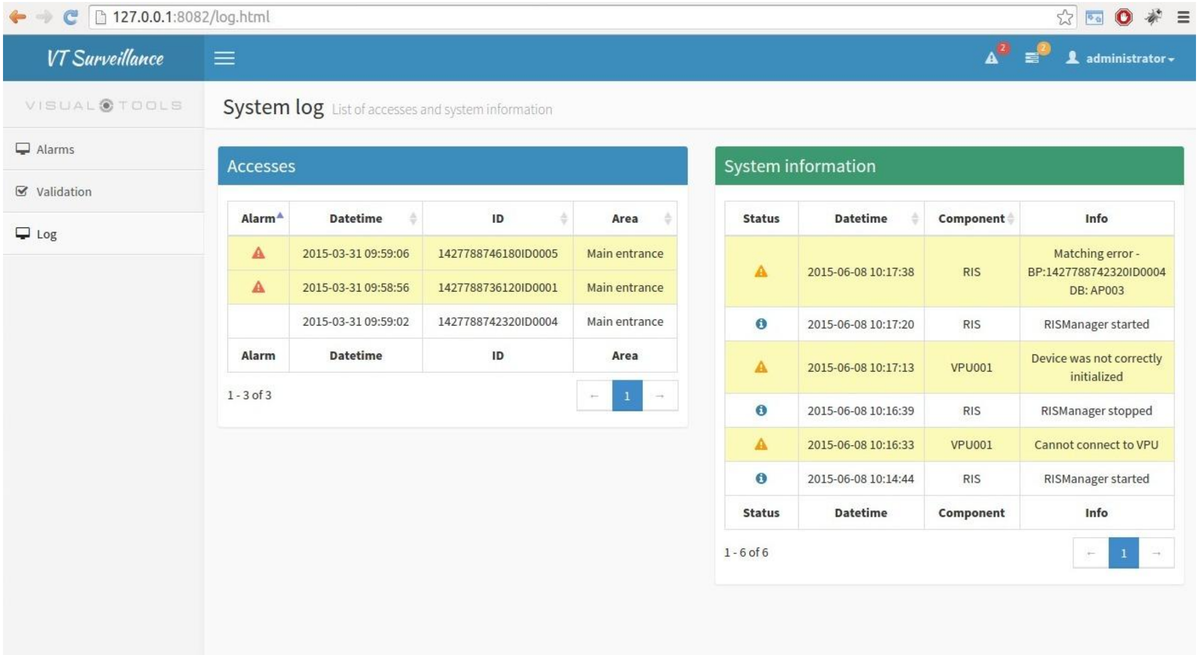
Figure 50: Surveillance UI: Validation panel

In case an alarm is validated as an alarm, the *System Operator* should initiate *the Action plan in case of unauthorized access*.

If the event is not an alarm, the "alarm" warning is removed, and the event is marked as "error". The RIS, that periodically requests the results of the validation to the RMS, will then store the error and raise a new system alarm indicating which bodyprint of the APDB is related to that error. If there are several errors related to the same bodyprint, it means that the bodyprint is not accurate and that it should be renewed. On the other hand, if the system detects errors in several bodyprints, it may indicate that the Bodyprint Matching module is not configured properly and that it should be reviewed.

Finally, there is a third panel in the Surveillance UI where the *System Operator* can consult all the events detected by the system (accesses to the office), and also the messages received by the different components of the system, that can be alerts, or just information that *the System Operator* should consider.

In case there are system errors (displayed in the Alarm and Log panels), the *System Operator* shall contact the *System Administrator* as soon as possible, as the SA is responsible for the maintenance of the system and the SO only has access to the Surveillance UI. Once a system error is fixed, the SA can log into the Surveillance UI and mark the system alarm as "fixed".



System log List of accesses and system information

Accesses

Alarm	Datetime	ID	Area
⚠	2015-03-31 09:59:06	1427788746180ID0005	Main entrance
⚠	2015-03-31 09:58:56	1427788736120ID0001	Main entrance
	2015-03-31 09:59:02	1427788742320ID0004	Main entrance
Alarm	Datetime	ID	Area

1 - 3 of 3

System information

Status	Datetime	Component	Info
⚠	2015-06-08 10:17:38	RIS	Matching error - BP:1427788742320ID0004 DB: AP003
ℹ	2015-06-08 10:17:20	RIS	RISManager started
⚠	2015-06-08 10:17:13	VPU001	Device was not correctly initialized
ℹ	2015-06-08 10:16:39	RIS	RISManager stopped
⚠	2015-06-08 10:16:33	VPU001	Cannot connect to VPU
ℹ	2015-06-08 10:14:44	RIS	RISManager started
Status	Datetime	Component	Info

1 - 6 of 6

Figure 51: Surveillance UI: Log panel

It is important to point out that there is a possibility that an unauthorized person enters in the office and the system makes a mistake deciding that it is an authorized person *(false positive)*. Taking into account the tests performed to the bodyprint algorithm, this type of errors is least likely to occur, as the algorithm provided a low rate of false positives, but it can happen. To deal with this situation, the matching is performed several times for each person appearing in the scene, increasing the probabilities of detecting correctly an unauthorized person. In any case, if the person is never detected as unauthorized, the intruder will access the office and the system will not raise an alarm, it will just show a trace in the log of events with the date and time of the access. At any time, just as a periodic check or in case something is missing at the office, the

System Operator (and also the *System Administrator*) can check from time to time the log of events and verify any access making use of the video surveillance system installed at the office to verify and get more information of an intrusion.

Data Management

- *Data captured by the depth cameras*: the information collected by the depth cameras (RGB and spatial information) is processed on-the-fly, thus, once processed for the extraction of bodyprints the images are directly removed from the system, except for a key frame that is stored with the folder of the bodyprint information. This folder is stored compressed and encrypted.
- *Bodyprints (VPU)*: the bodyprints obtained in a VPU are stored compressed and encrypted in a temporal folder until the RIS sends a request for deletion, which happens after a bodyprint has been correctly sent to the RIS. In case the RIS does not request the bodyprints, or their deletion, the temporary folder is emptied the next time the VPU is started.

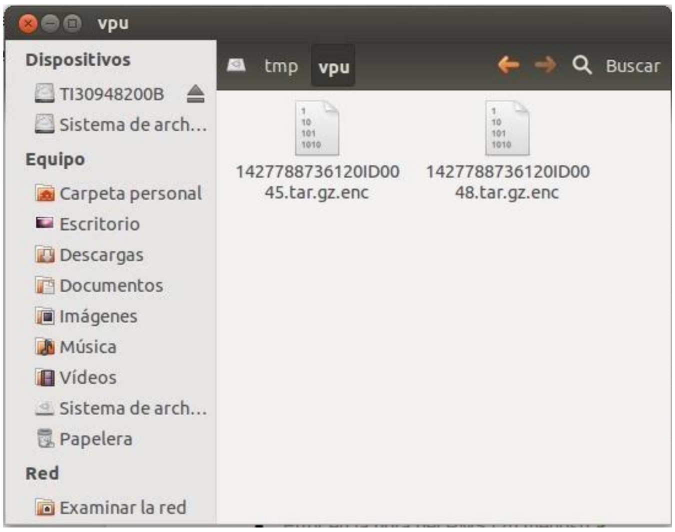


Figure 52: Temporal storage of bodyprints in the VPU

- *Bodyprints (RIS)*: in the RIS, the bodyprints are stored encrypted and compressed, and they are just decrypted to be compared with the templates of the APDB. After this, they are kept in a temporary storage just in case an alarm was generated, until the event is reviewed and validated by the *System Operator*.

  The RIS has a process that requests periodically the results of the validation of the alarms generated and not reviewed yet. Once an alarm has been discarded, the corresponding bodyprint is removed from the temporary folder. Otherwise, all the information is kept in the system (still protected by encryption).

- *Bodyprints (APDB)*: the biometric templates of the Authorized Persons are also stored compressed and encrypted, and they are just decrypted to be compared with incoming bodyprints.

As it will be defined in the system documentation, the bodyprints of the APDB shall be renewed every 6 months, or any time an error is detected in the bodyprints as a result of the validation process.

- *Results of the comparison (RIS)*: all the results of the comparison are stored in the database of the RIS, including all the parameters obtained in the matching process (e.g.: level of confidence of the results), which will serve to detect incorrect configurations of the re-identification module.
- *Events (RDB)*: the RIS sends to the RMS just the result of the comparison (authorized or not), the level of warning (alarm/not alarm), the detection timestamp, the identifier of the corresponding bodyprint and the key frame, that is stored encrypted. This is the information displayed to the SO, that has to authenticate himself to have access to the Surveillance UI. The positive results, as well as the false alarms, will be removed from the RDB once verified. Any result associated to an alleged unauthorized access will be kept as evidence for the local authorities.

Regarding the retention period, according to the Spanish legislation we have defined a maximum retention period for any image of one month, except for those belonging to the people enrolled in the system, that will be kept as long as necessary to achieve the system purpose. The rest of the information (results & bodyprints) will also be kept for as long as necessary, which normally means that if an access is authorized, the corresponding information is removed from the system almost immediately.

Artifacts used	
A8-A10	Use of logs to trace the main operations performed by the system
A12	Encryption of videos and bodyprints
A15	Performance monitoring
A16	System monitoring
A18	Creation of a record containing the results of the recognition process
A20	Access control mechanism for the Web Services
A21	Access control mechanisms for the User Interfaces

Table 19: Artifacts for the matching phase (II)

6.2.2 Action plan in case of unauthorized access

Anytime an *Unauthorized Person* is detected, the *Biometric System* generates an alarm that is displayed to the *System Operator* through the Surveillance UI. Once the event has been confirmed to be an intrusion, the *System Operator* shall call the *System Administrator*, who is responsible for reporting the incident to the local authorities.

A *Police Officer* is sent to collect information of the incidents in order to take the adequate measures for law enforcement. For this, the *Police Officer* may request to have access to the information stored in the system, for which the authorization of the *System Administrator* is required. The data collected by the system as evidence of the intrusion will only be shared with the local authorities, which will be traced in, for example, a document signed by the police indicating why they require the information. The data shared with the police will be watermarked, whenever possible, to make clear that the data is shared with the authorities for law enforcement.

Id	Operational requirement
OR_9	The System Administrator shall be able to authorize the access to the information stored in the system
OR_15	The System Administrator shall assist the Police Officers and the Data Protection Officers for auditing tasks
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

Table 14: Summary of the operational requirements related to the action plan for unauthorized accesses

Besides, to mitigate the impact of false positives, the *System Operators* should check periodically the log of events even if no alarm is raised by the system.

Further details of the action plan will be included in the system documentation.

> This action plan, listed as artifact A24, is still under development and have to be checked with the person who will take the role of the System Administrator, that has experience with this kind of situations.

6.3 Maintenance & Retirement

The last stages of the system lifecycle cover the revisions and updates of the system (Maintenance) until the system is no longer used and has to be uninstalled (Retirement).

Regarding the use of the SALT Framework, there can also be SALT references in the SALT repository providing guidelines for these stages, for example, recommending procedures or verifications to perform in order to retire the system in a controlled manner and respecting users' privacy.

During these stages, the *System Operator* is just in charge of monitoring the different system alarms through the Surveillance UI and of warning the *System Administrator* if there is a problem. The *System Administrator*, that has been registered in the documentation for the General Register as responsible for the system, shall ensure that the system is properly fixed solving the problem himself or contacting the *Surveillance Service Provider* in order to get technical assistance.

These are some of the tasks that are planned for the operation & maintenance stage:

- *Periodic revision of policies and procedures every two years* (A17): for this task, the person responsible for the review (e.g. the System Administrator) can use the SALT Framework to check if the concerns have changed. A report with the results and updates made will be generated.

- *Periodic revision of the need for the system once a year* (A22): at least once a year, the efficiency of the system will be evaluated in order to verify if the system based on bodyprints is really necessary and useful. A report with the results of the evaluation will be generated.
- *Renewal of bodyprints every 6 months* (A15, REQ_ACC_10): at least once every six months the bodyprints composing the APDB will be renewed.

Apart from the mentioned revisions, the system also perform several maintenance operations automatically:

- *Data deletion mechanisms*: automatic procedures have been implemented to delete the information collected from Data Subjects during the matching phase once it is no longer necessary (REQ_LEG_9, REQ_QUE_14, REQ_ACC_53-54).
- *Detection of inaccurate bodyprints*: the results of the validation of alarms will be compared with the results of the matching process to detect inaccurate bodyprints that are producing errors in the matching (REQ_ACC_10). The accuracy of the data is covered by several of the SALT references used in WP6, such as WP6_REF_3.
- *Control of unattended operations:* it is also important to identify the operations performed without any user interaction, and to implement the adequate mechanisms to control them in order to verify that they are working as expected (REQ_QUE_17).

Due, for example, to organizational reasons, or because the solution selected does not provide the expected results or it is just no longer necessary, a system may have to be completely removed. The retirement or decommissioning has to be carried out in a controlled manner according to the laws and regulations. Therefore, the SALT references can contain recommendations on how to perform this task and the privacy and accountability concerns around it. In this particular case of WP6, it is important to ensure that all the biometric data, or any other identity information, are completely deleted from the system and cannot be recovered.

The *Data Controller* is the main responsible for the correct decommissioning of the system, and normally retires the system with technical assistance provided by the SSP. In some cases, the SSP may provide a service for the retirement of old equipment. A technical person should be in charge of this task, but it is also important to involve a legal expert in the process to consider all the issues stated by the current legislations.

Following the SALT Approach, these steps should be followed:

- First, identify all the risks associated with the retirement of the system
- Implement the organizational and technical measures to address these risks
- Evaluate at the end of the retirement process that all the risks have been addressed correctly and that the system has been correctly removed.

During the last semester of the project, we will evaluate more deeply the use of the SALT tools for both the Maintenance and Retirement stages.

7 Conclusion

This document is in line with the previous deliverables of WP6. The design of the biometric system has been a progressive work that has been refined in parallel with the development of the SALT methodology. This way, the stakeholder's needs identified in D6.1 have been analyzed in depth using the SALT tools, which allowed to improve the selected solution as described in D6.2. Following the SALT process, deliverable D6.3 describes how the SALT resources can be used for the development of biometric systems taking into account privacy and accountability, focusing on the initial stages of the system lifecycle (Concept, Design & Development).

By now, in the first stages in which the system is drafted and implemented, the main privacy and accountability concerns pointed out by the SALT questionnaires and references have been integrated into the system design. In general, thanks to the information provided by the SALT Framework we think that we have identified and addressed more privacy and accountability requirements using the SALT Framework, and that we have also obtained useful guidelines to address those concerns more adequately.

During the next semester, we will deploy the system at the Visual Tools' premises in order to verify that the system behaves as expected in the targeted scenario, if it really solves the stakeholder's problems, and also if the privacy and accountability concerns are properly covered. The next deliverable D6.4 will describe the results of this work, trying to evaluate the use of the SALT processes and tools for the whole system lifecycle in order to see the added value of the SALT Framework for the development of biometric systems.

8 References

[1] Directive, E. U. "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Official Journal of the EC 23.6 (1995).

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011, Brussels, 25 January 2012.

[3] Lucas D. Introna and David Wood (2004) "Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems", In Surveillance & Society CCTV Special (eds. Norris, McCahill and Wood) 2(2/3): 177-198

[4] Rachel L. Finn, David Wright, and Michael Friedewald. "Seven Types of Privacy" European Data Protection: Coming of Age. Ed. S. Gutwirth et al.. Dordrecht: Springer Science+Business Media, 2013

[5] "Organic Law 15/1999 of 13 December on the Protection of Personal Data (LOPD)", Spanish Parliament, Official State Gazette (BOE) nº 298, 14-Dic-1999.

[6] The Regulation developing the Data Protection Act 15/1999 of 13th of December (RDLOPD for short), approved by Royal Decree 1720/2007 of 21st of December.

[7] Spanish Data Protection Agency. Instruction 1/2006, on processing personal data for surveillance purposes through camera or video-camera systems, 8th of November 2006.

[8] "Guide on Video Surveillance", AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (SPANISH DATA PROTECTION AGENCY), Official Publications Identification Number: 052-08-007-8.

[9] Denis Butin and Daniel Le Métayer et al., "End-to-end Privacy Accountability: Systematic Analysis of the General Data Protection Regulation Draft", Inria, Université de Lyon, France.

[10] Article 29 Data Protection WorKing Party, "Opinion 3/2012 on Developments in Biometric Technologies," 00720/12/EN, Adopted on 27th April 2012.

[11] Ann Cavoukian, Alex Stoianov, "Privacy by Design Solutions for Biometric One-to-Many Identification Systems", June 20, 2014.

[12] ISO/IEC 2382-37: Information technology — Vocabulary — Part 37: Biometrics. First edition 2012-12-15.

[13] "Guía de Seguridad de Datos", AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (SPANISH DATA PROTECTION AGENCY), Official Publications Identification Number: 052-08-003-6.