PrivAcy pReserving Infrastructure for Surveillance

Deliverable D6.4

Biometrics Use Case Evaluation

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D6.4
Title:	Biometrics Use Case Evaluation
Version:	v1.0
Date:	18/12/15
Confidentiality:	Public
Contributors:	INRIA AIT KU Leuven University of Malaga Visual Tools

Funded by the European Union's Seventh Framework Programme

Table of Contents

Version	Status	Date
v0.1	First draft of ToC	24/9/2015
v0.2	Contribution to section 3.1 by AIT and VT	22/10/2015
v0.3	Contribution to section 2 by UMA	17/11/2015
v0.4	Contribution to lessons learnt by INRIA, LEUVEN	09/12/2015
v0.5	Contribution to added value by UMA	09/12/2015
v0.6	Contribution to evaluation of SALT by AIT	09/12/2015
v0.7	Added Conclusions and UC details	11/12/2015
V1.0	Added comments from the reviewers	18/12/2015

Approval		
	Name	**Date**
Prepared	Visual Tools	11/12/2015
Reviewed	AIT, THALES, KU LEUVEN	18/12/2015
Authorised		

Circulation	
Recipient	**Date of submission**
Project partners	21/12/2015
European Commission	

List of Figures

List of Tables

Abbreviations and Definitions

Abbreviation	Definition
AEPD	Spanish Data Protection Commissioner's Office *(Agencia Española de Protección de Datos)*
APDB	Authorized People Database (also known as biometric enrolment database)
DC	Depth Camera
ICT	Information and Communication Technologies
LOPD	Spanish Organic Law 15/1999 of Personal Data Protection

PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PIA	Privacy Impact Assessment
RIS	Re-Identification Server
SALT	Socio-ethicAl, Legal, Technical
SFMT	SALT Framework Management Tool
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 summarises the usage of the framework in the context of the biometrics use case demo providing some information about the process followed and giving some details on the evaluation of the value of the SALT Framework in the Biometrics Use Case. Information about the added value of the approach the lessons learnt is also provided.

1. Introduction

This deliverable complements the other deliverables on WP6 dealing with the use case in the context of biometrics. Specifically this deliverable deals with the evaluate the approach and the relevance of the SALT framework.

This documents begins with the definition of the scenario and the biometrics use case. It consist of the **detection of non authorized accesses to a building with security requirements and preserving users' privacy**. A summary of the use case process is provided and a list of the artefacts is presented. These artefacts serve as validation mechanism since they cover the requirements of the use case. A table linking artefacts and use case requirements is provided (More details related to the artefacts and the requirements can be found in D6.2 “Biometric Use Case: SALT compliant Framework”). A summary of the SALT framework and the SALT process is also provided.

The document follows with the evaluation, which is done at different levels. First the evaluation approach is presented, and later the evaluation at system level and the evaluation of the SALT framework are presented. The evaluation of the resulting SALT process is also provided.

The results of the evaluation provided us with useful information about the added value of the approach we followed. The lessons learnt and some recommendations for extensions of the SALT Framework Management Tool (SFMT) are proposed, based in the information received.

This document takes as a base the information related to the SALT framework described in D2.1 to D2.4, the tools from work package 3 and the SALT process from the deliverables of the work package 4. The approach followed for evaluation is similar to the one followed in the other use case of the project, the video surveillance use case (WP5).

This deliverable is structured as follows: In section 2 the summary of the use case is provided. In section 3 the evaluation is presented. Section 4 is related to the possible extensions to the SFMT and section 5 presents the conclusions.

2. Description of the biometrics use case and the SALT Framework

2.1 Biometrics use case description

2.1.1 Scenario and use case description

The biometrics use case addresses 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 its 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 fulfil the following requirements from the stakeholder (surveillance goals):

- Prevention against theft (deterrence);
- Facilitation of the work of security operators during the night period, reducing the false alarms;
- 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 has been deployed at the Visual Tools' premises covering the main transit areas of the office with cameras, providing depth and spatial information that is analyzed to detect the people accessing to the office. It also includes a mechanism for re-identification allowing to match any person detected with a database of authorized people. (See “D6.3 PARIS Biometrics Use Case” for more information)

In case the system does not recognize the person detected, an alarm is automatically generated and displayed to the operator responsible for monitoring the facilities. The operator is responsible for verifying the alarm, and in case it is an unauthorized access, the operator shall execute the defined action plan for unauthorized accesses, which includes to contact the local authorities for law enforcement and the registration of the incident in a specific file.

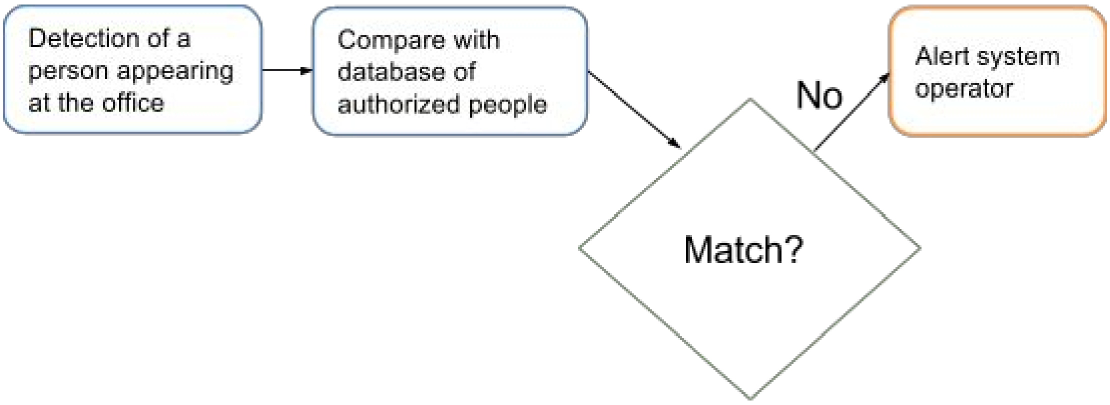

Detection of a person appearing at the office
Compare with database of authorized people
Match?
No
Alert system operator

Figure 1: Summary of the capabilities of the biometric system developed

The main features provided by the system that serve to solve the stakeholder problems are listed below:

- **Re-identification capability**, allowing to compare any data subject with a database of authorized people.
- **Management tool** (Surveillance User Interface) displaying the results of the re-identification, 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.

The Biometric system helped to validate a list of requirements. These requirements are detailed in the deliverable D6.2 “Biometric Use Case: SALT compliant Framework”. Below the summary of Artefacts validating the use case requirements is presented in order to show the traceability between requirements and the validation mechanism.

ID	Artefacts	Requirements
A1	***SALT Framework questionnaire for biometrics*** Analysis through the PIA questionnaire provided by the SALT Framework of the purpose, necessity and legitimacy of the system, and its potential impact on individuals’ privacy. A report containing the rationale of each response.	*REQ_QUE_*,* *REQ_LEG_1,* *REQ_ACC_2-4* *(and any other requirement related to the evaluation of the privacy impact)*
A2	***Public privacy policy*** Elaboration of a privacy policy, in which the purpose of the system and the treatment of personal data is explained. This policy will be sent to the people to be enrolled in the system as authorized, and also to the employees of the	*REQ_QUE_*,* *REQ_LEG_2,* *REQ_ACC_4-5,* *REQ_VSS_2* *(and any other requirement related to*

	client company working at the office where the system is going to be deployed. It will also be available for any data subject that requests it.	*the duty to inform)*
A3	***Inscription of the system in the General Register*** Visual Tools keeps a copy of the form provided to the AEPD for the inscription in the Agency's General Register of the video surveillance system installed at the Visual Tools headquarters, and also the favorable resolution for the registration of the system.	*REQ_VSS_3*
A4	***Use of informative signs*** Informative signs will be placed at least at the entrances leading onto the areas under surveillance.	*REQ_QUE_6, REQ_VSS_1, REQ_ACC_34 (and any other requirement related to the duty to inform during the matching phase)*
A5	***Definition of a procedure for enrolment in which the collaboration of the data subject is required*** In the system documentation, the process for the enrolment of people will be described, and also the periodicity for the revision and renewal of bodyprints (at least once every 6 months)	*REQ_QUE_5, REQ_LEG_3,* *REQ_ACC_18-19,REQ_ACC_37, REQ_ACC_39, REQ_LEG_7*
A6	***Role-based access control*** The access to the different system resources (interfaces, programs and data stored) will be restricted to certain users, being this roles defined: ● *System Administrator*: main responsible for the system, with access to all the system resources. ● *System Operator*: user with limited access to the information. The operator will only be able to use the interfaces for matching, and to view the results of the recognition process ● *System Auditor*: user with limited access to the system resources for auditing. This user will have to request authorization to the *System Administrator* indicating for which purpose the access to the system is required. ● *Data subject*: Data subjects (e.g. people enrolled in the system) will be able to request access to their personal information stored. For this, the authorization of the *System Administrator* is required, and the access is limited to the personal data belonging to that person.	*REQ_QUE_10,REQ_QUE_13, REQ_VSS_6, REQ_LEG_6, REQ_ACC_35-36*
A7	***Training sessions for the different system users*** We will organize at least two different sessions before the operation phase, to educate System Administrators and System Operators in the use of the system and the different procedures defined, informing them about their responsibilities and security obligations. We will keep a summary record signed by all the participants to prove that the sessions have been held.	*REQ_VSS_7, REQ_QUE_10, REQ_ACC_1*
A8	***Data collection logs***	*REQ_QUE_17,*

	Data collection processes will be recorded in logs. This logs will contain at least this information: ● Date and time ● Data collected ● Purpose of data collection ● The system user (if any) involved in the collection of data	*REQ_LEG_4,* *REQ_ACC_22* *(and any other requirement related to the limitation of the collection of personal data)*
A9	***Data access logs*** Any access to the data stored in the system will be recorded in logs. This logs will contain at least this information: ● Date and time ● Data accessed ● Purpose of the access ● the system user performing the action	*REQ_QUE_10,* *REQ_QUE_19,* *REQ_ACC_46-50,* *REQ_VSS_7* *(and any other requirement related to the limitation of the access to personal data)*
A10	***System logs*** Evidence about the operations performed by the system, such as data handling, will be generated in the form of system logs, containing at least this information: ● Date and time of the trace ● Modifications on the data stored (if any) ● Information of the main operations performed by the system ● Information of exceptions or errors detected during the operation of the system	*REQ_QUE_14,* *REQ_QUE_17,* *REQ_QUE_19,* *REQ_LEG_4,* *REQ_ACC_22,* *REQ_VSS_5 (and any other requirement related to the transparency of system processes)*
A11	***System documentation*** The surveillance system developed will be properly documented for internal use. At least, these documents will be elaborated: ● Manual explaining the technical implementation of the system (architecture, components, main system operations, available resources, security mechanisms, how to configure and set up the system, system maintenance, etc.). ● Privacy Management Program (PMP) describing the policies, procedures and practices of the company with regards to the processing of personal data. This documents can be provided to any data protection officer auditing the system	*REQ_VSS_2,* *REQ_ACC_1* *(and any other requirement related to the implementation of measures and procedures for data protection)*
A12	***Data encryption*** The following information will be encrypted: ● Videos captured during the enrollment process ● Key frames kept for the verification of alarms ● Biometric templates stored in the Authorized People Database (APDB) ● information transferred between the different system components (e.g. from a VPU to the RIS)	*REQ_QUE_13,* *REQ_QUE_15,* *REQ_LEG_6,* *REQ_VSS_6,* *REQ_ACC_35-36*

A13	***Connection of devices through a Local Area Network (LAN)*** The VPUs will be connected to the RIS through a LAN, and the remote access to the VPUs and the RIS will be disabled, being required to be physically at the office to use a VPU or the RIS.	*REQ_QUE_13,* *REQ_QUE_15,* *REQ_LEG_6,* *REQ_VSS_6*
A14	***Alarm management separated from the matching process*** It is necessary to use a module to read the results of the matching process, and to generate and send the alarms when an unauthorized access is detected. This module requires connection to the Internet, as the operators may be in a remote control centre. Initially, we thought that this module could be integrated in the RIS, but as the RIS contains the template database (APDB), to increase the database security, it is better to put the module in another device or partition that only has read access to the results of the matching process through the LAN, and that is just responsible for the generation and emission of alarms.	*REQ_QUE_13,* *REQ_LEG_6,* *REQ_VSS_6*
A15	***Performance monitoring*** To reduce the risks related to errors in the matching process, an automatic process will review the validation of the matching results, calculating the rate of false positives related to each bodyprint stored in the template database. This will serve to detect inaccurate bodyprints.	*REQ_QUE_9,* *REQ_QUE_17,* *REQ_QUE_18-19,REQ_SOC_2-3, REQ_LEG_7,* *REQ_ACC_37,* *REQ_ACC_39*
A16	***System monitoring*** The different components will be periodically reviewed by the System Administrator to check that the system is working as expected (at least twice a year). Moreover, other mechanisms have been implemented to facilitate the detection of component failures: ● Anytime the RIS requests information from a VPU, and the VPU does not respond, an alarm will be generated and displayed in a monitoring user interface. ● If a camera stop working, the VPU connected to it will not be able to collect any information, and thus it will not be possible to detect people accessing to the office. In this case, the VPU will not respond to any request from the RIS, so an alarm indicating a problem in the VPU will be generated. ● The monitoring user interface will also show the date and time when the RIS was started, and also when it performed the latest comparison. In case the RIS has not provided any data in the past 48 hours, an alarm will be generated and displayed.	*REQ_QUE_16-17*
A17	***Periodic revision of policies and procedures*** At least every two years the different policies and procedures defined will be reviewed. For this task, the person responsible for the review (e.g. the System Administrator) can use the SALTFramework to check if the concerns have changed. A report with the results and updates made will be generated.	*REQ_ACC_1*

A18	***Creation of a record containing the results of the recognition process*** The results of the matching process and the parameters used in the comparison will be stored, for two main reasons: ● To verify the correct functioning of the biometric system for the detection of unauthorized accesses ● To facilitate the collection of evidences in case of intrusion The *System Operator* will be responsible for the reviewing the alarms generated, and validating the results, which also serves to mitigate the consequences of errors in the matching process. After the alarms have been validated by the *System Operator*, for false alarms or positive matches only the date and time where a person was detected will be kept. This prevents the profiling of the data subjects enrolled in the system. In case of true alarm, all the information related to the incident is kept to be provided to the local authorities for law enforcement	*REQ_QUE_9,* *REQ_QUE_18-19*
A19	***Procedure to let data subjects access their personal information*** A specific procedure will be defined to let data subjects have access to their personal data stored in the system, for which the supervision and authorization of the *System Administrator* is required. This process will be described in the system documentation.	*REQ_QUE_18,* *REQ_LEG_8,* *REQ_ACC_42-45*
A20	***Access control mechanism for the Web Services*** Authentication and authorization will be required to request information to a VPU through its Web Services. This way, we will prevent unauthorized accesses to the bodyprints stored temporary there.	*REQ_QUE_10,* *REQ_QUE_13,* *REQ_QUE_15,* *REQ_QUE_19,* *REQ_ACC_50,* *REQ_VSS_7*
A21	***Access control mechanisms for the User Interfaces*** Authentication and authorization will be required to use the applications developed for setting-up the system, capturing images, enrolment and management of the results. Besides, during the login phase, it will also be necessary to indicate the purpose of the use of the application, which will be recorded in a log with the date and time of the login.	*REQ_QUE_10,* *REQ_QUE_13,* *REQ_QUE_19,* *REQ_VSS_6,* *REQ_LEG_6,* *REQ_ACC_35-36*
A22	***Periodic revision of the need for the system*** 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.	*REQ_QUE_3,* *REQ_ACC_35*
A23	***Document signed by the installer*** The installer is the person (or company) responsible for the deployment of the system at the Visual Tools' Headquarters, and the correct positioning of the cameras, that should not obtain images from public areas. We will keep a document signed by the installer indicating the details of the the installation of the system.	*REQ_VSS_4*

A24	***Action plan in case of unauthorized access*** The actions to be performed in case of intrusion will be detailed in the system documentation. 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.	*REQ_QUE_11,* *REQ_ACC_1,* *REQ_ACC_46*
A25	**Didactic sessions for data subjects** In order to inform, and take into consideration the points of view of any data subject, at least two didactic sessions will be scheduled: ● Session with VT employees ● Session with maintenance employees ● Session with system operator As a result of these sessions, a report will be generated. Furthermore, the data controller (VT) is committed to organize additional informative sessions on demand of data subjects if necessary, and whenever possible.	*REQ_SOC_1,* *REQ_ACC_1,* *REQ_LEG_2*
A26	***Provision of "surveillance breaks"*** *Neutral spaces, without surveillance, will be provided in areas close to the entrances and far from the critical areas.*	*REQ_SOC_4-5*

Table 1: List of artefacts to be implemented

2.1 SALT Framework and SALT global process

In order to make this document self-contained, this section provides an overall description of the SALT framework and the SALT compliant process (see deliverable D4.4 “SALT Compliant Processes General Guidelines” for an in depth description).

2.2.1 SALT Framework

The SALT framework refers to the whole set of information regarding privacy and accountability concerns for video surveillance and biometric systems that is used by the SALT methodology. The SALT Framework is a key component in the SALT methodology, since the developed tools as the SALT compliant process, are highly dependent of this information.

In practice, the SALT framework is stored into the SALT repository, a database where all the information is structured following a template called SALT reference. Each reference contains relevant privacy/accountability information divided into several (the minimum is just one) concerns. A whole set of information regarding the source, area and context of the information is also provided, and together with that, a series of OCL rules (some concerns may not have them) that will be used by the automatic validator during the design phase of the process.

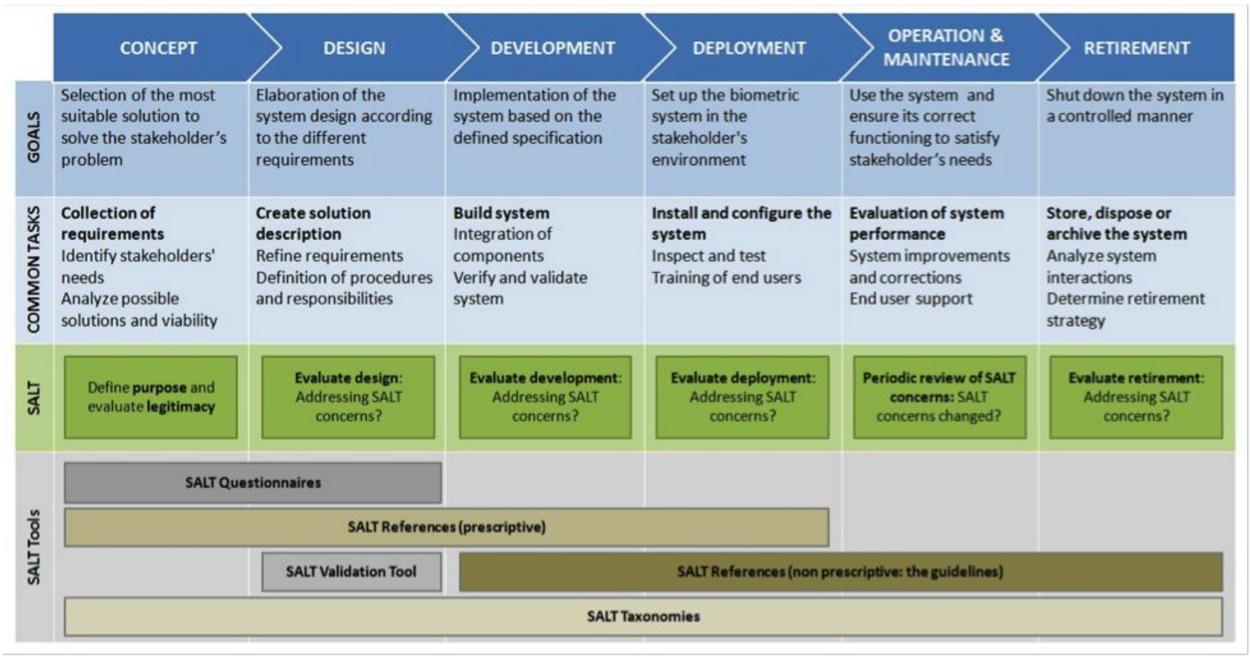
The size and the quality of the SALT framework depends on in the SALT experts, users with a relevant knowledge in privacy and/or accountability in one or several of the following areas: socio-contextual, ethical, legal, technological. These experts are the ones who will create the SALT references and populate the SALT repository, that is, they will contribute to the creation of the SALT framework.

2.2.2 SALT Process

The SALT compliant process bounds to the lifecycle of a surveillance system. It describes the whole system work flow through all the stages, from the concept stage to the final system retirement, indicating what type of user is involved at each stage. Besides, the particularities of this process ensures the creation and usage (if followed) of a SALT compliant system, that is, a surveillance system where privacy and accountability concerns have also been taken into account, together with the rest of functional requirements.

Even though the application of the SALT compliant process guarantees a SALT compliant system, it is important to nuance this statement. Since the content of the SALT framework depends on the input given by experts, it is clear that the information stored into the SALT repository will evolve with time: addition of new concerns, possible extensions, modifications to some others, etc. This means that a particular surveillance system developed following the SALT compliant process may differ on its final design/implementation according to the time when it was created, that is, depending on the maturity of the SALT framework. However, in every case we say we obtain a SALT compliant system because the privacy/accountability concerns that were available at that moment were taken into consideration.

Having clarified the nature and reason to be of the SALT compliant process, Figure 2 depicts the lifecycle of the process as it goes through the different stages. Starting from the concept phase, where the system stakeholders have the intention to create (and the initial requirements) a given surveillance system, and ending with the retirement of such system after its whole operational period.



	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. Stages of the SALT compliant process

Figure 3 shows a different perspective of the SALT compliant process, where the different user types (or roles) for each stage of the process can be seen. Nevertheless, it is important to remark that a user of the system is not forced to interact with just one stage of the process, as it may seem from Figure 3, but it can take part in any other stage if necessary (or not). For example, a system designer could participate in the design phase and also in the development phase, just to mention one possibility.

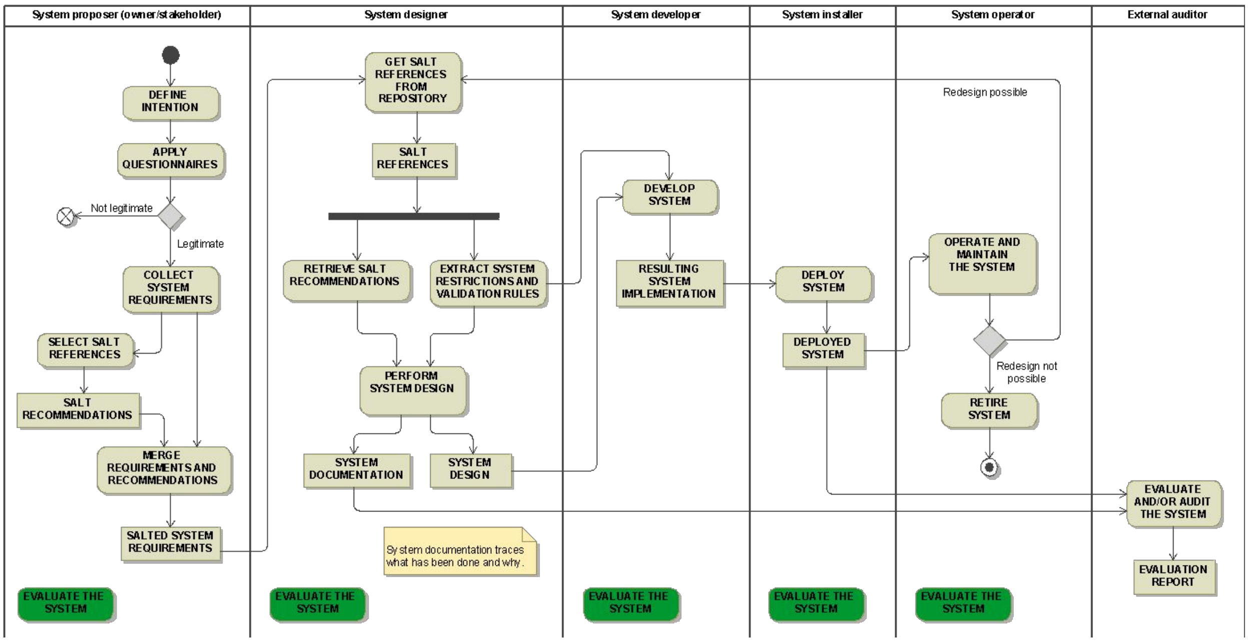


Figure 3. SALT compliant process and user types

3. Evaluation of the value of the SALT Framework in the Biometrics Use Case

3.1 Evaluation approach and method

The SALT Framework is, by design, a conceptual framework to integrate multi-party concerns in the design and development of surveillance systems. The digitalised representation of privacy and accountability relevant knowledge in the SALT Repository and the associated management tools are computerised ways to interact with such knowledge. The SALT Framework is associated with the SALT design process, designed by the PARIS consortium to streamline privacy-by-design process for surveillance systems.

The work described in this document has two main goals:

- Evaluate the added value and relevance of the SALT Framework in the biometrics use case presented in WP6;
- Evaluate the added value and relevance of the SALT process for the development of biometric systems for surveillance.

It is obvious that the target of evaluation (ToE) is neither a software/hardware system, of which the technical partners in the PARIS consortium are familiar in terms of evaluation; nor is it a system that the legal and social partners in the consortium are familiar with. After multiple discussions, the PARIS consortium decided to tackle the evaluation in a pragmatic way, addressed to evaluate the added value of SALT conceptual framework, management tools, and SALT compliant process in the context of the biometrics use case. Within this pragmatic approach, two methods for the evaluation have been used:

- The evaluation criteria defined in D6.1 to verify the functional aspects and the different requirements of both the surveillance system and the SALT Framework;
- Evaluation of the added value of the SALT methodology by opinions on the ToE in form of "lessons learned" from the partners involved in the development of the biometrics use case;

3.2 Evaluation at the system level

The objective of this section is to verify that the biometric system, that has been developed using the SALT methodology, accomplishes the intended surveillance purpose while fulfilling the privacy and accountability requirements.

3.2.1 Functional aspects of the biometric system

One of the key points to demonstrate the value of the SALT approach for the development of surveillance systems, is to check that following the SALT process the resulting system is able to provide the surveillance capabilities for which it was built.

In this case, the system was designed to **detect non authorized accesses** to the Visual Tools' headquarters in Madrid. The surveillance goals initially defined are addressed by the system with the following capabilities:

Surveillance goal	Technical capability
Prevention against theft	● People detection and tracking ● Extraction of biometric templates for people characterization ● Database of authorized people ● Re-identification capability to decide if an access is authorized ● Automatic generation of alarms in case of non-authorized access
Facilitation of the work of security operators and reduction of false alarms	● Management tool displaying the results of the re-identification ● Collection of information of each event detected (data, time, area, etc.) ● Validation functionality allowing to discard false alarms
Collection of evidences for law enforcement	● The system records any access detected to the monitored area, collecting information of every event (date, time, key frame, etc.) ● The system records the accesses to the data stored and the use of the system tools

Table 2: Mapping of technical capabilities with the technical capabilities

Once developed and deployed at the Visual Tools' premises different types of tests have been carried out for the evaluation of the system, that are based on the criteria defined in D6.1, and that are addressed to check the surveillance capabilities:

Acceptance test cases *(positive scenarios)*	
TEST_CASE_1	**Detection of a non-authorized person**
Preconditions	The biometric system has been properly installed and configured. The biometric system covers the main transit areas of the private office. The authorized people have already been enrolled in the system.
Test case	An unauthorized person enters the office.
Expected result	The system generates an alarm giving information of the intrusion and sends it to the *System Operator*.
Capabilities tested	All
TEST_CASE_2	**Detection of an authorized person**

Preconditions	The biometric system has been properly installed and configured. The biometric system covers the main transit areas of the private office. The authorized people have already been enrolled in the system.
Test case	An authorized person enters the office.
Expected result	The system recognizes the person as authorized, and does not generate any alarm, but the event can be reviewed through the Surveillance UI
Capabilities tested	● People detection and tracking ● Extraction of biometric templates for people characterization ● Database of authorized people ● Re-identification capability to decide if an access is authorized ● Management tool displaying the results of the re-identification ● Collection of information of each event detected (data, time, area, etc.) ● Validation functionality allowing to discard false alarms

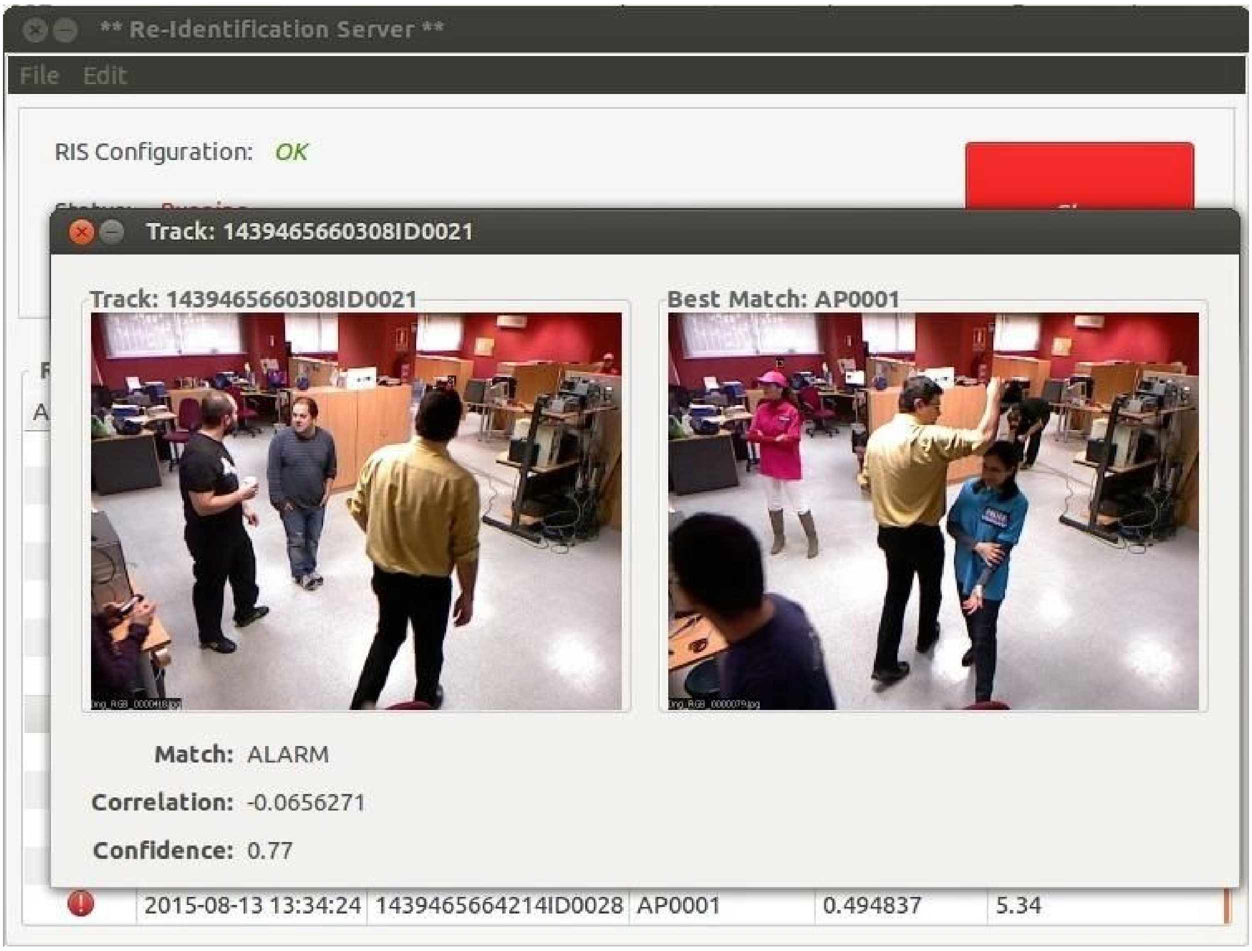
Table 3: Acceptance test cases

Besides, we have evaluated the usability of the *Surveillance User Interface* through an interview to the *System Operator*, to find out his experience and expectations using the tool. We have elaborated a survey to measure the usefulness and the user acceptance of the interface, based on several questions related to the usefulness of the tool, ease of use, ease of learn and subjective opinion

Some of the tests performed to evaluate the functional aspects of the system are described in the following subsections.

3.2.1.1 Detection of non-authorized accesses

As it is mentioned in the different documents of the work package 6, once a person enters into the monitored area, their presence is detected and a bodyprint is generated. This bodyprint is compared with the authorised bodyprint list and the results related to correlation and confidence are generated (see the image below).



RIS Configuration: OK

Track: 1439465660308ID0021

Track: 1439465660308ID0021

Best Match: AP0001

Match: ALARM

Correlation: -0.0656271

Confidence: 0.77

2015-08-13 13:34:24 1439465664214ID0028 AP0001 0.494837 5.34

Figure 4: Non-Authorised access test

At it is described in the rest of the deliverables of the WP6 (D6.1 to D6.3), the bodyprints use a 3D video analysis technique in order to detect a person. Once a person is detected a template of the bodyprint based in the height and the wearing clothes is generated. This template is compared with already stored templates in order to get the correlation and confidence. Below the step followed for generating the templates is shown.

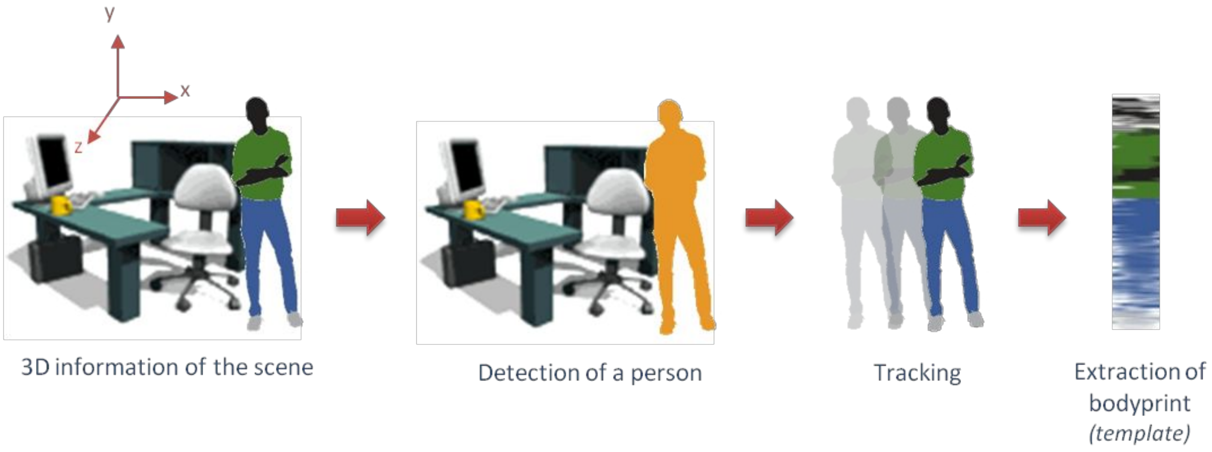
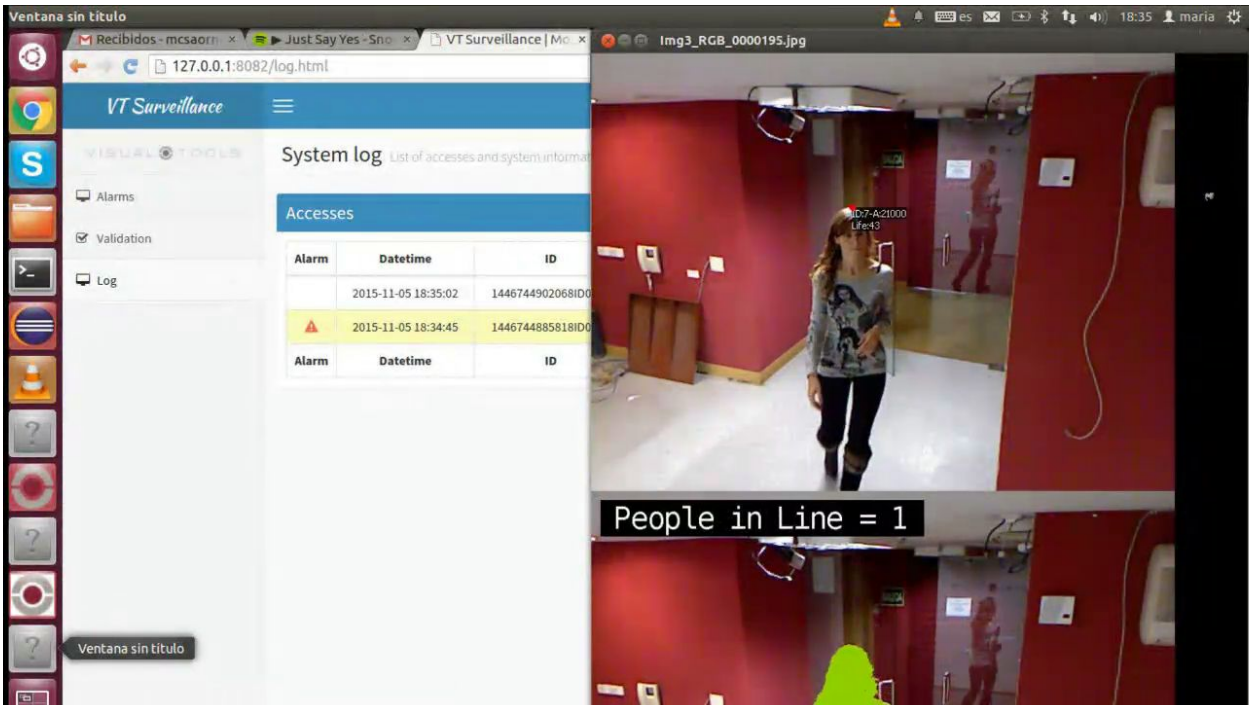


Figure 5: Technology for people re-identification

The already mentioned correlation and confidence information is sent from the Re-Identification Server (RIS) to the Re-Identification Management System (RMS) in which an alarm is generated. In the following image the system log is shown together with the video capture. The system log shows a warning symbol indicating that a non-authorised access has been detected. Apart from this, a system wide alarm is sent in order to use system notifications to notify the operator about the intrusion.



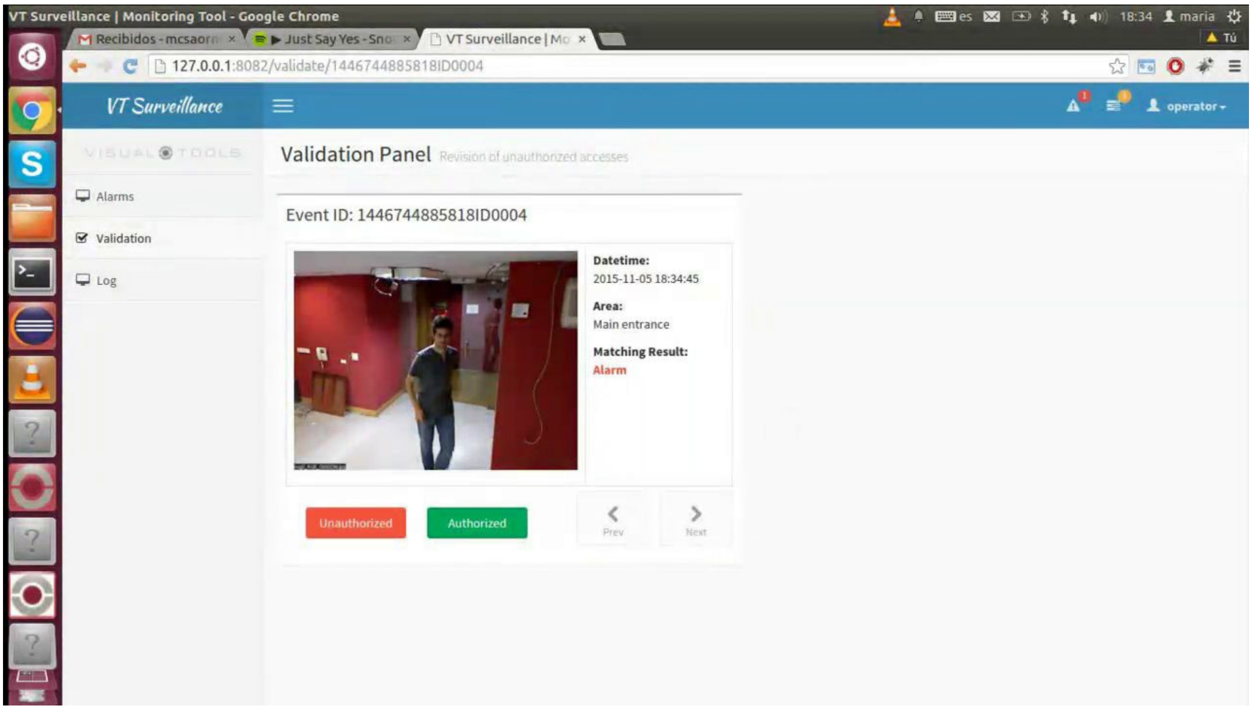
System log List of accesses and system informat

Accesses

Alarm	Datetime	ID
	2015-11-05 18:35:02	1446744902068ID0
⚠	2015-11-05 18:34:45	1446744885818ID0
Alarm	Datetime	ID

Figure 6: Non-Authorised access test, System Log

Once the operator accesses to the event, the operator may check the date and the images related to the intrusion and override the system decision if it was a false positive.



VT Surveillance | Monitoring Tool - Google Chrome

127.0.0.1:8082/validate/1446744885818ID0004

Validation Panel Revision of unauthorized accesses

Event ID: 1446744885818ID0004

Datetime:
2015-11-05 18:34:45

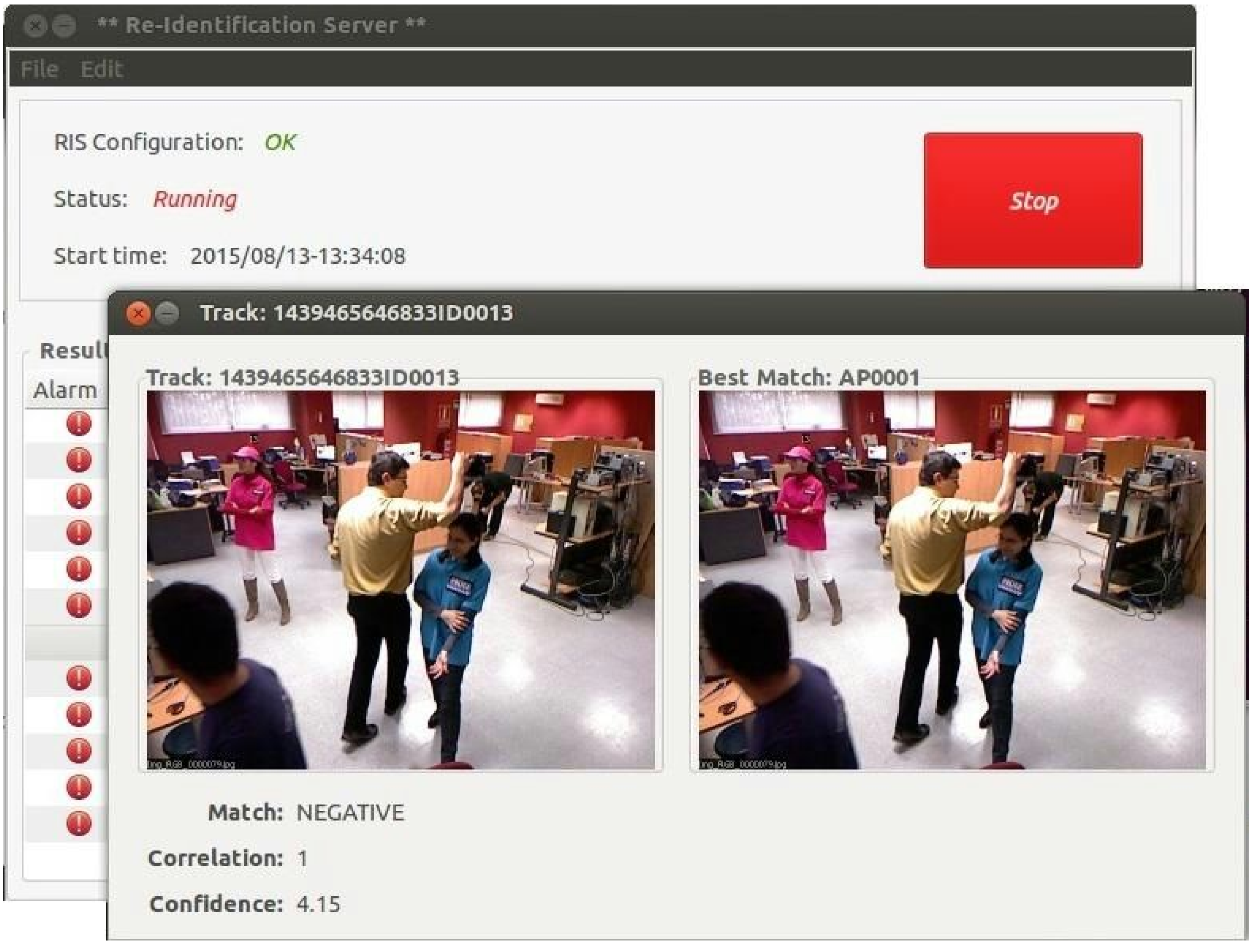
Area:
Main entrance

Matching Result:
Alarm

Figure 7: Non-Authorised access test, validation screen

3.2.1.2 Detection of authorized accesses

The detection of authorized access is similar to the detection of a non-authorised access. In this case if the person detected is recognized as one of the authorized persons, just the information of the event is sent to the RMS, in order to have the information saved in a log.



RIS Configuration: OK

Status: Running

Start time: 2015/08/13-13:34:08

Track: 1439465646833ID0013

Match: NEGATIVE

Correlation: 1

Confidence: 4.15

Figure 8: Authorised access test

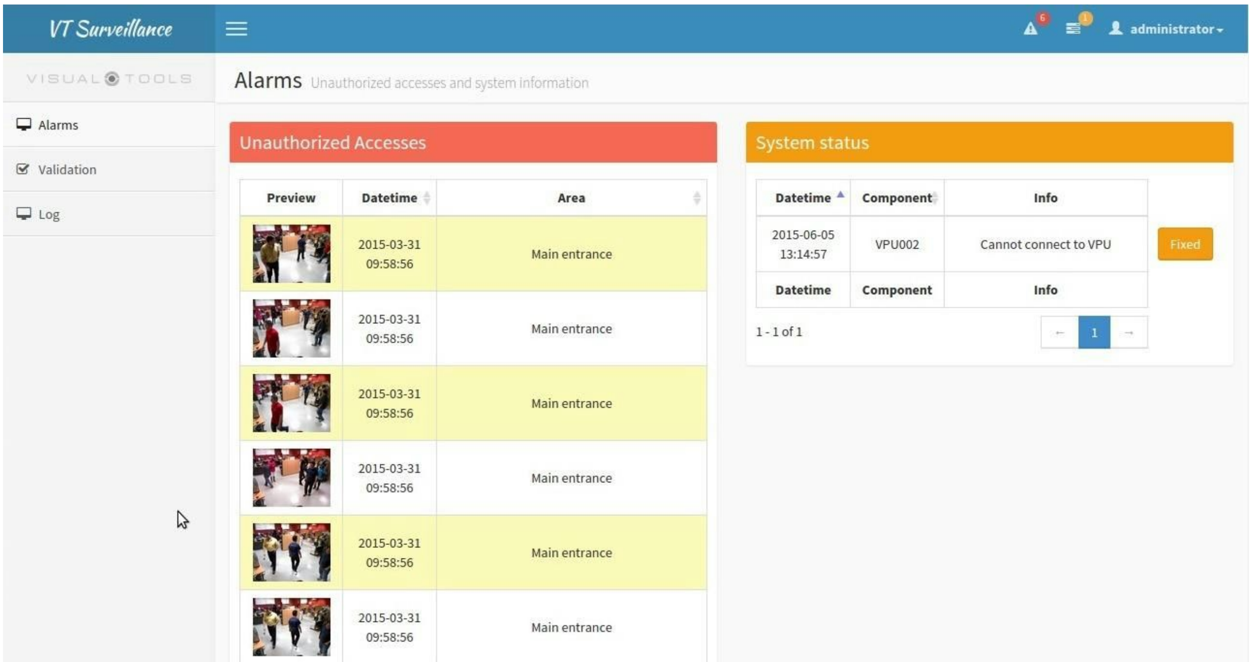
3.2.1.3 Surveillance User Interface

In order to improve the usability of the system, a web based user interface was developed. The idea was to make a system that allows to manage the alarms without the need of an extensive learning. Offering the operator the possibility of doing just 3 different tasks:

- ❖ Show Alarms
- ❖ Validate Alarms
- ❖ Show a log

Regarding to the display alarms, the main panel of the Surveillance UI shows the list of unauthorized accesses not verified yet, and also the list of system alarms informing of errors in the system that can cause the loss of data or functionalities. In both cases, the alarms are ordered by date/time, so the user can see first the most recent events.

Clicking in an alarm, the user 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.



Alarms Unauthorized accesses and system information

Unauthorized Accesses

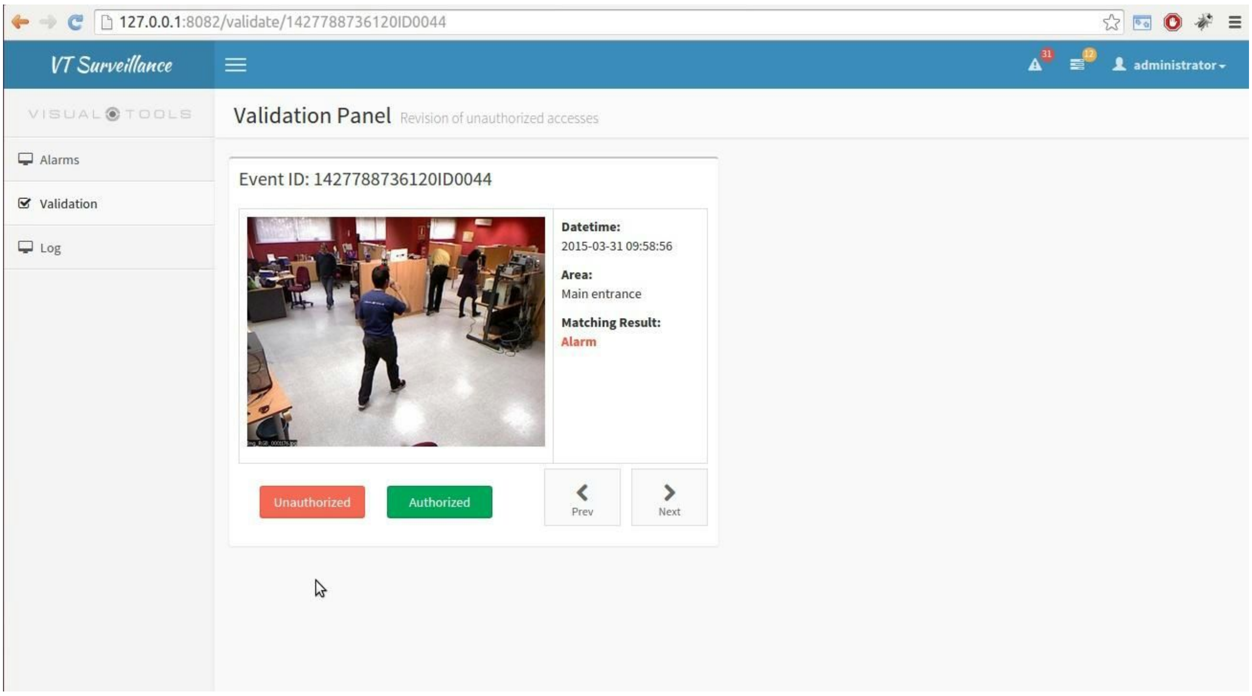
Preview	Datetime	Area
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance
	2015-03-31 09:58:56	Main entrance

System status

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

1 - 1 of 1

Figure 9: UI: Alarms



Validation Panel Revision of unauthorized accesses

Event ID: 1427788736120ID0044

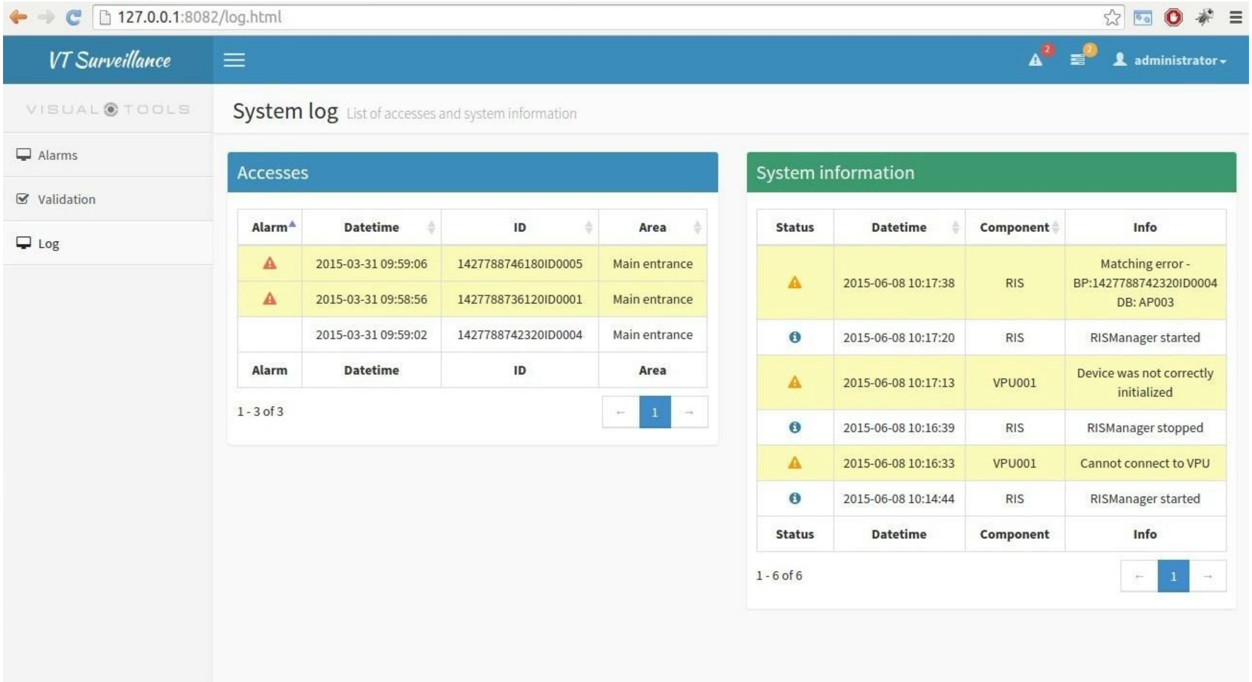
Datetime: 2015-03-31 09:58:56

Area: Main entrance

Matching Result: Alarm

Figure 10: UI: Validation Panel

VT Surveillance UI allows operator to access the system log in order to get a summary of the accesses to the system.



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 ← 1 →

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 ← 1 →

Figure 11: UI: System Log

After the test with the operators the overall opinion was that the tool was easy enough to use without need of special tutorial and that the tools provides a simple and intuitive way to check the alarm information.

3.2.2 Legal, socio-ethical, privacy & accountability aspects: Lessons learnt

In the evaluation of the added value of the SALT methodology, just as important as the provision of the adequate surveillance capabilities, is the fulfilment of the privacy and accountability concerns.

We have identified in previous deliverables of this Work Package 6 the main privacy and accountability concerns around the biometrics use case and scenario, and also a set of mechanisms and procedures that can be implemented to address those concerns.

Ideally, an external auditor should check that the artefacts implemented are really enough to address the concerns, and that they have been implemented correctly (not only quantity, but also quality), in this specific case, and as we are the ones proposing the solution, we have agreed to evaluate the SALT aspects in the form of lessons learnt.

Regarding the lessons learnt, one of the most important lessons, was related to the evolution of the privacy and accountability requirements. At it is stated in the D6.3, the requirements changed significantly from the initial list identified at the beginning of the project in D6.1, to the list of requirements obtained from the different evaluations carried out following the SALT approach. This was the result of lengthy discussions between Visual Tools, U Namur, INRIA and KU Leuven in order to bring the technical, legal and ethical perspectives together. Each discipline had a different understanding of the privacy risks created by the system. As a way of example, while the legal discipline viewed the use of bodyprints as a highly intrusive technology, the technical discipline was promoting this technology as having a low impact on privacy because the bodyprints only resulted in the capture of graphs. Similarly while the need to actively involve data subjects in the collection phase was paramount for the legal discipline, the convenience of use of the tool was put forward by the technical side. Several meetings were necessary to come to a mutual understanding and to agree on a list of measures that would lower the impact on the privacy.

Interesting enough, when the system was presented to the end users, they did not feel this system to be at all intrusive. Users were more concerned about the usability of the system and by the fact that it would not interfere into their work or their freedom of movement within the office. This might be explained by the fact that the end users consulted are employees of Visual Tool, thus engineers focused on the development of video surveillance technologies. In any case, this shows the importance of consulting stakeholders during the privacy by design process as the perceptions of the privacy concerns of a given technology might differ fundamentally between its users and the experts involved in the development process. This also highlights that it is often difficult to anticipate users' expectations based on the analysis of the sole technological features or of the legal framework.

Along the same lines, another lesson learnt from this experience is the importance of conducting a detailed and precise risk analysis in which all assumptions and contextual factors are taken into account. PIAs have become more and more popular during the last decade. However, if existing PIA frameworks and guidelines provide a good deal of details on organizational aspects, they are much less precise on the technical part. Considering their ever increasing role in privacy regulations and the critical need to characterize risks precisely, as exemplified by studies conducted in the PARIS project, PIAs should be defined at a higher level of rigour and be more precise with regard to the technical aspects of privacy risk analysis. This is a key requirement to ensure that their results are trustworthy, well understood by all stakeholders, and can be subject to independent checks.

Another of the basic lesson learnt when developing the biometrics use case is that SALT framework based design process strongly depends on the system development lifecycle used by the company producing the system.

During the overall cycle and in order to explain certain concepts, contextual help was provided, this was very useful to clarify at any moment of the development cycle the contents of the SALT References and to help understand when a given reference can be applied.

There were also some lessons learnt related to the viability, in particular on the importance to evaluate not only the cost of the solution but a several other factors (environmental constraints, ease of integration in the current procedures,...) which had huge impact on the overall solution.

On the validation phase, and thanks to the validation tools, it was possible to assess the privacy risks associated to design decisions using the Questionnaire for biometrics, which included most relevant privacy and accountability concerns related to biometric systems

3.3 Evaluation of the SALT Framework and the SFMT

As it is mentioned in the evaluation criteria of the project (D6.1) the idea was to specify a set of criteria in order to evaluate the SALT Framework. In the following subsections the criteria are listed and evaluated together with the instrument of evaluation.

3.3.1 Functional aspects of the SALT Framework

The SALT Framework shall provide all the capabilities required by the different users during the biometric system lifecycle, thus the first goal consists of evaluating if the SALT Framework includes all the functionalities needed. For this reason, one criteria was defined: "**The SALT Framework includes all the capabilities required during the design process**". The idea behind this criteria was to evaluate the usefulness and the functionality of the framework.

In order to validate this criteria we validated that the required tools and capabilities mentioned in the criteria were available. Once we verified that the tool for adding the specification and the tools for introducing in the SALT Framework the profile of a biometric system were available, together with the list of accountability and privacy references, we considered the functional aspects evaluated.

3.3.2 Data requirements

The second goal is to verify that the references provide the necessary concerns and recommendations about privacy and accountability, and that they are adequate to the system specified. In order to evaluate this three criteria were defined:

- Relevance of the references to the system specified
- Provision of concerns about accountability
- Provision of concerns about privacy

In order to evaluate this criteria we checked that the accountability and privacy references were available and they were relevant for the biometric use case.

3.3.3 Usability

The third goal was related to evaluating the usability of the framework, in particular the next three criteria:

- Accuracy of the references
- Ease of learning
- Easy of using

In order to evaluate these criteria a group a survey and questionnaires were developed and the feedback of a group of user was collected, a report of the biometrics questionnaire was also made. (see the demonstration documents "PARIS Biometrics Use Case SALT questionnaire" and "System Deployment and consultation of stakeholders" for more detailed information)

3.3.4 Evaluation of the SALT Framework and the SFMTF from the legal experts point of view

This section details The SALT Framework and the SFMTF as tools to support multi-disciplinarity and the traceability of the decision-making process from the KU Leuven layer's point of view.

In a Privacy-by-design process, the goal of the lawyer is first to ensure compliance with the applicable legal framework and to provide evidence of such compliance through accountability mechanisms. A second goal is to engage into dialogue with engineers in order to ensure the highest possible level of protection for data subjects' privacy through the design of the technology at stake.

In the context of PARIS, legal experts have assumed both the roles of "SALT experts", in charge of providing input to the knowledge base through the creation of references, and of "SALT users", when reviewing and actively discussing the answers provided by the engineers to the questionnaire. This means that the lessons learned during the project are most useful for lawyers that would get actively involved into the Privacy by Design (PbD) process and would like to use the SFMT as a tool to enable multidisciplinarity, in addition to allow the traceability of the decision-making process.

The two aforementioned goals that guide lawyers in a PbD process have informed the choice of the tools put at disposal of the user of the SALT framework:

- ❖ The creation of references is meant to provide the SALT users with the relevant legal provisions, i.e. the provisions applicable to the design of the system. It is thus purely informative but this requires the lawyer to make a first selection of the applicable legal framework. In WP6 use case, this meant to review the EU and the Spanish legal framework and select the most appropriate legal and policy documents. This thus required the knowledge of the Spanish legal framework, apart from expertise in privacy and data protection laws to be able to classify the different provisions into the list established to facilitate the search and understanding of the body of the law. The references are meant to support with raw information the questionnaire. The legal provisions are copied as is in order to avoid any interpretative bias from the legal expert.
- ❖ The building of a questionnaire that is both intended (1) to guide the SALT users towards legal compliance, pointing out to relevant issues raised by the system designed and/or aspects that should be integrated as functional requirements, and (2) to generate a reflexive process that will guide the SALT users to understand the logic of protection underlying the content of the legal framework. The addition of a questionnaire and recommendations to organize the consultations of relevant stakeholders, with a focus put on specific categories of more vulnerable data subjects

such as minors and employees, fully participates to the reflexive process in so far as it would allow to integrate other perspectives on the system than the ones of the (technical and legal) experts.

The application of the SALT Framework to WP6 use case allowed to identify five challenges specific to the SALT compliant process:

- The first challenge is to define precisely the contours of the case study, i.e. the key features of a given surveillance system that will trigger the application of a given set of legal rules. Legal documents and relative interpretative sources are so extensive that the lawyer should have a clear view of the possible impact of a given system. Under PARIS, as we started from scratch, preliminary discussions were necessary between the owners of the system (VT) and the lawyers (U Namur, KU Leuven) in order to identify the applicable laws. The purpose of the system, e.g. to detect intrusions or to identify people accessing the premises under surveillance might call the application of different provisions. The scope was further narrowed down to the focus of the project, namely privacy and surveillance. Additional provisions stemming from other areas of the Law, such as Labour Law, were excluded from the scope. Yet, the exercise remains long and tedious for the legal expert. Ideally, the exercise should become less necessary as the SFMT is used over time by one organization, as the content fed into the database grows.
- The second challenge is to be able to guide engineers through legal reasoning by the way of the order of the questions asked. This requires the lawyer to take some distance with its own reasoning to be able to make it explicit to a third party not trained into legal thinking. Designing a sound questionnaire requires time.
- The third challenge is to build a constructive dialogue between the lawyers and the engineers in order to clarify the misunderstandings that could arise from the answers given to the questionnaire. The exact goal of the question (i.e. the type of information expected) might not always be apparent to the engineer, or the way how to answer the question might be more complex than expected. As a way of example the exact definition of the purpose is key for the legal analysis. Much time was dedicated to discuss with VT in order to narrow down the definition of purposes. This required to go back and forth several questions (what is the purpose? Why is this information absolutely necessary? Aren't there any alternative means less intrusive for privacy?). Similarly, it might take time for the lawyer to get a precise understanding of the technology in order to fit it back into legal concepts. For instance, lengthy discussions were necessary for lawyers to understand which was the result of the analysis of the individuals' biometrics (verification/ identification/categorization) as this has an impact on the type of safeguards that should be put in place. It was made apparent that this dialogue was key to achieve both goals of legal compliance and ensuring a high level of protection as it helped creating mutual understanding. It was also key to generate a reflexive process, avoiding the risk of the "checklist" approach that had been discarded at the beginning of the project. At the end of the process both the engineers and the lawyers got a deeper understanding of the impact of the system to be deployed.

- The fourth challenge is to confront the design decisions to the opinion of stakeholders affected by the system. While the SALT framework cannot but recommend the organization of consultations, the feedback from these consultations should feed back into the process and be documented. This was done under WP6. In that case, none of the stakeholders consulted raised additional issues or concerns. The system could thus be deployed as resulting from the SALT compliant process. Documenting the consultations participates to the traceability of the decision-making process.
- The fifth and final challenge was to ensure the traceability of the decision-making process and thus the accountability of the different actors taking part to the process. It was agreed that the SFMT should allow each user to see the modifications made by the other users and would keep trace of the history.

3.4 Evaluation of the resulting SALT process

This section evaluates the SALT compliant process against the actual process used for design and developing WP6 biometric use case. The goal is to evaluate how SALT process can be applied to real world problem to take privacy and accountability into consideration during the system design phase. It should be noted that WP6 biometric use case is assumed to be built on a clean slate, i.e. we build a totally new surveillance system from scratch. This is different from the WP5 use case for surveillance data management lifecycle, where the focus is on the extended use of surveillance data and the technologies to enable such usage for law enforcement. Therefore, in our evaluation, we focus on the very early stage of a system lifecycle.

In D6.2 Biometric use case SALT compliant framework, the design process for the biometric use case is captured and elaborated. Most noteworthy is that the design process for the biometric system integrated the 3-stage process defined in the SALT framework.

The 3-stage process is illustrated in Figure 1. Some highlights of process is summarized as:

- **Stage 1 Intention.** The intention is evaluate the considerations and requirements regarding privacy and accountability from a broader based. The planned system needs to justify the necessity to implement the biometric technology, as well as to ensure the least intrusive approach is used for the planned surveillance goal. In this phase, a surveillance project should be terminated if it doesn't provide a faire balance of its purpose in terms of proportionality and beneficence. If the purpose is regarded as legitimate, the national legislations need to be reviewed to identify legal requirements. SALT framework questionnaires, or the questionnaire tool can be used to identify relevant aspect for this state.

- **Stage 2 Integration of considerations.** In this stage, multi-disciplinary requirements covering social, ethical, legal, and technical concerns regarding privacy and accountability are collected. In this stage, questionnaires from SALT framework can be used to assist designer to elaborate a system design to fulfill surveillance needs while addressing stakeholder concerns. System proposers and system designers are involved in this stage. SALT references in the SALT repository can be used for looking for relevant knowledge or existing design.

- **Stage 3 overall assessment.** An evaluation of the design in the previous stage should be assessed. The SALT framework use questionnaires that allow system designer to assess the overall system, with respect to its initial aims, and provides final checks of legal requirements and ethical and legal proportionality and opportunity. In addition, system owners are required to demonstrate their awareness of the impact of the surveillance system on privacy and data protection.

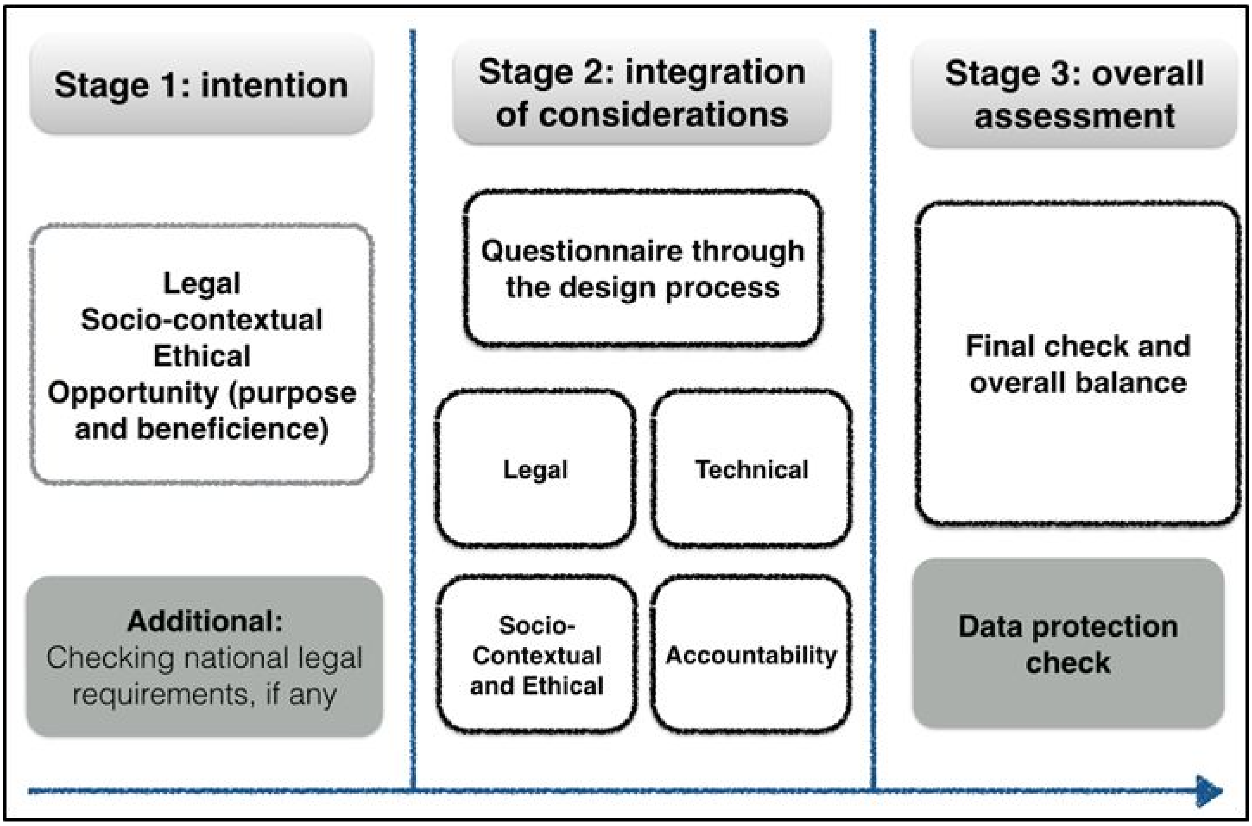

Stage 1: intention
Legal
Socio-contextual
Ethical
Opportunity (purpose and beneficience)
Additional:
Checking national legal requirements, if any
Stage 2: integration of considerations
Questionnaire through the design process
Legal
Technical
Socio-Contextual and Ethical
Accountability
Stage 3: overall assessment
Final check and overall balance
Data protection check

Figure 12: SALT framework 3-stage design process

The 3-stage can be regarded as a coarse-grained overlay of stages of common development lifecycle for system engineering, which match existing industry standard and thus can be integrated into existing engineering companies without with high chance of acceptance. The biometric use case demonstrated how the 3-stage process can be perfectly combined and integrated into partner VT's existing engineering process.

The adapted process is illustrated below.

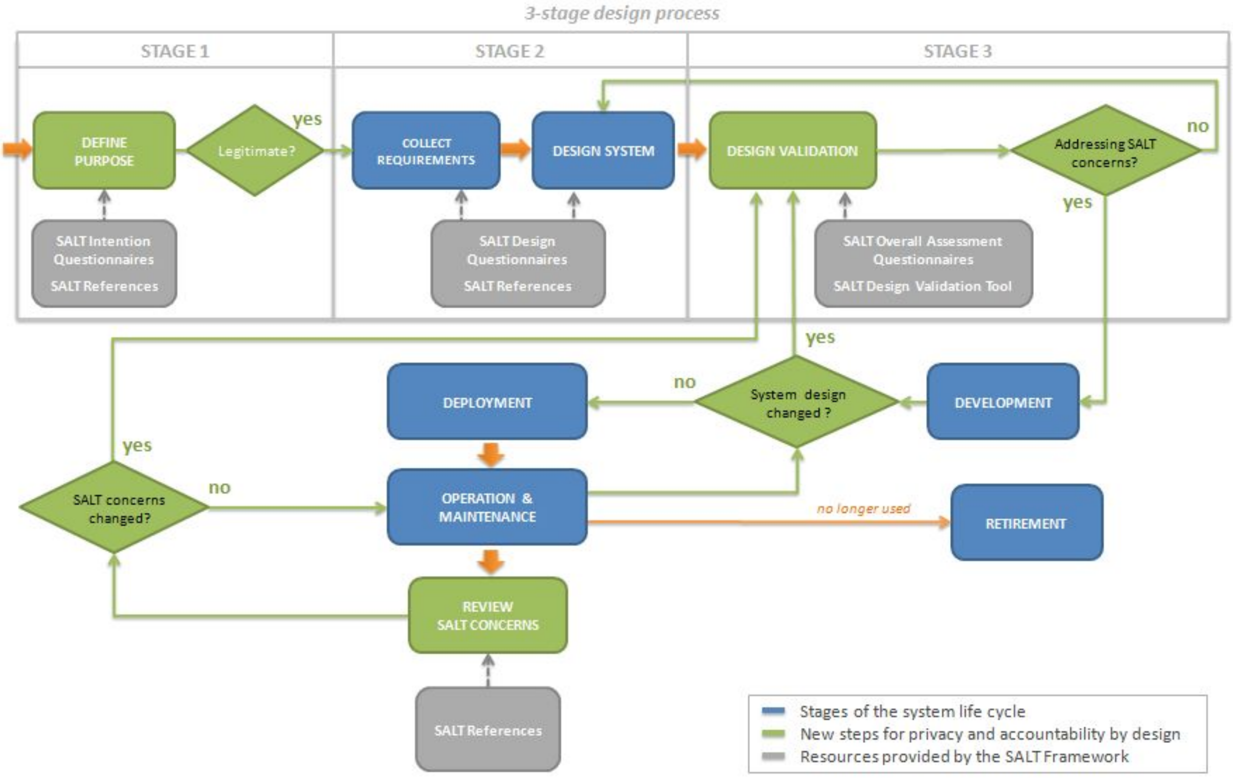


Figure 13: System development grouped under the 3-stage process

Based on the general 3-stage process, the existing engineering process for biometric system development (see Figure 13) is adapted to integrate privacy and accountability into consideration. The resulting “new” and privacy- and accountability-enhanced process is illustrated in Figure 4. The details of adapting existing industrial process to the 3-stage process and SALT compliant process are given in D6.3 “Biometric use case”.

Although we are aware that companies will be different in their adopted development methodology and the accompanied system development process, we believe the due to the broad applicability of the 3-stage process, it is feasible to combine and adapt the existing industry process for surveillance project to include privacy and accountability activities without incurring too much overhead.

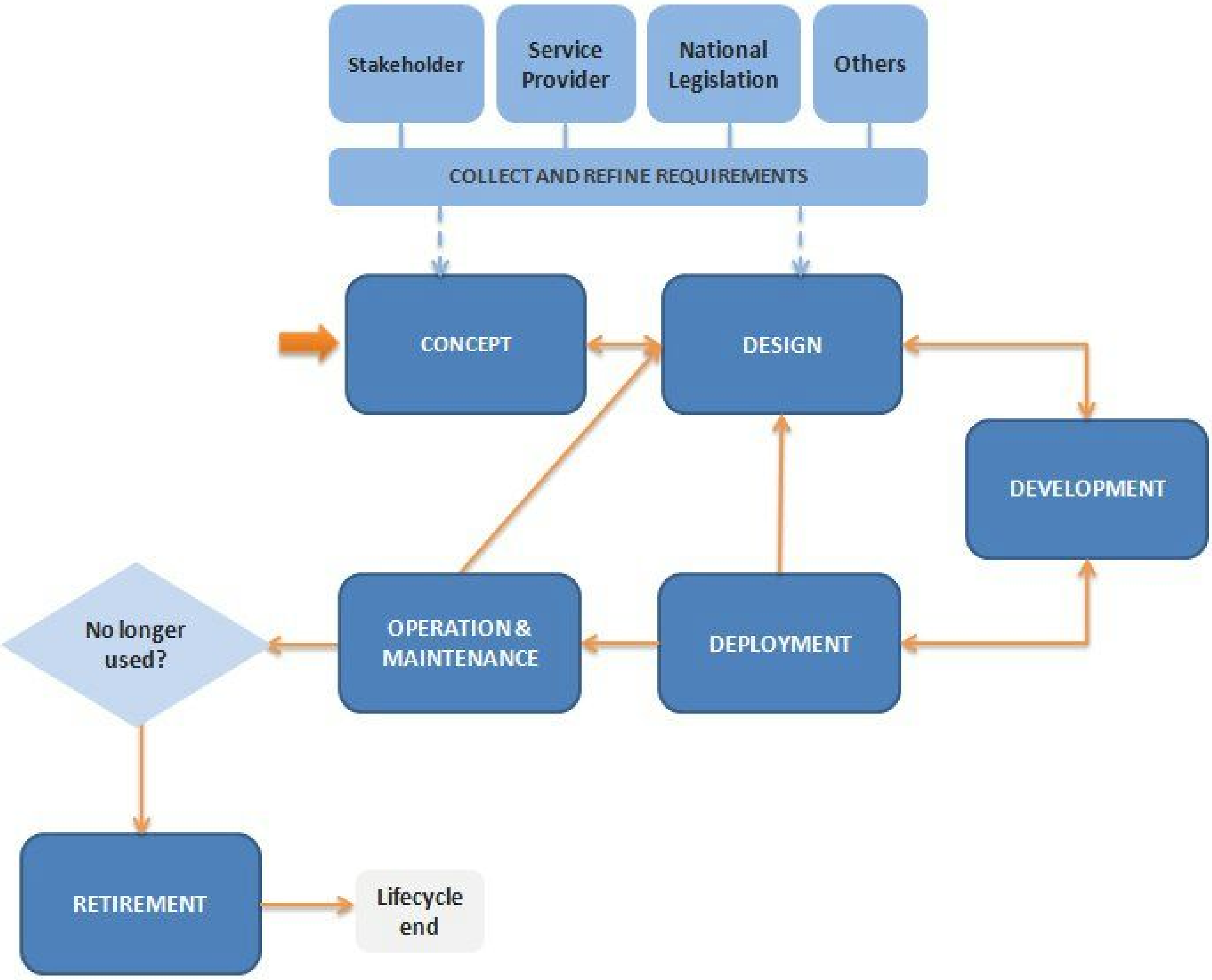


Figure 14: Engineering process at VT

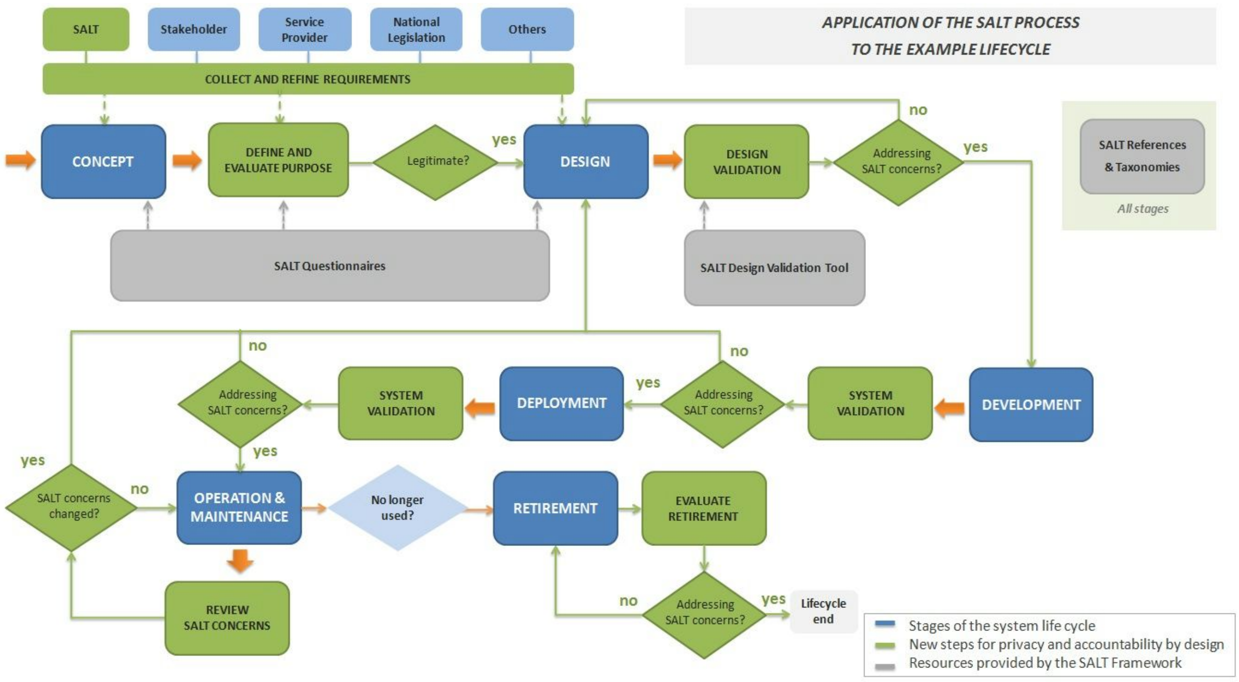

SALT
Stakeholder
Service Provider
National Legislation
Others
APPLICATION OF THE SALT PROCESS TO THE EXAMPLE LIFECYCLE
COLLECT AND REFINE REQUIREMENTS
CONCEPT
DEFINE AND EVALUATE PURPOSE
Legitimate?
yes
DESIGN
DESIGN VALIDATION
Addressing SALT concerns?
no
yes
SALT References & Taxonomies
All stages
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 15: New engineering process adapting SALT process

3.5 SALT Framework added value

For biometric systems, special attention must be paid to privacy and data protection aspects, from design to development in future implementations. Since biometric data is very sensitive and cannot be easily changed, privacy-preserving solutions are needed to avoid the misuse, loss or theft of biometric data. By adding activities in the design phase to review the privacy issues, the SALT framework can point to the blind spots of system engineers, who might not necessarily have all the privacy and accountability expertise, especially areas outside the technical domain, to be aware of the issues and interactively pinpoint the privacy issues in the design. The questionnaire can be re-used by all engineers involved in designing biometric systems, by accessing to the SALT repository. It should be noted that the added value is not only at the privacy protection, but also economical. SMEs, which are usually have the pressure of time-to-market and limited budget for having in-house legal consult, can utilize SALT framework while still integrating privacy and accountability in their designs.

Thanks to the SALT framework, together with the whole SALT methodology, companies and institutions with existing production processes regarding to surveillance systems have the opportunity to increase their efficiency (and even their productivity) in relation to the privacy and accountability issues inherent to this type of systems.

Those companies willing to adapt their existing processes by the adoption of the SALT methodology (or even introducing the SALT compliant process from scratch. See deliverable D4.4. "SALT Compliant Processes General Guidelines"), will benefit from a series of added values, which are the main objectives of the entire PARIS project.

The SALT compliant process provides a structured workflow that enables the monitoring of a given surveillance system from the very beginning of its lifecycle (starting at the concept stage) until its end with the system dismantling and retrieval. And not only that, but the adoption of the SALT compliant process ensures the user will know what to do, when to do it, and what tools to have at hand in order to provide a privacy-aware and accountability-aware surveillance system. The final output, will be what we called a SALT compliant system (see Deliverable D4.4. "SALT Compliant Processes General Guidelines" for more details).

The SALT framework is the body of knowledge gathering all the privacy and accountability information for surveillance systems. It is physically materialized in the form of a digital data base called the SALT repository, becoming one of the most important (if not the most) tools of the SALT methodology. Here we can find data relevant to surveillance systems that will be accessed during the different stages of the SALT compliant process. The use of this data, together with the appropriate tools ensures the achievement of privacy and accountability requirements that are not usually addressed in the design, implementation, deployment and operation of current surveillance systems.

4. Recommendations for extensions of the SFMT

Although the SALT framework and SALT compliant process include assistance on how to develop privacy and accountability for biometric system in the design phase, the current SALT framework does not include contents on how to protect a biometric system from security attacks. In other words, the “SALTed” biometric system might be able to ensure privacy by itself. However, it does not prevent malicious security attacks that compromise all privacy protection. For example, an attacker can inject malware into the system that steal credentials or sensitive information, and extract data from the system, such that all privacy consideration put in the place become useless. At attacker can target the general IT system or the biometric subsystem. Therefore, baseline information security considerations including technologies, design patterns, and procedures should be a part of the SALT framework for privacy.

Currently there are no effective means to conduct quality controls and verify the legitimacy of the content in the SALT repository. This should not be a problem if the repository is small. However, to be really scalable, tools must be designed to assist quality assurance, community-based validation of entries in the SALT repository. Another very important extension of SFMT will be to have tools that dealing with semantics of the text in the repository in order to index, sort, and resolve conflicting information and references.

Apart from the already mentioned ideas, below it is provided a list of possible extensions to the PARIS project that could be taken into account for future works,

- ❖ The creation of a "project space" in the SALT repository. This would be intended to store all the references, questionnaires and artefacts related to a single surveillance project. In this way, only accredited personnel for the given system would have access to this project space (authors of the system model, users of a given company, etc.).
- ❖ Establishment of a third party authority in charge of the validation of the contents to be added to the SALT repository: SALT references, questionnaires, taxonomies. This entity would ensure the quality and accuracy of each data gathered within the repository.
- ❖ Establishment of links with public authorities in order to ensure the correctness and regular update of all mandatory restrictions regarding surveillance systems and privacy, at least from the legal perspective. This would ensure that every SALT compliant systems is also fully compliant with the local laws.

5. Conclusions

This document takes into account and relies on all the work done in the project and it is in line with the rest of the deliverables of the WP6. 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 life cycle (Concept, Design & Development). In this D6.4 the focus is on the evaluation and results.

We were able to deploy the system at the Visual Tools' premises and to verify that the system behaves as expected in the targeted scenario, and we can say that in this proof of concept solved the stakeholder's problems, always taking into account privacy and accountability concerns.

We feel that all the fundamental requirements were met; this was validated thanks tothe development of the biometric use case all the artefacts linked to the requirements. Apart from this the meetings with the stakeholders and the questionnaires showed that the approach was valid.

Lessons have been learnt during the overall processes of the design/development of the system, for instance, the fact that the requirements changed significantly from the initial list identified at the beginning of the project. This is probably related to the new knowledge related to privacy acquired by the stakeholders.

Another lesson learnt is that SALT framework based design process strongly depends on the system development lifecycle used by the company producing the system, and the fact that the importance of solution is not only linked to the cost or to the privacy but to several other factors (environmental constraints, ease of integration in the current procedures,...) which had huge impact on the solution.

The impact due to the cost of implementing privacy requirements of the lack of knowledge on privacy aware systems could be reduced thanks to tools like the SALT Framework. After the usage of the Framework and SALT methodology, companies with surveillance systems have the opportunity to increase their efficiency (and even their productivity) in relation to the privacy and accountability issues inherent to this type of systems. We feel that this is one of the main added values of the approach.

We described also several possibilities for future work linked adding quality controls or the establishment of a third party authority in charge of the validation of the contents to be added to the SALT repository.

Overall, from the use case perspective it is believed that the SALT approach gave us an important overview of the privacy issues of our systems and helped us during the development.