PrivAcy pReserving Infrastructure for Surveillance

Deliverable D4.4 SALT Compliant Processes General Guidelines

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D4.4
Title:	SALT Compliant Processes General Guidelines
Version:	v1.0
Date:	22/12/2015
Confidentiality:	Public
Authors:	Antonio Maña (UMA) Francisco Jaime (UMA) Claire Gayrel (UNamur) Zhendong Ma (AIT) Mathias Bossuet (Thales) Christophe Jouvray (Trialog) María Saornil (Visual Tools) Daniel Le Métayer (Inria) Fanny Coudert (KU Leuven)

Funded by the European Union's Seventh Framework Programme

Table of Contents

Document History

Version	Status	Date
v0.1	Document structure and initial content	07/10/2015
v0.2	Addition of sections 1, 2 and 3	28/10/2015
v0.3	Addition of section 5.1	30/10/2015
v0.4	Addition of sections 5.4.1, 5.4.2 and 5.4.3	05/11/2015
v0.5	Addition of section 4.2 and refinement of section 5.1	19/11/2015
v0.6	Addition of sections 5.2, 5.4.4 and 5.4.5	09/12/2015
v0.7	Addition of sections 4.1 and 6. Document revised	11/12/2015
v0.8	Addition of section 5.3. Document revised	14/12/2015
v1.0	Final revised version	22/12/2015

Approval		
	Name	Date
Prepared	Francisco Jaime	22/12/2015
Prepared		
Reviewed	Zhendong Ma	16/12/2015
Reviewed	Daniel Le Métayer	18/12/2015
Authorised	Antonio Maña	22/12/2015

Circulation	
Recipient	Date of submission
Project partners	14/12/2015
European Commission	22/12/2015

Executive Summary

This document is the last deliverable of WP4 and provides the general guidelines for the final revised version of the SALT compliant process. Therefore, all stages within the process have been covered and detailed described, showing what to do and when to do it. Special attention has been given to the different types of users who can interact in a way or another with a surveillance system, providing a list of the different roles and their relations with the different stages of the process.

On the other hand, the SALT tools also have a prevailing place in this document, since they are an inherent complement to the SALT compliant process. Thanks to them, it is feasible to follow the whole process lifecycle from beginning to end. This document mentions not only the tools developed within the PARIS project, but also their usage.

The adoption of the SALT compliant process is another key factor for current companies who may already have their own engineering processes. This means that they have to undergo an adaptation process in order to fulfill the SALT compliant requirements. For this reason, several recommendations for the adaptation of current engineering processes to the SALT compliant process are provided. Two examples, corresponding to the two use cases defined within the scope of the PARIS project (video-surveillance and biometric systems) are described for a better understanding.

Finally, there is also a section covering the process validation from the point of view of the main artifacts and concepts surrounding the SALT compliant process: the conceptual framework, the two main objectives (privacy-by-design and accountability-by-design) and the developed tools.

List of Figures

Abbreviations and Definitions

Abbreviation	Definition
AbD	Accountability-by-Design
ADVISE	Advanced Video Surveillance archives search Engine for security application
DPIA	Data Protection Impact assessment
NVR	Network Video Recorder
OCL	Object Constraint Language
PAERIS	PrivAcy-by-design EngineeRing aSsistant
PARIS	PrivAcy Preserving Infrastructure for Surveillance
PbD	Privacy-by-Design
PIA	Privacy Impact assessment
SALT	Socio-contextual, ethicAl, Legal, Technological
SSP	Surveillance Service Provider
SUD	System Under Development
UML	Unified Modeling Language
VAS	Video Archive Search
WP	Work Package

1 Introduction

The works carried out within the scope of the PARIS project have led to the so-called SALT methodology. The application of this methodology ensures the integration of privacy and accountability aspects into actual surveillance systems (video surveillance and biometric systems), and hence several elements have been devised in order to support this methodology: frameworks, concepts, processes, tools, example use-cases, etc.

This document is mainly related to the workpackage 4 of the PARIS project and hence the SALT compliant process, one of the elements being part of the SALT methodology. The SALT compliant process has undergone changes and refinements since its first version created at the beginning of the project. During all this time, the process has evolved according to the needs and new features that have appeared as a consequence of the work carried out by all partners involved in the project. Different versions and revisions of the SALT compliant process have been provided in previous deliverables, with additions, eliminations and changes of features as required at each given moment.

Now, facing the last phase of the PARIS project, the PARIS consortium comes up with the final release of the SALT compliant process, where all requirements, constraints and comments raised during the whole project have been taken into account.

In the following sections we provide the general guidelines for the SALT compliant process, which mainly describes the action/work flow to be followed from the initial phases of a surveillance system to be, until its final deployment and operation (including maintenance) and eventually the system removal. If the guidelines attached to this process are followed, we state that the final outcome is a SALT compliant system (a concept coined by the PARIS project and whose definition is provided in Section 2.1).

The SALT compliant process is, together with the privacy/accountability information included in the SALT references, a key component of the SALT methodology, since it defines who can handle the methodology elements, how to handle them and at what stage of the process. This is crucial for the proper development of a surveillance system. In any case, apart from the process guidelines, there are more considerations of importance to be taken into account in the description of the SALT compliant process. The goal of this document is to present all these aspects in a synthetic way.

In Section 2, we provide the general process guidelines, but also considering the different roles/types of users who can interact with a surveillance system. Depending on the type of user, they will access the SALT compliant process at different stages, with different purposes and carrying out different actions in the lifecycle of a surveillance system.

Section 3 deals with the adaptation of current processes (from companies or institutions) to the SALT compliant process, providing relevant recommendations to help in this adoption.

Section 4 is the most practical one. Here we show how the SALT compliant process is applied to the two use-cases developed in the PARIS project: the first is a video-surveillance system and the second one a biometric system.

In Section 5 we consider the process validation. To accomplish this task, we show that the key concepts and elements of the SALT methodology are present in the SALT compliant process, i.e., the conceptual framework elements, the privacy-by-design, the accountability-by-design and the developed tools.

Finally, Section 6 concludes this document and the overall work carried out in WP4 and the SALT compliant process during the execution of the PARIS project.

2 Process adoption according to user profiles

We can see a user profile as a role or type of user/actor who interacts with the surveillance system in a way or another, depending on the category (profile) it belongs to. Each profile has a different objective and hence its relation with the system is different from the others'.

This section fully describes the SALT compliant process, providing the general guidelines in order to properly apply its workflow to an actual surveillance system. However, as described in Section 2.1, several user profiles interact with this workflow depending on the current process stage. Therefore, here we also provide (see Section 2.2) an analysis of who, when and how takes part in the SALT compliant process.

2.1 SALT compliant process

In order to properly understand the meaning of the SALT compliant process, it is important to have a clear view of its main goal: to integrate privacy and accountability aspects into nowadays surveillance systems, in particular into video-surveillance systems and biometric systems (the type of systems covered by the PARIS project).

Surveillance systems have typically focused in security as their primary objective, favoring system owner at the expense of the subjects under surveillance (normal citizens). Compliance with the legal framework or other policies has always been considered as external to the design process, thus often making difficult to come up with solutions that could fully take into account the privacy and data protection concerns raised by a given surveillance system. The concept of Privacy by Design has gained momentum and intends to tackle the issue. It however lacks tools for effective implementation in practice. And here is where the PARIS project comes in, developing a set of tools, concepts and body of knowledge, which help to add privacy and accountability aspects to nowadays surveillance systems.

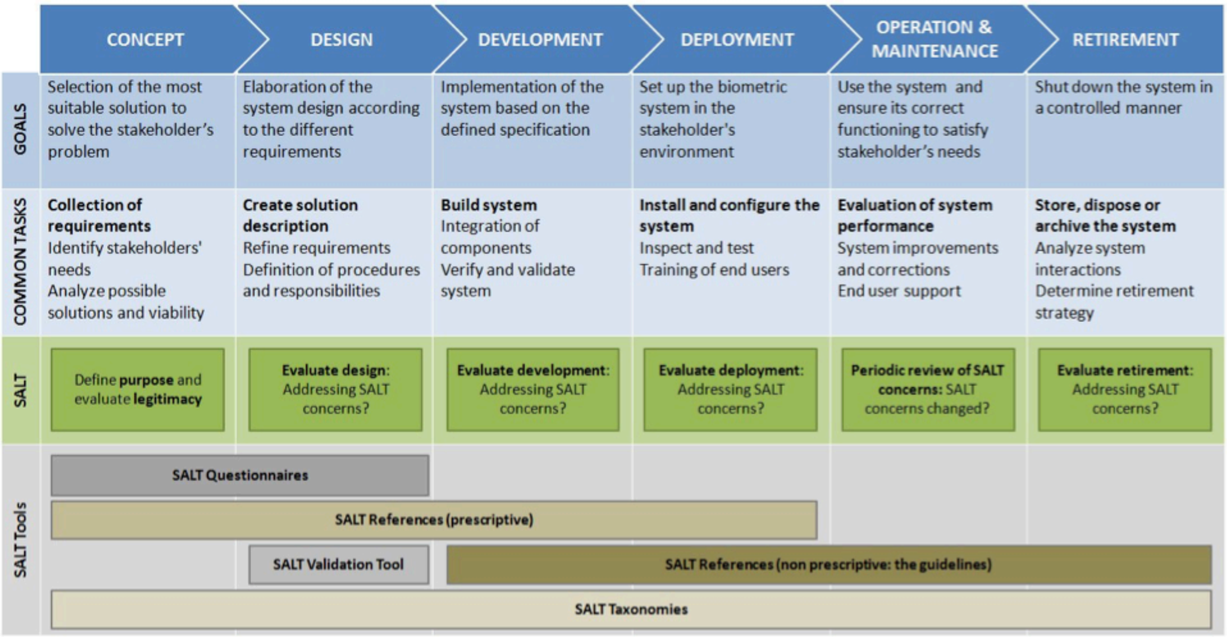
Among all this content, the SALT compliant process rises as a key element, since it provides the guidelines to follow for an adherence to a workflow that considers all stages during the lifecycle of a surveillance system, from the intention phase to the operation and eventual retirement of the system. Privacy and accountability aspects (issues, restrictions, recommendations, limitations…) are integrated in this workflow. This means that by following the SALT compliant process, new surveillance systems will be more privacy respectful (from the citizens point of view) and will also be accountable of the actions carried out during the system operation.

As a result of the use of this process, we obtain a "SALT compliant system". It is very important to fully understand the exact meaning of this expression because it is tightly bounded to the SALT compliant process. The understanding of it guarantees a complete understanding of the SALT compliant process' reason to be.

The SALT compliant process links with the SALT repository and the privacy/accountability information it stores. That information includes aspects from socio-contextual, ethical, legal and technological fields related to surveillance systems. It also includes a series of guidelines indicating how to take into account such aspects into the future system. By following the SALT compliant process, system designers get the chance of applying these guidelines into their system designs (they can also choose not to do that, but the process offers the possibility of doing it). Because of this, we can ensure that at least system designers have been made aware of the privacy and accountability concerns raised by the SUD (System Under Development) and they have also been provided with guidelines to integrate them into their systems. This is the foundation of a SALT compliant system.

Of course, the amount and quality of privacy and accountability aspects will depend on the quantity and the accuracy of the content stored in the SALT repository. It is logical to think that the repository contents will grow in size and will refine after years of operation, although the fact of following the SALT compliant process will lead to a SALT compliant system regardless the information gathered in the repository (whether the surveillance system was created at the beginning of the repository life, or after years of operation).

Therefore, now that we know the importance and the goals of the SALT compliant process, we can describe the general guidelines. In first place, let us keep in mind the lifecycle of a SALT compliant system and the different stages it goes through, since it matches the stages of the SALT compliant process. In Figure 1 we can see all stages of the lifecycle of a SALT compliant system, i.e., concept, design, development, deployment, operation and maintenance, retirement. These stages are also shown in the PARIS project deliverable D6.3, “Biometrics Use Case”.



	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 1. Lifecycle of a SALT compliant system

Figure 2 shows a general overview of the whole process, where each stage is identified according to the profile of the user that interacts with the system. As the graph shows, stages from Figure 2 correspond to stages from Figure 1:

- Concept stage: mainly performed by system proposers.
- Design stage: mainly performed by system designers.
- Development stage: mainly performed by system developers.
- Deployment stage: mainly performed by system installers.
- Operation and maintenance stage: mainly performed by system operators.
- Retirement stage: it may involve several user profiles, such as operators and installers.

- External auditors can perform system evaluations at any stage during the process.

It is worth noting that in real life systems we can have a same user sharing different roles, e. g. a system developer and a system installer could be the same person (just to mention a possibility).

Starting from the system proposer, this role is usually assigned to the system owner, although it could be any other stakeholder (it could be a company, a consortium, etc.). This is the user who initially has the intention of creating a surveillance system for given purposes. The first thing to do is to go through the questionnaires developed by the PARIS project (see PARIS project deliverables D2.2 “Structure and Dynamics of SALT Frameworks” and D2.3 “Guidelines for SALT Conceptual Frameworks”). Due to the legal dimension of these questionnaires, they should be reviewed by a lawyer in order to avoid a final illegitimate system. However, thanks to the existence of such questionnaires, this lawyer does not need to be an expert regarding data protection because the questionnaires will guide him with the appropriate questions. But in any case, it is highly recommended to use a lawyer to ensure a right usage of the questionnaires.

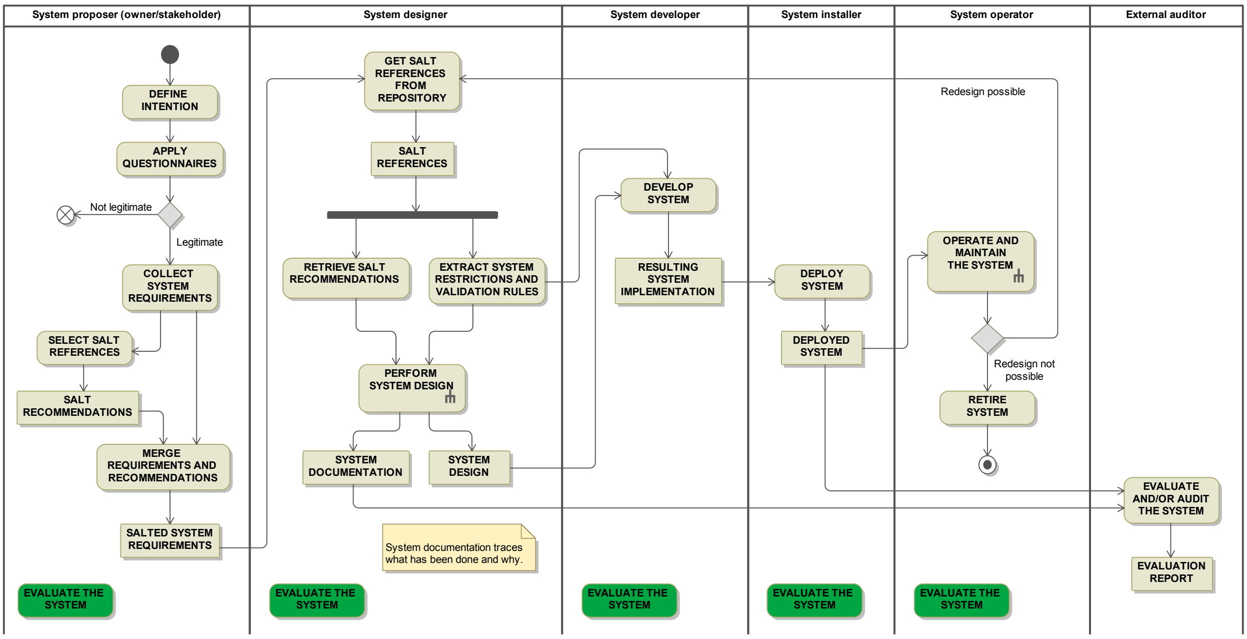


Figure 2. SALT compliant process overview

According to the results of the questionnaires the system proposer can get a first idea of whether the proposed surveillance system is legitimate (from a legal point of view) or not. In case the answers point to the fact that the system is most likely not legitimate, system proposers should revise the initial intentions/purposes in order to go through the questionnaires again. Otherwise, if, based on the answers given to the questionnaires, the result indicates the system is likely to be legitimate, the system proposer can go on with the SALT compliant process by collecting the system requirements. These are all functional and no functional requirements provided by the system proposer and those that might arise from the application of the questionnaires (though legal requirements may also be present).

The system proposer can also access the SALT repository and search for the appropriate SALT references applicable to the current surveillance system. The SALT references provide a series of SALT recommendations (see deliverable D6.3 “Biometrics Use Case” for a complete description of a SALT reference and its content), which together with the initial system requirements lead to the final SALTed system requirements, the input to the system design.

System design is the next stage of the process and it starts with the SALTed system requirements from the previous stage. However, since system designers may have a vision of a surveillance system different from the vision of the system proposer, it is also a good practice to access the SALT repository in the design stage and retrieve (possibly) new SALT references. All together, this process will lead to a set of SALT recommendations, system restrictions and validation rules (also extracted from the SALT references), all the ingredients needed to perform the system design, depicted in Figure 3.

The performance of the system design is based on the design restrictions and the recommended design artifacts (extracted from the SALT recommendations). Besides, the SALT compliant process allows for a system validation that is carried out in parallel with the system design thanks to a set of validation rules (actually, they are OCL rules) extracted from the SALT references. This means there is a secondary process (actually we might say it is a software procedure) always running in the background in charge of continuously checking the validation rules against the current system design. Whenever one of these rules is not fulfilled a warning/error message is displayed to the user, and hence he will know all SALT requirements have been met when no messages are shown. Finally, the system design will be complete once the designer decides all required elements have been taken into account. Nevertheless, let us not forget that the system designer always has the last word, therefore he can decide not to include some of the proposed SALT recommendations according to his criteria. In this case, the system designer must document these decisions in order to preserve accountability.

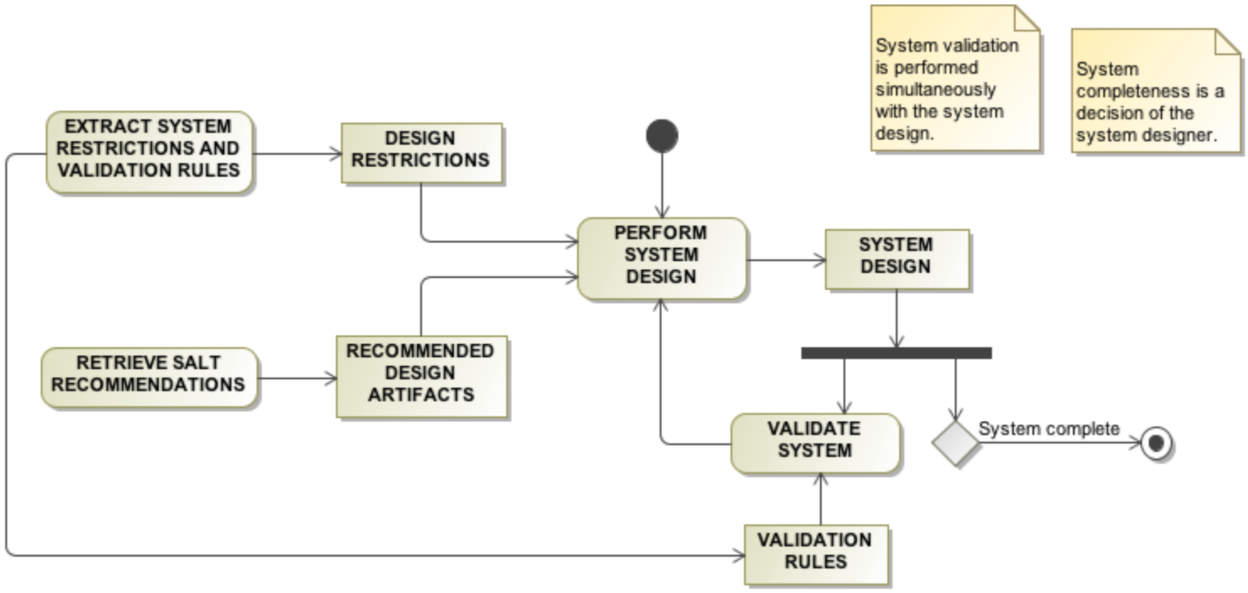

System validation is performed simultaneously with the system design.
System completeness is a decision of the system designer.
EXTRACT SYSTEM RESTRICTIONS AND VALIDATION RULES
DESIGN RESTRICTIONS
PERFORM SYSTEM DESIGN
SYSTEM DESIGN
RETRIEVE SALT RECOMMENDATIONS
RECOMMENDED DESIGN ARTIFACTS
VALIDATE SYSTEM
System complete
VALIDATION RULES

Figure 3. SALT compliant process: System design

As a result of this stage, we get the system design (typically in the form of a UML model) together with the system documentation. This documentation provides information related to how the system has been modeled and why.

System development comes next, given the system restrictions and the system design generated in the previous stage. Here we get an implementation regarding the software and hardware involved in the surveillance system. Following we can continue with the system deployment, physically installing all the components in their right locations. At this point the surveillance system is ready to be used, that is, operation and maintenance take place.

Figure 4 shows a diagram explaining the operation and maintenance subprocess. Apart from the normal system operation, we have two other operation-flows. The first one periodically checks whether the SALT references used by the system design are still up to date or outdated. If they are up to date, the system operation carries on normally (at least until during the period until the next references checking), whereas the operation halts if some SALT reference happens to be outdated. In this case, the process goes back to the design phase in order to retrieve the new versions of the SALT references and update the system accordingly (see Figure 2). The second operation-flow relates to the system maintenance. Each time a maintenance event arises, the system operation continues normally if the system design remains unchanged. However, analogously to the SALT references update process, they system will go back to the design phase when its design is somehow modified. If for some reason a system redesign is not possible (but needed due to the SALT references changes or the maintenance events), then there is no other possibility but to retire the system.

The next phase of the SALT compliant process is dedicated to evaluate and/or audit the surveillance system (although an undefined amount of audits can be carried out and at any stage of the process, as depicted by green boxes from Figure 2). This task is based on the physically deployed system, together with the system documentation generated in the design phase. As a result, we get an evaluation report.

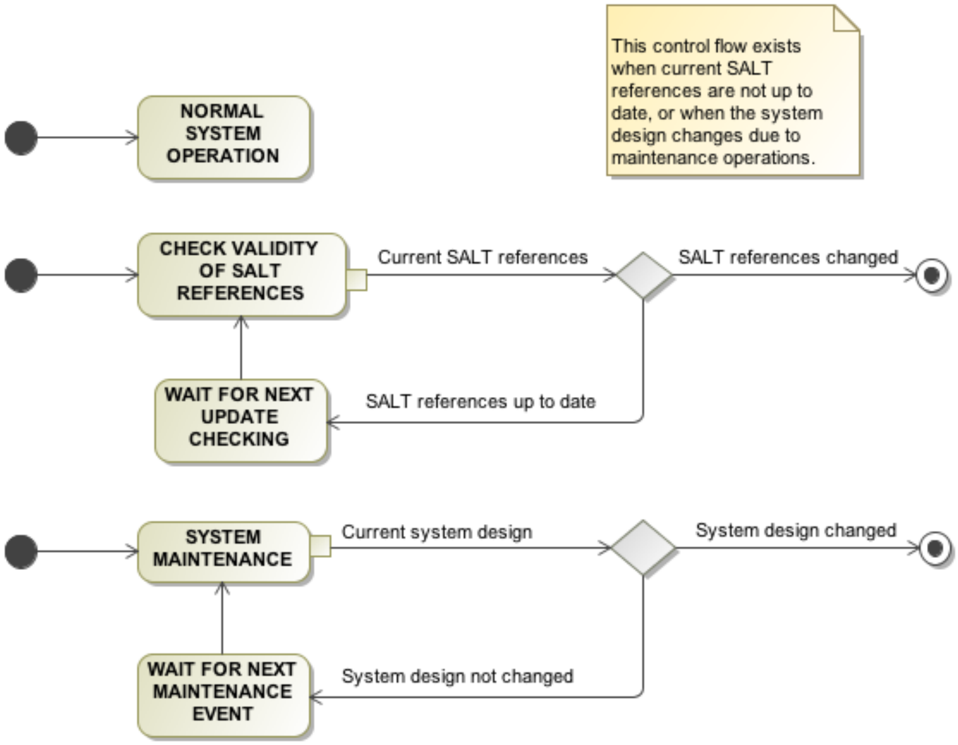

This control flow exists when current SALT references are not up to date, or when the system design changes due to maintenance operations.
NORMAL SYSTEM OPERATION
CHECK VALIDITY OF SALT REFERENCES
Current SALT references
SALT references changed
WAIT FOR NEXT UPDATE CHECKING
SALT references up to date
SYSTEM MAINTENANCE
Current system design
System design changed
WAIT FOR NEXT MAINTENANCE EVENT
System design not changed

Figure 4. SALT compliant process: Operation and maintenance

Moreover, having a look at Figure 2, we can see that it is also possible to evaluate the system at each stage, not only in the last one. This evaluation is intended to be from a privacy point of view. SALT references that can be used at a given stage could also be used to perform this evaluation.

It is also remarkable the fact that not only engineers, but also lawyers should be involved in the whole SALT compliant process from the beginning to the end. Besides, some phases of the process could be skipped if they have already been carried out in the past in another instantiation of the process.

2.2 *Different types of users*

This section analyzes the different user profiles (roles) that can interact with the SALT compliant process, at what stage, what inputs they expect and what outputs are going to be generated once the stages they are involved in are finished. How a user sees the process (and hence, the surveillance system) and what type of interfaces they are going to have, will heavily depend on their profiles.

2.2.1 System proposer

This is the user who initially propels the surveillance system. It usually is the system owner, but it could also be any other type of stakeholder interested in the creation of a new surveillance system.

The system proposer is usually involved in the concept phase (also called the intention phase in previous deliverables of the PARIS project), but since the proposer commonly provides the funding, he may also appear in other stages, at least for information.

Due to its nature, this type of user does not require any special input (apart from his own intention, purposes and desirable functionalities for the surveillance system to be), although it is actively involved in the first phase of the questionnaire (assessing the opportunity of the system). The system proposer also decides to what extent he wants to involve stakeholders in the process and organises consultations. In other words, the system proposer is an active role any time a decision that is not purely technical or related to the design has to be made (political decisions). After his participation in the process we get very important outputs: the initial system requirements and recommendations. This output does not only come from the proposer intention and requirements, but also from the interaction with some of the SALT tools developed within the project, mainly the questionnaires and the SALT repository.

Answering the questionnaires requires the collaboration of a lawyer (or any other person with legal expertise), since its content is mainly oriented towards the legal viability of the surveillance system. Thanks to these questions the system proposer knows whether the intended system may be legitimate or not, in which case some modifications and/or restrictions will have to be applied depending on the initial purposes and requirements. Then, he can connect to the SALT repository that will allow him to search for SALT references relevant to the current surveillance system. These SALT references will provide additional requirements and recommendations related to privacy and accountability concerns. All the system requirements and recommendations together are the outputs of this process phase.

2.2.2 System designer

This user is a technological expert in relation to the type of surveillance System Under Development (SUD). Obviously, system designers are part of the SALT compliant process during the design phase, and hence they receive the system requirements and recommendations generated during the concept phase. This information will be their starting point, although it may be expanded with new restrictions and recommendations coming from SALT references.

System designers are provided with an interface to access the SALT repository and search for new SALT references. Due to their knowledge of the surveillance technology, they may get some references that were unnoticed for system proposers, but still relevant to the SUD.

Thanks to the SALT methodology, system designers have a couple of tools to help them create the system design. The first one is an UML profile with a set of predefined elements specifically intended to create surveillance systems models (video surveillance and biometrics), whereas the second one is an automatic validator that works in parallel with the system designer while he creates a system design (an UML model) with the UML profile.

SALT references obtained from the SALT repository have some OCL rules included. System designers can ignore them, they do not even need to know about their existence. However these rules will be used in the background by the automatic validator. Each time a rule is not fulfilled, meaning the restriction/recommendation given by its corresponding SALT reference has not been addressed, the automatic validator will show a message to the system designer. These messages remain noticeable until the designer addresses its corresponding concern (from a SALT reference) or until he deactivates it. There are several levels of messages depending on the OCL rule/concern severity: error, warning, info.

It is important to remark the possibility of the system designer to ignore the restrictions and recommendations from the SALT references, and even the possibility to deactivate the error messages generated by the automatic validator. This fact demonstrates the objective of the SALT compliant process: **to help** in the creation, use, maintenance and removal of a surveillance system, taking into account both surveillance requirements and privacy and accountability concerns. However, the user (system designer in this case) always has the power to take the final decision (he may ignore a given SALT recommendation because, due to his experience, he knows a better way of addressing a concern than the proposed one). In such a case, the system designer is also responsible for providing documentation regarding the decision taken, thus we can keep a traceable system.

As a result of the system designer actions, we get a system design at the end of the design phase. This design is materialized with an UML model, together with relevant documentation regarding the design process, the decisions taken and how they have been implemented.

2.2.3 System developer

System developers are in charge of the implementation of the hardware and software components of the surveillance system. Many elements will directly come from a given manufacturer: cameras, recorders… although some other will have to be created or specially customized for a particular system. This elements customization is typically achieved via software, however hardware development cannot be discarded.

Therefore, it is clear that system developers enter the SALT compliant process at the development stage. They receive the UML model from system designers, together with the system restrictions, and they provide a system implementation. This implementation also requires a testing/validation team to ensure a correct functioning of the system. This means that at the end of the development phase, all system elements are physically created and ready to be deployed in their final location.

The tools and interfaces used by this type of users have not been considered by the SALT compliant process. Each user (company, association, organization…) will use those tools better suited for each situation: a given company may strongly recommend (enforce) the use of a particular programming language, a particular development framework, etc. to their employees.

2.2.4 System installer

The system installer belongs to the deployment phase of the SALT compliant process. The installer receives all elements implemented by the system developers in the previous phase and physically deploys them in a given environment, making all the required connections between components and producing as a result the final surveillance system, ready for operation.

This is mostly a physical task, hence system installers do not need to use any of the SALT tools provided by the SALT methodology.

2.2.5 System operator

The system operator interacts with the operation and maintenance phase of the SALT compliant process, hence system operators carry on two main tasks: normal operation of the surveillance system and maintenance (see Figure 4). Because of this, it is clear that their input is the deployed surveillance system provided by system installers, whereas they do not produce any concrete result, besides those obtained from the system operation.

Besides, periodical system maintenance events may occur, where operators will have to check the correct functioning of the system and apply corrective methods when necessary. It may also happen that system operators detect the need of a change in the system design during a maintenance event, or they may even realize that initial SALT references used to create the system are not valid anymore (their validity period has expired, a new version is available, etc.). In both cases, system operators may revert to the design phase of the SALT compliant process, where system designers will handle the issues raised during the system maintenance in order to update the system design.

The interfaces used by system operators within the SALT compliant process heavily depend on the type of surveillance system, together with each operator task. They can use a screen to monitor a camera, use filters and search algorithms within a NVR, use some kind of biometric device to ensure the control access at a given location, etc.

2.2.6 External auditor

As it can be seen in Figure 2, each phase of the SALT compliant process allows for the possibility to evaluate the system. An evaluation within a given phase is usually performed by the user profiles directly related to that phase: the evaluation of the design phase is performed by system designers, the evaluation of the deployment phase is performed by systems installers, etc. However, even though this is the most common case, it does not have to always be in this way. These evaluations can also be performed by users with different profiles and in many cases they are carried out by dedicated teams.

In any case, the external auditor is a profile different from all others. The auditor can also evaluate the system at each phase of the process (if he has the appropriate knowledge to do so), but this role is focused to an evaluation and/or audit of the surveillance system at the end of the SALT compliant process, that is, during the operation and maintenance phase (he can also audit that the system is properly retired when it is no more needed).

To accomplish this task, the external auditor obviously needs access to the deployed system, but also to the system documentation gathered during the design phase and the logs produced by the system during its operation. With this information, the auditor knows what design decisions have been take, why, and how they have been implemented in the final system. Then, he can verify this information against the actual system and its logs. Of course, the information provided by the SALT compliant process may not be the only information used by an external auditor, he might also use some information regarding policies, procedures, etc. from its own auditing company.

As a result of this task, the external auditor will provide an evaluation report with the conclusions and results he gathered throughout the system evaluation.

3 Adaptation to a SALT compliant process

This section provides guidelines for the adaptation of current processes from actual companies in order to adopt the SALT compliant process described in Section 2.1. This step needs to be as straightforward as possible, since any unnecessary overhead regarding this adaptation will drive companies away from using not only the SALT compliant process, but the whole SALT methodology.

Moreover, since each company may have its own process, the adaptation to a SALT compliant process will differ from one company to another. Therefore, we cannot not provide and algorithm or a step-by-step method to follow in order to achieve this adaptation, although we can provide a set of recommendations to facilitate the transition.

3.1 Recommendations to adopt a SALT compliant process

We provide a list of recommendations and guidelines for the adoption of a SALT compliant process. We assume an actual process is currently being used and it is going to be adapted to the SALT compliant process. In case an original process does not exist, but still the SALT methodology wants to be adopted, then a first step could be using the SALT compliant process previously defined in Section 2.1. After a period of operation, this process could be adapted to the company particularities.

- Have a list, schema, diagram or any specification of the current process of the company, indicating the steps the workflow has to go through.
- Make a comparison between the current process and the SALT compliant process.
- As a result of the previous comparison, find a correspondence between the stages of the current process and the stages of the SALT compliant process. Some of the stages may perform the same tasks and some other can be totally different (of course, this will depend on each particular case).
- It should be easier the addition of stages of the SALT compliant process into the current process than the other way around (inclusion of stages into the SALT compliant process).
- Even though the order of the stages in the SALT compliant process is rather logical and most of existing processes will follow it, this could not be always the case. If that happens, the company should put some effort in adapting the order of the process workflow.
- It is a good idea to divide the current process specification into as much subtasks as possible. This will help to make a correspondence between processes and fuse them into a bigger stage if it matches with another one from the SALT compliant process.
- Integrate the SALT tools, which are required by the SALT compliant process, into the set of tools of the company.
- Make an evaluation of a possible gradual adaptation of the process. If the cost to do it is admissible (in terms of money and time), the company should consider doing it that way. A gradual adoption will make it easier for every user related to the process.
- Users of the adapted SALT compliant process should receive specific training regarding the new process lifecycle and the involved SALT tools.

- The company can perform a study to decide whether the aforementioned training can be carried out in parallel with the process adaptation (and hence reducing time and cost) or not.
- It is also recommended to study and evaluate the different possibilities regarding the SALT repository (where privacy and accountability information is stored). Is it more convenient to have a private or public repository? What kind of storage better fits the company needs, distributed or centralized? Should we have different access levels (authorizations) to information depending on the user profile?
- The company should also check that the adoption of the SALT compliance process does not interfere with any other standard already in use. In case this happens, the company must evaluate the pros and cons of both approaches and decide which one yields them a better benefit.

4 Practical application to use cases

This section provides a description regarding how the SALT compliant process has been adopted and applied to two realistic use-cases in the scope of the PARIS project.

4.1 Use of a SALT compliant process for a video surveillance use case

This section is dedicated to a quick overview of the lessons learnt about the SALT process in the frame of the WP5 use case of the project ("Video Surveillance Lifecycle management use case").

This section addresses the SALT process from a global point of view, and also from the SALT tools point of view (as they support the SALT process itself). Some more elaboration about the SALT usage and SALT tools and process feedbacks can be found in the deliverable D5.4 of the project ("Video Surveillance Lifecycle management use case evaluation").

4.1.1 SALT process followed within the WP5 use case

The standard design process proposed within the frame of the PARIS project is described in Figure 1 and Figure 2 above in this document; the main steps at stake during all the phases of the lifecycle of a security system are identified in these generic process.

The WP5 use case proposes an interesting variation compared to this standard process as it addresses the modification of an existing video-surveillance system, rather than its definition, design, development, ex nihilo.

For this reason, the SALT global process has been a bit adapted to handle the WP5 use-case, as shown in **¡Error! No se encuentra el origen de la referencia.**.

An "Analysis" phase has been added to point out that the first task to perform in this case is a review and audit of the system. Then the most classical steps are performed to handle the modifications and upgrades required on the system (mainly the addition of video-lifecycle management capabilities and of a Video Archive Search module with a dedicated front-end for access management).

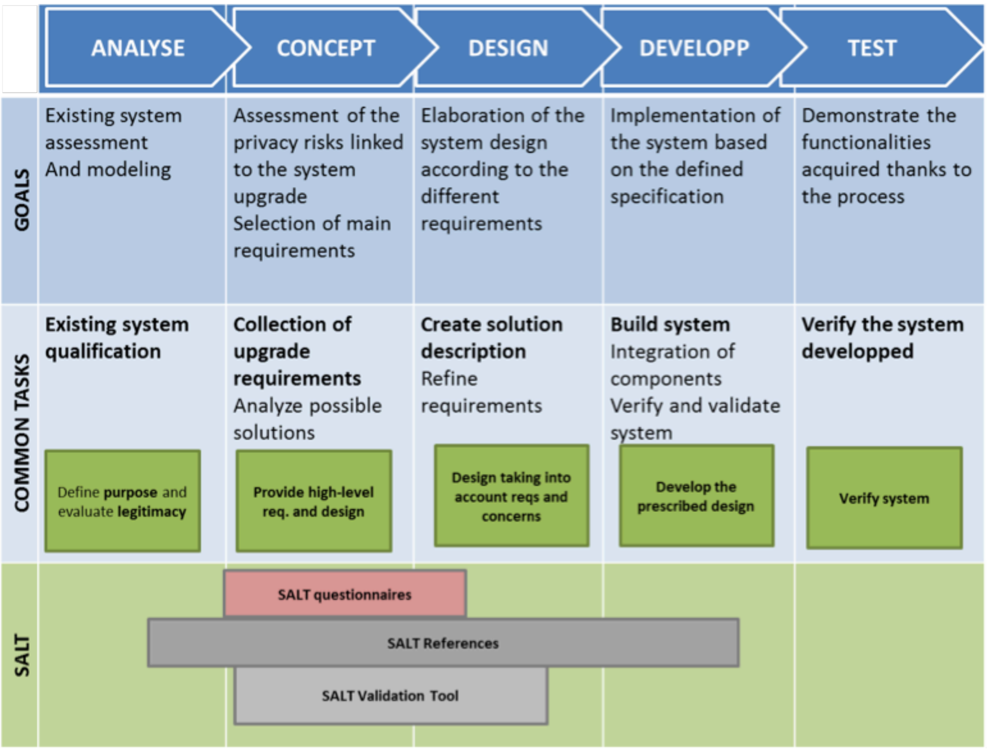
Fortunately, the PARIS process main steps and supporting tools (SALT taxonomies, SALT questionnaires, SALT references and the SALT validation tool) are sufficiently generic and adaptable to be used in this modified process.

This flexibility appears to the WP5 partners of primary importance because the process to be followed is very often a bit different for the possible following reasons:

- The existence within organizations of processes that preexist (large organizations like Thales decide and implement their own processes based on best of the breed practices and tools and also to the exact nature of systems that make their core activity).
- The fact that in many cases the development process is based on modern engineering and coding techniques which can be much less sequential compared to a simple "V-Cycle" standard linear process : extreme programming, agile processes are examples of processes more and more spread within the industry (for their increased productivity

and adaptability) which are based on iterations of the whole conception, development and test cycle.

- In most of the cases, the responsibilities and stages described in the SALT process are shared between several organizations, which can be very different in their size or location. Standard sharing of the tasks on a big size surveillance project may at least imply:
    - The organization that will run the system.
    - The organization that will act as prescriber of the system.
    - A consulting company who will partially issue the specifications.
    - A company that develops and installs the system.
    - A company that maintains the system.



	ANALYSE	CONCEPT	DESIGN	DEVELOPP	TEST
GOALS	Existing system assessment And modeling	Assessment of the privacy risks linked to the system upgrade Selection of main requirements	Elaboration of the system design according to the different requirements	Implementation of the system based on the defined specification	Demonstrate the functionalities acquired thanks to the process
COMMON TASKS	**Existing system qualification** Define **purpose** and evaluate **legitimacy**	**Collection of upgrade requirements** Analyze possible solutions **Provide high-level req. and design**	**Create solution description** Refine requirements **Design taking into account reqs and concerns**	**Build system** Integration of components Verify and validate system **Develop the prescribed design**	**Verify the system developped** **Verify system**
SALT		SALT questionnaires SALT References SALT Validation Tool			

Figure 5. Adaptation of the SALT process within the WP5 use case

An example of another process is given by Thales internal development process which can rely on standard waterfall cycle as well as on agile cycle (an example of this is proposed in Figure 6, from a Thales internal document "adoption of agile technology within Thales").

The agile development cycle as described here is very different from the standard linear waterfall cycle; it appears nevertheless that it is easy to use the SALT tools within this process to make it a "SALTed" or "SALT compliant" process.

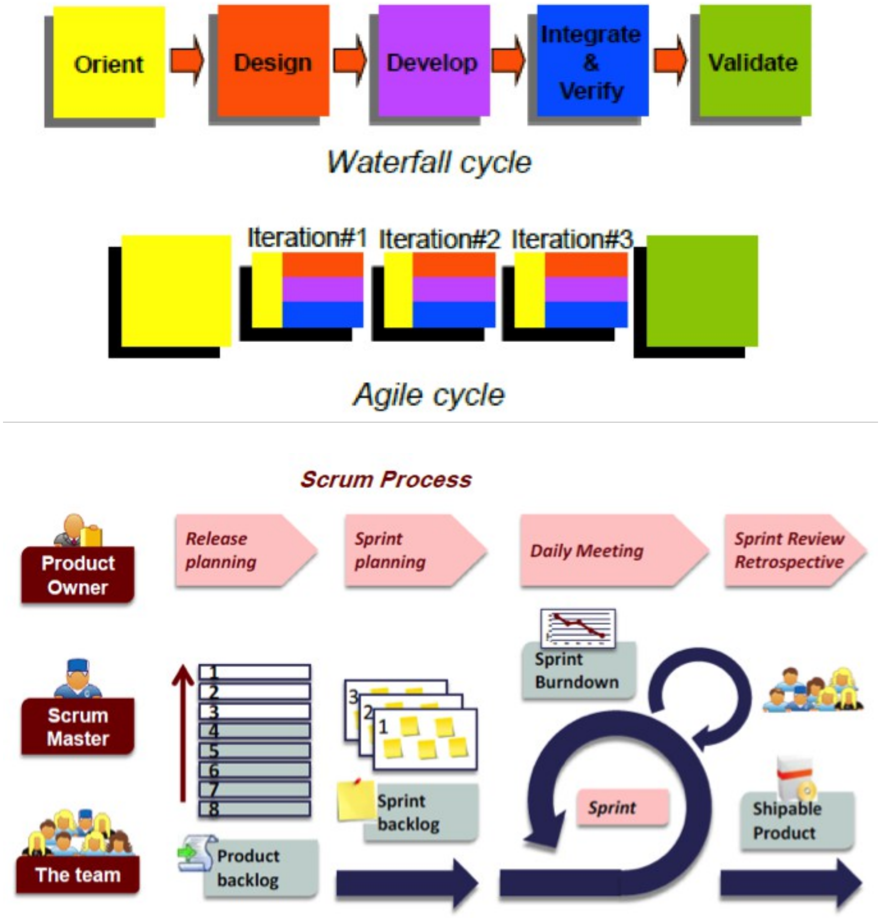


Figure 6. Waterfall and agile development cycles in Thales company

4.1.2 Use of SALT tools within WP5 as support to SALT process implementation

WP5 has been the opportunity to provide a concrete example for the use of the SALT tools, which are the pillars for the concrete implementation of the SALT process. SALT tools can be simply presented as shown in Figure 7.

SALT tools used within WP5 use case approach:

- SALT questionnaires.
- SALT taxonomies.
- SALT references.
- SALT modeling and validation tools.

Within WP5 use-case, the questionnaire is expected to provide some feedback and analysis about the system already in use (video-surveillance management and recording system) and to help specifying some new features (video archive search). The Privacy Impact Assessment (PIA) questionnaire from the ADVISE FP7 project is adapted to these needs and fully reused using the SALT management tools. It is noticeable that this has been performed without any limitation due to the tool itself.

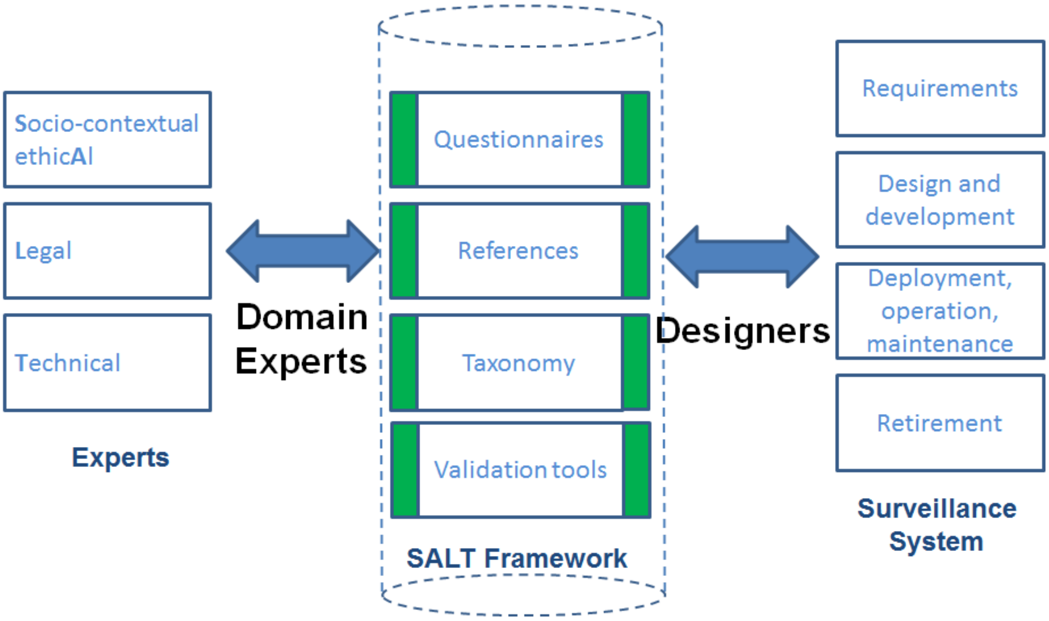


Figure 7. Overview of SALT tools within their ecosystem

The taxonomy tools provided by the SALT framework have been used to provide general awareness about the domain of application (video surveillance), by defining in a simple way some technical words from the domain.

WP5 has also been the opportunity to build many references from the three SALT points of view (Legal, Socio-Ethical, Technical) and to enter them within the SALT framework thanks to the SALT tools. Also, the capability to browse the references is being tested; it exhibits very nice capabilities and enables to select the references of interest to define the enhancements to perform on the video-surveillance system (however this is a reconstruction from the conclusion which is known in advance; fortunately the privacy-preserving developments that were forecasted within the PARIS project easily match with legitimate outcomes from this analysis).

Then the SALT model dedicated to video-surveillance has been used to produce an updated system model likely to be at least partially subject to automatic validation (using rules that are derived from the selected references).

The SALT tools demonstrate a very important flexibility in their use and deployment. Also they are loosely coupled (some but few and optional dependencies between the different tools). This is a key feature to allow coping with this versatility of the organizations and of their practices.

Although our evaluation of the SALT process is only limited to the video surveillance data management use case, we expect that the processes defined in the PARIS project provide several salient features for strengthening privacy-by-design and accountability-by-design. Most feasible adaptation of the SALT complaint process, we assume, will be to apply the activities and control/review elements from the SALT compliant process to existing established system engineering process. More specifically, the activities and the definition of the roles in the SALT compliant process can be adapted to different contexts in the "real-world". The activities include those implementing privacy and accountability and those reviewing and deciding whether privacy and accountability obligations are fulfilled or not.

4.2 Use of a SALT compliant process for a biometric use case

In this section we explain how the lifecycle model normally used by Visual Tools for its systems and products has been adapted to the proposed SALT compliant process for the development of the biometrics system presented in WP6.

First of all it was necessary to analyze the development process followed by the company to identify and group the tasks carried out, and then map them to the stages defined in the SALT compliant process, as the company does not have a manual where the process is detailed. The process followed and the different stages are explained in detail in D6.3, but as a summary:

- **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.

  Normally, there is a sales agent involved at this stage who is a link between the customer and the development team. There is also the system proposer, that is the product manager of the company, who is in contact with customers and has in mind all technical solutions the company can provide.
- **Design stage**: it elaborates the specific strategy to follow to produce the system that will solve the stakeholder's problems. At this stage, the list of system requirements, that have been completed with a set of concerns extracted from the PIA, are more deeply examined. 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.

  Normally, this stage is carried out by just the development team of the company, although the product manager may also be involved.
- **Development stage**: it produces an implementation of the system based on the design specification elaborated in the previous phase.

  Development and testing teams are in charge of this stage.
- **Deployment stage**: at this stage the system is installed in the stakeholder's environment. It also includes other supporting actions required to leave the system fully operational and ready to use by the target users, such as the system configuration or the realization of didactic sessions for system users.

  In this stage, at least the stakeholder, the installer and the Surveillance Service Povider (SSP) are involved. It is important to correctly set up the system in the deployment stage, but also to prepare the required documentation (e.g. system manuals, privacy policies...), and to define the responsibilities and procedures related to the processing of the data stored in the system.
- **Operation and Maintenance stage**: the system is used for the surveillance purpose which it was built for, and it is also monitored in terms of performance and availability to ensure that it works as expected and that it does not become obsolete.

The System Operator and the System Administrator are normally in charge of the operation and maintenance tasks.

- **Retirement stage**: this is the end of the biometric system life cycle. The system is normally disposed 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.

Taking into account the iterations and loops within the different stages we have defined the diagram from Figure 8, which represents the development process normally followed by the company.

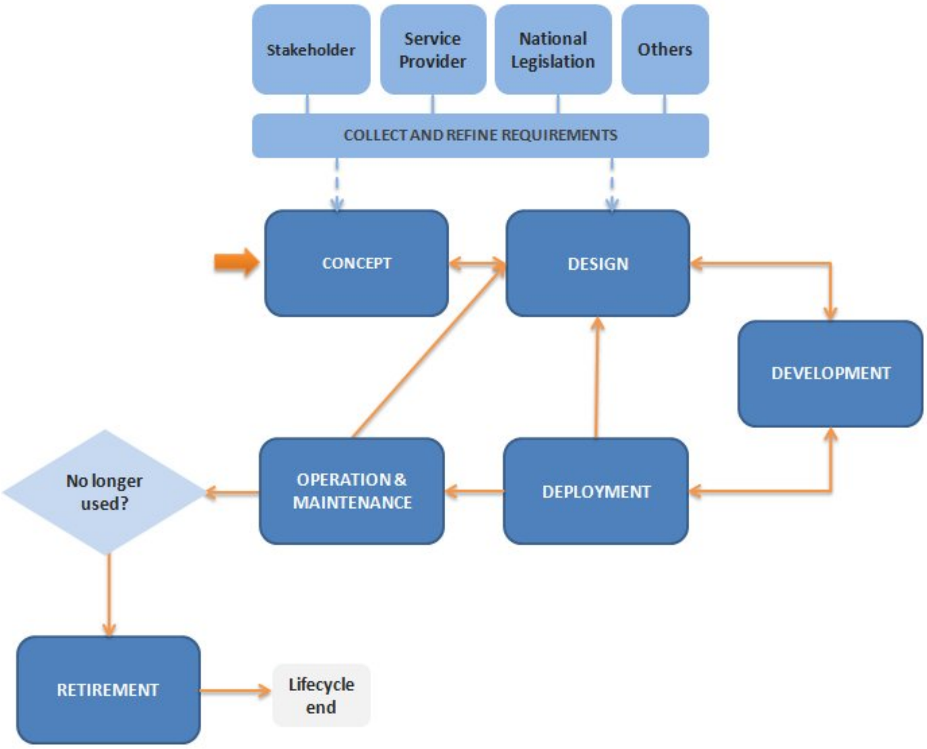


Figure 8. Common lifecyle of Visual Tools' systems

Now we have to consider the changes that the SALT compliant process proposes for this lifecycle and the provided resources:

- First, the SALT approach adds specific requirements to take into account privacy and accountability in the different stages of the development process.

- Besides, it requires to carry out different evaluations and revisions at the end of every stage to ensure that the system addresses the SALT concerns during all its lifecycle.
- Finally, the SALT Framework provides a set of resources to obtain information and guidance through all the process, and specially in the first stages:
    - SALT Questionnaires, that allow to evaluate the concept of the system and the viability of the solution selected in terms of privacy from a legal and technical point of view.
    - *SALT Validation Tool*, that highlights the main privacy and accountability concerns filled (and not filled) by a given design, allowing to refine the design decisions before the development stage.
    - SALT References and Taxonomies, that provide information and recommendations given by experts in different fields to guide the development process.

With this in mind, we adapted the development process of the company, depicted in Figure 9.

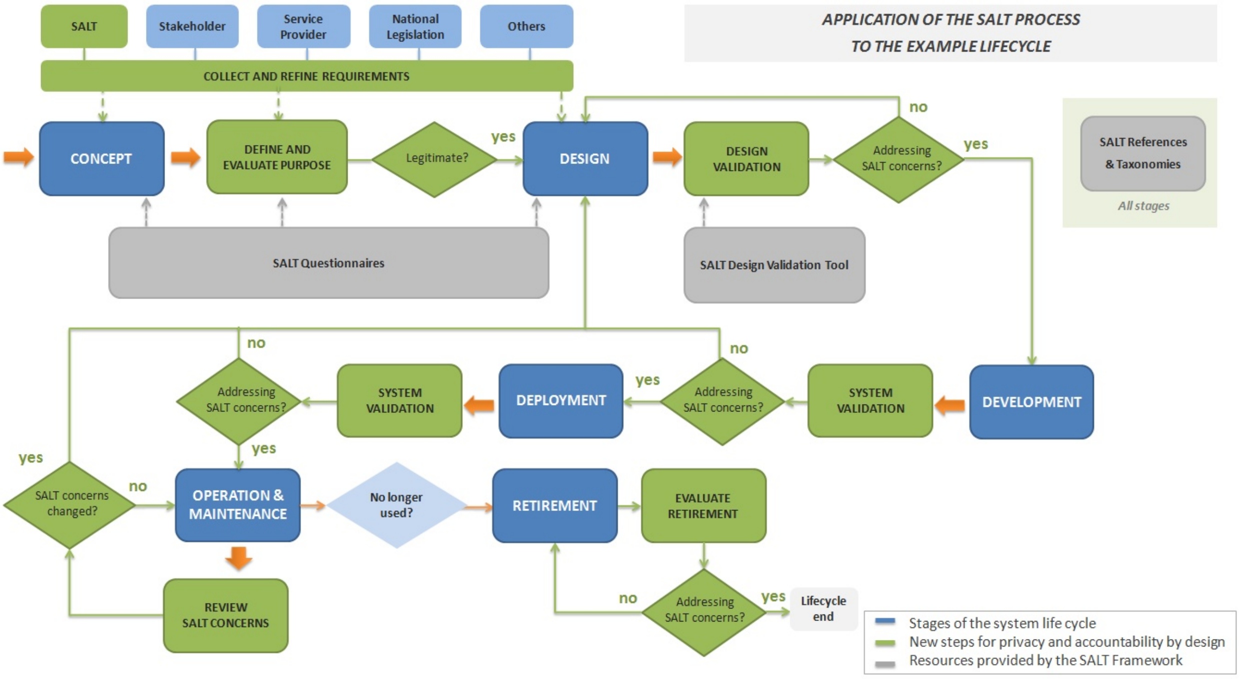

SALT
Stakeholder
Service Provider
National Legislation
Others
APPLICATION OF THE SALT PROCESS TO THE EXAMPLE LIFECYCLE
COLLECT AND REFINE REQUIREMENTS
CONCEPT
DEFINE AND EVALUATE PURPOSE
Legitimate?
yes
DESIGN
DESIGN VALIDATION
Addressing SALT concerns?
no
yes
SALT References & Taxonomies
All stages
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 9. Lifecycle of Visual Tools' systems applying the SALT methodology

This process has been used for the development of the biometrics use case presented in WP6, that is aimed at the detection of unauthorized accesses at the Visual Tools' headquarters in Madrid.

Regarding the use of the SALT Framework and its resources, this is also detailed in D6.3.

5 Process assessment

This section deals with the process assessment. We will show how and why key concepts and elements are reflected by the SALT methodology and present in the SALT compliant process.

5.1 Conceptual framework elements

Privacy and data protection requirements, both from a socio-ethical and legal perspectives, are reflected by the SALT methodology, especially at the concept and design phases. Both phases heavily rely on the approach supported in the beginning of the project in the deliverable D2.1 “Contexts and concepts for SALT framework”. Indeed, the concept phase sought to integrate a pragmatic approach of ethics, through a question-based approach and address ethical issues in such a way that those questions will be likely to generate reflexivity among the stakeholders. To support the use of the questionnaires, a taxonomy and extensive references, including both hard law and soft law instruments (legal texts, doctrine, guidance of public authorities and possibly remarkable caselaw), but also scientific literature is made available to the SALT users. The use of these tools plays a validation role under the SALT compliant process in particular with regard to two dimensions.

5.1.1 Using the questionnaire demonstrates willingness to adopt a reflexive approach with respect to a surveillance project

First, the use of the questionnaires demonstrates the willingness on part of the system owner to adopt a reflexive approach with regard to its surveillance project. At the time of the conception phase, the questionnaire will help the system owner to assess the impacts of its project on individual’s rights. We have seen that there are various questionnaires available, in particular different Privacy Impact Assessments (PIA) or Data Protection Impact Assessments (DPIA) that could be used at the stage of the conception. Questionnaire may be more or less developed and dynamic, but they can all be considered to contribute to generate reflexivity and self-questioning, which is one of the core objective of the SALT framework. Existing PIAs, although very useful, nevertheless leaves an important space for interpretation and misuse of the questionnaire so that it is not possible to guarantee compliance with privacy and data protection requirements. This is why the SALT compliant process can only show the “demonstration of a willingness to adopt a reflexive approach with respect to privacy and data protection issues”.

In spite of these limits, part of the PARIS research consisted in developing a specific questionnaire regarding biometrics. This questionnaire tends to get as closed as possible to an assistance to decision-making in order to strengthen the validation process. It provides assistance to the decision-making to both the concept and design phases. In the concept phase, the questionnaire assists decision-makers in assessing the overall proportionality of the surveillance system envisaged with respect to individual’s’ fundamental rights. A series of criteria have been retained to be the basis for an automatic evaluation, which may be compared to a validation process. In the design phase, the questionnaire assists the decision-makers in defining the main characteristics of the system in order to comply with data protection requirements. The use of the biometric questionnaire demonstrates that privacy and data protection have been thoroughly taken into account.

We can say that the use of the questionnaire validates a reflexive approach with regard to surveillance and its impacts on privacy and data protection.

5.1.2 Using references and glossary demonstrates disposal to increase awareness by SALT users regarding the rich, complex and vivid legal and societal environment in which the surveillance system is destined to be deployed

The references and taxonomy are intended to contain a vast amount of references regarding privacy and data protection. Although the SALT framework is not exhaustive, the references nevertheless reflect the complexity of the legal and societal impacts of surveillance technologies on privacy and data protection rights. They also serve to extract requirements to be taken into account when designing, installing and maintaining the system. Again, users may be more or less active in searching for references and processing the information enshrined in it to conceive and design their system. It is possible that a user searches for legal references, but deliberately decides to ignore them. On the contrary, it is possible that users search for references, process the information, adapt the requirements to their specific situation and by thus increase their knowledge of the privacy and data protection issues at stake when conceiving surveillance systems. In that sense, the references and taxonomy play an important learning role likely to increase awareness among SALT users of the legal, socio-ethical and technical environment in which surveillance system operate.

We can say that the use of the references and taxonomy validates a good level of awareness among SALT users of the legal, socio-ethical and technical environment in which a surveillance system operates.

Regarding the implementation of the recommendations provided by the SALT Framework in the design of systems, it is up to the system designers to include adequate privacy mechanisms into the design. However, as system designers are not used to handle legal or ethical concerns, the use of the SALT Framework to consult recommendations already demonstrates their awareness in terms of privacy. Besides, the use of the automatic validation tool developed within the PARIS project (see Section 2.1) requires an effort from designers to create the model of the system in the format required for its validation, which also indicates a good level of awareness.

5.2 Privacy-by-Design (PbD)

The SALT Compliant Process covers the whole life-cycle of the system from the requirements to the retirement phases. The PARIS consortium has provided some solutions in order to ensure privacy at design phase.

First of all, the consortium has decided to use model based approaches. For this reason, we have developed a UML profile dedicated to privacy and surveillance systems. More details are given in the following subsection 5.4.2. Additionally, some references are digitalized in the SALT repository (see Section **¡Error! No se encuentra el origen de la referencia.**). A SALT reference can include some design constraints (formally represented as OCL rules) in order to check that a design is compliant with a reference. At the end, the system is modelled in UML with privacy tags. According to the selected SALT references, it is possible to automatically check the correctness of a model (i.e., the model respects or not the SALT reference constraints). For this, a tool has been developed for checking the constraints (see Section 5.4.3).

The second valuable result of the project is to associate the PIA and the PbD processes. As defined in WP2, some questions help stakeholders to reason on privacy for surveillance systems. The project proposes to allow the possibility to answer a question by providing more information on the design. In particular, it is possible to refer to SALT references included in the design. Figure 10 highlights the PARIS proposal.

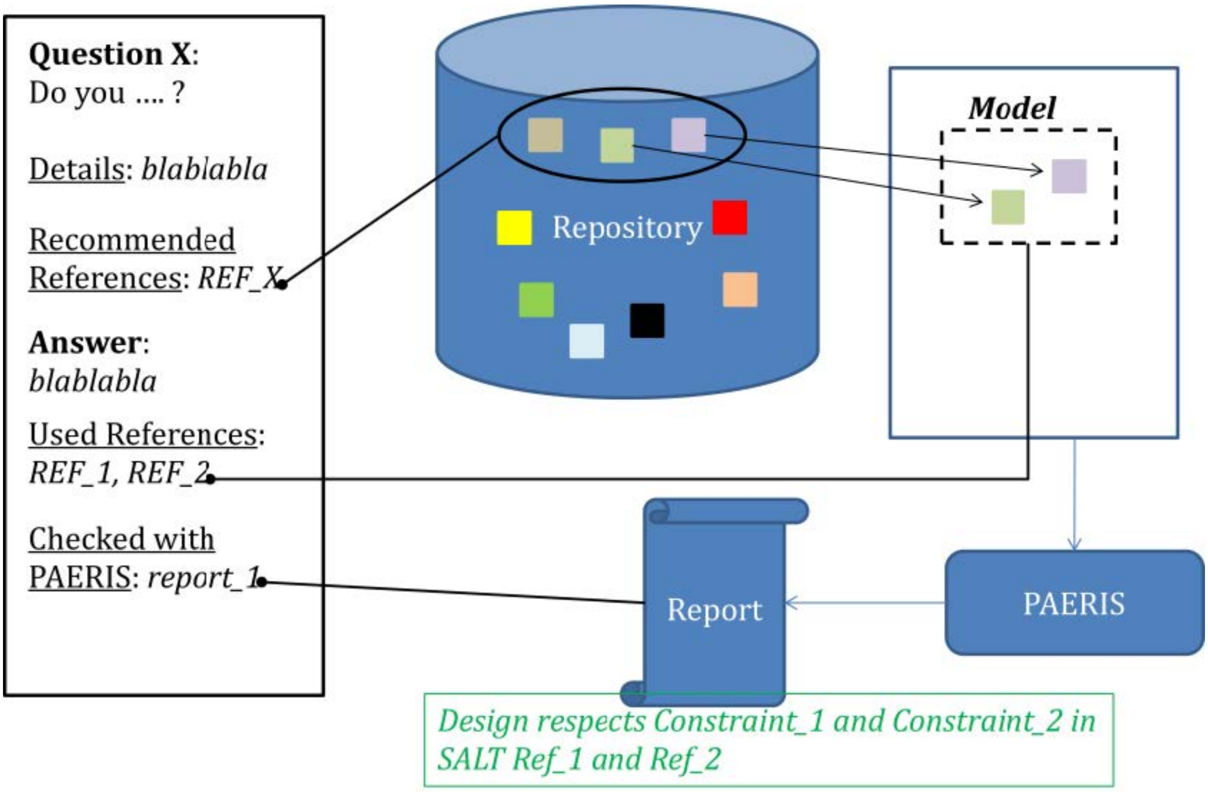

Question X:
Do you .... ?
Details: blablabla
Recommended References: REF_X
Answer: blablabla
Used References: REF_1, REF_2
Checked with PAERIS: report_1
Repository
Model
Report
PAERIS
Design respects Constraint_1 and Constraint_2 in SALT Ref_1 and Ref_2

Figure 10. Integration of the questionnaire tool with design tools

As depicted in Figure 10, the answer to a question can recommend some SALT references stored in the repository. The user who answers to the questionnaire can indicate all SALT references included in the model related to this question. Finally, the report generated by the automatic validator (i.e., what we have called PAERIS in Figure 10) could also be attached to the answer.

Note that due to time constraints, the project has not implemented this feature in the current version of the questionnaire tool.

5.3 Accountability-by-Design (AbD)

Generally speaking, accountability mechanisms are concerned with the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating compliance with the commitments and obligations of the surveillance system owner. More precisely, as stated in Deliverable D2.3, the goals of accountability mechanisms are twofold: (1) to ease answerability[1] and (2) to increase verifiability.

From the technical point of view the core of the accountability mechanisms are:

1. The "accounts" which have to be complete and trustworthy to provide convincing evidence that the system complies with all its privacy requirements.
2. The verification process (including organizational and technical aspects) to ensure that the accounts can be checked and responsibilities allocated in case of non-compliance.

However, as pointed out in [6], accountability does not emerge spontaneously. A system has to be designed with accountability requirements in mind. Indeed, the feasibility of accurate and comprehensive verifications depends directly on the design process and the technical architecture of the system. Accountability should thus be included in the design in the same way as privacy, following an *accountability by design* approach. The SALT compliant process implements the accountability by design approach in several ways.

First the application of the process in itself contributes to the accountability requirements because it enforces the creation of a specific documentation to justify each choice in the life cycle of the system.

In addition, each phase of the life cycle also includes specific provisions for accountability. A number of questions and recommendations of the SALT framework focus on the nature of relevant evidence to facilitate the compliance checking process. Before system design, accountability mechanisms concern mainly the answerability of the surveillance system, ensuring participation of the stakeholders and proper consideration of their concerns (with justifications). They also include steps to take into account any applicable national legal regulation which can integrate specific obligations for controllers. During system design, the questions concern the choice of relevant categories of personal data, their storage (centralized or decentralized, encrypted, etc.), the processing operations that affect them, retention delays, automatic deletion mechanisms, etc.

All aspects of log construction and security are also considered because the evidence (accounts) for a posteriori checks (accountability of practice) is provided by these logs. Designing the structure of logs is a task of significant importance since meaningful compliance analysis is only possible if the evidence is sufficiently rich and unequivocal. In addition, careful choices need to be made to ensure that the minimal amount of personal data is kept into the logs to comply with the data minimality principle and avoid the introduction of additional risks of personal data leaks. The conditions under which logs are stored are also part of the accountability process, since insecure storage could lead to new privacy concerns given that logs may contain actual personal data, or at least metadata. The definition of the content of the logs, the use of proper log securing technology such as encryption and the methods used to verify these logs should therefore be documented as part of the accountability process. In practice, a person within the organization should be appointed to monitor the whole process (from the PIA, to the

[1] Answerability is the process through which an organization makes a commitment to respond to and balance the needs of stakeholders in its decision-making process and activities and delivers against this commitment (see D2.3).

definition and implementation of the internal policies that will regulate the data processing activities generated by the system) and be given sufficient resources to carry out the task. The audit procedure should be described precisely and conducted by an independent third party.

5.4 Tools developed within the project

Several tools have been developed to support the SALT compliant process. This section validates them by proving their inclusion into the process, at what level and describing their contribution in the process lifecycle.

5.4.1 SALT repository

The SALT repository is the main privacy and accountability provider of the SALT methodology, since it is the place where all SALT references are stored. These SALT references contain the privacy and accountability concerns for surveillance systems regarding four possible categories: socio-contextual, ethical, legal and technological.

As it can be seen in Figure 1, the SALT repository may be accessed throughout the whole SALT compliant process, meaning that it can be used by system stakeholders, designers, developers, installers, operators and even external auditors. Therefore, it is clear that it is a key component of the process. Besides, the information retrieved from the SALT repository will not only be used by the different types of user, but also by other tools (even though this could be transparent for human users).

5.4.2 UML profile

The UML profile is only intended to be used by system designers, hence it fits into the design stage of the SALT compliant process. This tool helps system designers to create a model of the SUD (using UML), that is a diagram (or set of diagrams) with all the information regarding a particular surveillance system.

It provides an interface that allows for connecting to the SALT repository and search for the appropriate SALT references that may be relevant for the current SUD. Thanks to this (and the system specifications from previous stages of the process), system designers have access to privacy and accountability requirements at design time. The SALT references also provide a series of OCL rules that will serve as an input to the automatic validator (see Section 5.4.3).

Strictly speaking, the SALT compliant process could be set up without the need of the UML profile. In this case, the company or organization using the process can use its own modeling tool, although the automatic validator would not be available because it would not have access to the OCL rules. For this reason, the usage of the UML profile is recommended.

5.4.3 Automatic validator

The use of the automatic validator is tightly bounded to the UML profile (see Section 5.4.2), since it is through the profile how a user connects to the SALT repository and retrieves the SALT references where the OCL rules are included. These rules are continuously checked against the system model in the background by the automatic validator (showing a message whenever a rule is not fulfilled). Therefore, it is clear this tool belongs to the design phase of the SALT compliant process.

However, it should be noted that system designers (or any other type of user) do not directly interact with the automatic validator. As its own name states, it is an automatic tool which starts to work as soon as the designer begins the creation of the system model (as long as the aforementioned UML profile is also used), and the only thing the user will see from its operation is a set of messages.

5.4.4 Questionnaire tool

All PIAs rely on questionnaires. The PARIS project also follows this way for reasoning and assessing privacy risks. The project has developed a tool for managing questionnaires. The questionnaire is used from the beginning of the project up to the end of the design phase. However, it is important to note that some questions can be related to next phases (in particular the retirement phase where private data has to be deleted).

At the end, a privacy assessment report including recommendations is generated. This report is in particular useful for accountability.

5.4.5 Taxonomy tool

An important issue, in particular in the context of privacy, is to have common understanding. This tool aims at providing a dictionary of each term used in this project. This dictionary can be consulted by different stakeholders (e.g., a technical user who needs to understand a legal term). During the full SALT compliant process, all other SALT tools can refer to taxonomies. For instance, all concepts defined in the taxonomy are highlighted in the questionnaire.

6 Conclusion

This document is the last deliverable of WP4, and hence this section serves as a concluding remark for the whole work developed and delivered within this workpackage during the working period of the PARIS project.

The main output generated from WP4 is the SALT compliant process. This process, whose guidelines have been detailed in the above sections, states the steps for designing and developing a surveillance system in order to fulfill with the SALT methodology. In this way, the SALT compliant process serves as a guide for all type of users who interact (in a way or another) with a given surveillance system at any stage of its lifecycle. Of course, depending on the type of user and/or the process stage, the guidance provided by the process may be different.

It is important to remark that the SALT compliant process is attached to the general concept of the SALT methodology, i.e. to help users, but not to take decisions for them. This means that following the SALT compliant process can be as flexible as the user wishes it to be, since it is the user the one with the responsibility of carrying out the actions suggested by the process or choosing something different he may consider more appropriate, provided however that all these decisions are documented and traceable (accountability requirement).

But following the SALT compliant process and using the associated tools brings a major reward: the attainment of a SALT compliant surveillance system. This is a term coined by the PARIS project consortium, meaning that the resulting surveillance system has taken into account the privacy and accountability concerns provided within the SALT repository. This is a significant achievement, since current surveillance systems are usually focused on functional requirements and the privacy of the subject under surveillance (typically citizens) is commonly omitted, and so it happens with the accountability issues.

As we have already stated, the SALT compliant process is not alone in its task of helping users in the creation and operation of SALT compliant processes. A set of tools has been developed and delivered to users in order to be used when and how it is indicated by the SALT compliant process (see deliverable D3.4 "Guidelines for SALT Framework Management Tool" for an in depth explanation of the tool set).

Among all the tools, the SALT repository may possibly emerge as the most relevant one, since it is the place where all privacy and accountability concerns are stored. All the information is encapsulated in logical units called SALT references, each one also having a set (at least one) of concerns. The amount, quality and accuracy of these references will increase in time when the all SALT tools are released and begin to be used by the community.

Of course, the usage of the SALT compliant process requires an effort from incoming companies and institutions who wish to adopt the SALT methodology. Some of them will use the standard SALT compliant process as it is, whereas some others will adapt their current engineering processes looking for a correspondence with the SALT compliant one. Therefore, we also provide a set of recommendations that could help in the adoption of the proposed process. Even more, two practical examples (one for video surveillance systems and another one for biometric systems) have been provided to better understand how this procedure can be carried out.

7 References

[1] PARIS FP7 Project Deliverable D2.2 "Structure and Dynamics of SALT Frameworks".

[2] PARIS FP7 Project Deliverable D2.3 "Guidelines for SALT Conceptual Frameworks".

[3] PARIS FP7 Project Deliverable D3.4 "Guidelines for SALT Framework Management Tool".

[4] PARIS FP7 Project Deliverable D6.3 "Biometrics Use Case".

[5] Unified Modeling Language (UML). http://www.uml.org

[6] Denis Butin, Marcos Chicote and Daniel Le Métayer, *Strong Accountability: Beyond Vague Promises*, in *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, edited by Serge Gutwirth, Ronald Leenes and Paul De Hert, Springer, 2014.