SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document type	Report
Title	D1.2- Requirements Assessment Report
Work Package	WP1
Deliverable Number	D1.2
Editor(s)	S. Gürses, K.U. Leuven, N. Zannone, TUE
Dissemination level	Public
Preparation date	30. June 2010
Version	2.0

The TAS3 Consortium

Nr.	Participant name	Country	Participant short name	Participant role
1	K.U. Leuven	BE	KUL	Coordinator
2	Synergetics	BE	SYN	Project Manager
3	University of Kent	UK	KENT	Partner
4	University of Karlsruhe	BE	KARL	Partner
5	Technische Universiteit Eindhoven	NL	TUE	Partner
6	CNR/ISTI	IT	CNR	Partner
7	University of Koblenz-Landau	DE	UNIKOLD	Partner
8	Vrije Universiteit Brussel	BE	VUB	Partner
9	University of Zaragoza	ES	UNIZAR	Partner
10	University of Nottingham	UK	NOT	Partner
11	SAP Research	DE	SAP	Partner
12	Eifel	FR	EIF	Partner
13	Intalio	FR	INT	Partner
14	Risaris	IR	RIS	Partner
15	Kenteq	BE	KETQ	Partner
16	Oracle	UK	ORACLE	Partner
17	Custodix	BE	CUS	Partner
18	Medisoft	NL	MEDI	Partner

Contributors

	Name	**Organisation**
1	Antonia Bertolino	CNR/ISTI
2	David Chadwick	KENT
3	Danny DeCock	K.U. Leuven
4	Brendan van Alsenoy	K.U. Leuven
5	Jeroen Hoppenbrouwers	K.U. Leuven
6	Lex Polman	KETQ
7	Carlos Flavian	UNIZAR
8	Sandra Winfield	NOT
9	Sampo Kellomäki	SYM
10	Marc Van Coillie	EIF
11	Marc Santos	KOBLENZ
12	Jerry den Hartog	TUE
13	Joseph Alhadeff	ORACLE
14	Brecht Claerhout	CUS
15	Luk Vervenne	Synergetics
16	Jens Müller	KARL
17	Jutta Mülle	KARL
18	Gilles Montagnon	SAP

Table of Contents

Keyword List

Requirements assessment, Gap analysis, Requirements elaboration

1 Executive Summary

This document presents the final (third) iteration of Deliverable 1.2. The objective of D1.2 is to gather requirements regarding unsolved problems in the field of security and trust in service-oriented open and distributed environments that apply to the TAS^3 project. Specifically, the deliverable translates the design requirements defined in Deliverable 1.4 [22] into the research and development activities that will be carried out in the different TAS^3 WPs.

In order to fulfill the objectives of this deliverable, we have completed a number of sequentially ordered activities. The results of these activities are documented in the different sections, while some of the material we used and collected is included in the Appendices.

During the first iteration, we have reviewed the objectives of each work package and the solved and unsolved problems they are addressing with respect to the objectives of their work package. Next, we asked partners to elaborate or refine requirements based on these objectives and scenarios provided by the demonstrators in D1.4. Then, we compared the requirements elaborated by the TAS^3 partners with the existing solutions for trust and security in service-oriented open and distributed environments. We then identified research and development challenges to be addressed by the partners in their future activities in order to fulfill their requirements. Last, we mapped the requirements to the TAS^3 architecture.

In addition, in order to prioritize activities and discover interdependencies within and among work package activities, we analyzed requirements interactions in each WP and between WPs. The WP-internal interactions are represented in the form of graphs to support the analysis. The inter-WP interdependencies are captured in tables and later analyzed using a tool to detect inconsistency candidates. In the second and third iteration of D1.2, we repeated the requirements elaboration steps to capture the evolution of the requirements. Further, we re-iterated the analysis of inter-WP requirements interactions in order to find inconsistencies and incompleteness in the D1.2 requirements.

Next, once the consistency and completeness analysis was completed, we completed another interaction analysis activity between the refined legal requirements elaborated by WP6 and the technical requirements of the WPs. Finally, we validated the consistency of the requirements in D1.2 with the architecture of TAS^3.

Hence, the contribution of the deliverable is threefold. First, it provides a gap analysis which is used to map out future activities. Second, the deliverable elaborates on the technical, legal and application domain requirements of TAS^3. Finally, the inter-WP requirements interaction analysis provides the partners with an understanding of the relationships between WP requirements, and provides the grounds upon which to assign responsibilities and detect cooperation needs between partners.

Readers Guide: We have added a number of chapters or expanded existing ones to include all the activities and results in all iterations of D1.2. The introduction has been expanded to give an overview of all the activities that were part of D1.2. Most activities in the second and third iteration of D1.2 have concentrated on consolidating the different viewpoints of the technical work packages, integrating the legal and technical requirements, and validating the requirements with the architecture. In order to achieve these objectives, we conducted a number of interaction analysis activities.

Specifically, in Section 5 we provide an overview of how we analyzed the interaction of

technical requirements of different technical and application domain oriented WPs and the results achieved. We moved the documentation of the interactions to Appendix E and F. The analysis of the interaction of legal and technical requirements and the resulting gap analysis is documented in Section 6. The mapping of global requirements to the architecture and the related gap analysis is provided in Section 7. Finally, the mapping of all technical requirements to the architecture and the gap analysis is provided in Section 8. All the templates we sent out to the partners for requirements, requirements interactions, and existing solutions is included in Appendix A. We added Section B to document all the additions and changes to the requirements due to the re-iteration of requirements elaboration and the various requirements interaction analysis activities. Last, we added some new insights into the conclusion in Section 11.

The following chapters remained identical with the first iteration of Deliverable 1.2. Section 3 provides a review of the objectives of each work package and the objectives are related to solved and unsolved problems in the field of security and trust in service-oriented open and distributed environments. Section 4 provides an analysis of the technical, legal and application domain requirements that address the solved and unsolved problems related to TAS^3. The technical, legal and application domain requirements elaborated for D1.2 are documented in Appendix C. This detailed listing of the requirements includes the justifications for each requirement and the interactions of each requirement within each WP.

Section 9 provides an analysis of the requirements fulfilled by existing solutions. The justifications for selected solutions are summed up in Section 9 and are included in detail in Appendix D. Section 10 lists the activities that each work package has to complete in order to fulfill the requirements that cannot be fulfilled using existing solutions. Section 7 maps the WP requirements to the Architecture.

2 Introduction

2.1 Scope and Objectives

The objective of Deliverable 1.2 is to gather requirements about unsolved problems in the field of security and trust in service-oriented open and distributed environments that apply to the TAS^3 project. Specifically, the deliverable translates the design requirements defined in Deliverable 1.4 [22] into the research and development activities that will be carried out in the different TAS^3 WPs. Here, we revisit and refine the requirements presented in Deliverable 1.4 [22], and take Deliverable 1.1 [25] on State of the Art as well as the objectives of TAS^3 as a reference in order to provide a gap analysis. This deliverable is hence different in its main focus than D1.4 which focuses on requirements elicitation.

There are two main objectives fulfilled by this deliverable:

- the identification of the activities that will be performed by each WP in the course of the project based on a gap analysis;
- the identification of the relationships among the activities of WPs with respect to the requirements that need to be fulfilled in order to realize the TAS^3 architecture.

The gap analysis presented in this document serves as a basis for the identification of the activities and research challenges that will be addressed by the WPs in the course of the project. In order to complete the gap analysis, it is first necessary to elaborate on the requirements that each of the WPs need to fulfill for the realization of the TAS^3 architecture and how these interact with each other. A detailed description of the methods and process that was used by the TAS^3 partners for the gap analysis are given in Sections 2.2 through 2.4.

Communication with Partners: In the first iteration of D1.2 we communicated with the partners through emails and during face-to-face meetings. In the later iterations of D1.2, we used the Trac Wiki tool which was introduced to the project by WP12. The Trac Wiki tool provides a collaborative environment in which partners can also view the contributions of other partners. Especially inter-WP requirements interaction analysis required intensive communication among partners. The Trac Wiki offered us the collaborative environment to mitigate some of the problems that arise when a distributed requirements engineering team has to interact intensively. Further, we are able to integrate and edit Graphviz[1] DOT[2] files in Trac Wiki pages. This allowed us to address problems with the presentation of Inter-WP interactions, as we discussed in Section **??**.

In addition, in the re-iteration of the deliverable we organized four workshops with the partners. In the first workshop, we provided an overview of the steps to come. In the second workshop, we completed the analysis of inter-WP requirements interactions. In

[1] Graphviz is open source graph visualization software. The Graphviz layout programs take descriptions of graphs in a simple text language, and make diagrams in several useful formats such as images and SVG for web pages, Postscript for inclusion in PDF or other documents; or display in an interactive graph browser. http://www.graphviz.org

[2] DOT draws “hierarchical” or layered drawings of directed graphs. The layout algorithm aims edges in the same direction (top to bottom, or left to right) and then attempts to avoid edge crossings and reduce edge length.

the third workshop, we executed the analysis of interactions between legal and technical requirements. The final workshop was used to validate the requirements by mapping them to the architecture together with the architecture team.

2.2 Gap Analysis

A gap analysis is a process of identifying delta between the current situation and the future desired situation [8]. Therefore, a gap analysis requires both establishing the state of the art and the missing elements with respect to the desired future state. The two other deliverables in Work Package 1 provide the necessary building blocks of a gap analysis: the state-of-the-art of trust and security in service oriented architectures in D1.1 [25] and definition of the design requirements that the future TAS^3 architecture should fulfill in D1.4 [22].

To perform a gap analysis based on these two documents, we took the following steps:

Step 1: Define objectives and problems. The partners revisited the objectives of their work packages with respect to the objectives of TAS^3. They were also asked to identify solved and unsolved problems in the field of trust and security in service oriented environments in the scope of their work package.

Step 2: Elaborate requirements. The partners elaborated on the technical, legal and application domain requirements that they had to fulfill to achieve the objectives of TAS^3 and the objectives of their work package.

Step 3: Identify existing solutions. The partners listed existing solutions that addressed the solved problems they had identified in Step 1. They further stated which of their requirements elaborated in this deliverable were fully or partially fulfilled given the existing solutions.

Step 4: Plan future activities. The partners identified the activities that are necessary to fulfill the requirements that are not addressed by existing solutions and stated how they plan to validate the fulfillment of these requirements.

Part of the gap analysis activity included the elaboration and analysis of the technical, legal and application domain requirements of TAS^3. We shortly describe the methods we used for this step in the gap analysis in the next section.

2.3 Requirements Elaboration

We preferred a template based methodology for requirements elaboration and analysis since it is an accepted standard approach to requirements engineering and produces comparable results among many work packages. We prepared and distributed a template to the partners to elicit their technical, legal and application domain requirements that they have to fulfill with their work package activities in order to achieve the objectives of TAS^3. The partners were expected to make use of the two prior deliverables D1.1 for state-of-the-art for the gap analysis, and, D1.4 for the requirements elaboration. During this phase we supported the partners mostly through written electronic communication, but also through phone conferences and occasional face-to-face meetings. In the process we iteratively reviewed all the

inputs from the partners in order to reach a comparable level of requirements and activity granularity among many partners and 10 WPs.

The template for requirements elaboration (See Template 1 in Appendix A) was based on the two methodologies for template based requirements elicitation. The first one is a popular industrial requirements elicitation template called Volere [26] and a second template which is described in [27]. We preferred to use the latter for its simplicity, and enhanced it using Volere. Purpose of the project, the scope of the work etc. were questions from Volere that we included to support the gap analysis.

The template in [27] defines the following mandatory fields: requirement id, version, author, source, purpose, description, time interval, importance, urgency, comments. Of these fields we used: requirement id, source, justification (instead of purpose, as it better conditioned the author to state why the requirement is necessary), requirements (instead of requirement description for brevity). The other fields were addressed through the versioning of the deliverable itself (version), the list of contributors (author), and our later interaction analysis (importance, urgency and comments). In a different version of their template for functional requirements the authors in [27] suggest integrating also a use case template similar to that defined by [10]. We avoided this in order to keep the separation between this deliverable and Deliverable 1.4 [22] which works with detailed scenarios. Participants were encouraged to make use of those scenarios but not to repeat them in this deliverable.

For the first interaction analysis activity, we asked partners to fill out a field in the template for interactions among their requirements within their work package. We provided a controlled vocabulary which consisted of the following elements:

- A depends on B: requirement A requires requirement B. B is a condition for A.
- A supports B: requirement A is needed to fulfill requirement B. A is a condition for B.
- A implements B: requirement A is a specialization of requirement B.
- A abstracts B: requirement A is a generalization of requirement B.
- A is in conflict with B: requirement A and requirement B are logically inconsistent or the implementation of both requirements is not feasible.

There were two further iterations of Deliverable D1.2. In the second year of the project, the TAS^3 partners made considerable progress with respect to the implementation of the TAS^3 architecture. This also led to changes in requirements: some requirements were eliminated and changed, additional requirements were captured. We asked the partners to document these changes in a WP specific wiki page. For each edited or deleted requirement, partners were asked to provide a justification. For additional requirements, the partners had to fulfill the requirements template provided in the initial iteration of D1.2, which also includes a justification of the requirement (See Requirements Template 3 in Appendix A).

In particular, the following five objectives were met through the re-iterations of the deliverable:

- review and update the elaborated requirements, in order to capture changes and additional requirements.

- re-iterate the inter-WP requirements interactions in order to detect and solve inconsistencies and check for completeness.
- update used solutions and validation plans of each WP
- integrate the legal requirements to the finalized requirements.
- map the requirements to the architecture in order to validate the finalized requirements.

We explain in more detail the interaction analysis activities in the next section.

2.4 Interaction Analysis

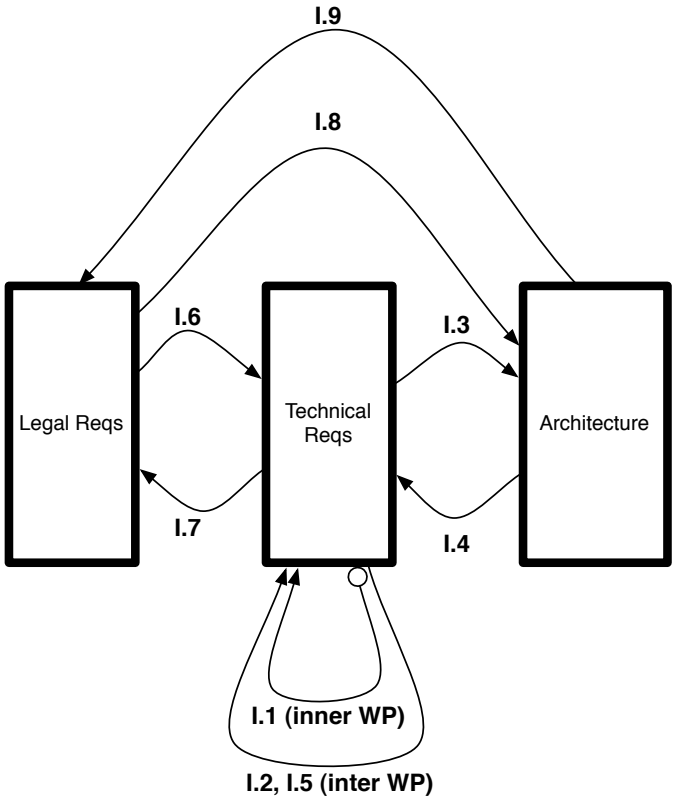

Figure 2.1: Overview of interaction analysis activities in D1.2. The numbers indicate the order of the activities.

Figure 2.1 provides an overview of the nine interaction analysis activities executed during the various iterations of D1.2. In Sections 2.4.1 through 2.4.6 we describe the interaction analysis activities that we executed in D1.2.

2.4.1 Inner WP Requirements Interaction (I.1)

Once all the requirements were elaborated, we analyzed the inner-WP requirement interactions. For the inner-WP interaction analysis we visualized the interactions with diagrams

in order to improve the readability and resulting analysis, as suggested in [4]. The diagrams in Section 4 were inspired by [21] where responsibilities with respect to requirements-dependency social networks are mapped out to determine team members who are likely to work together and who would play an important role in requirements traceability.

In particular, we used *requirements graphs* based on [21]. In requirements graphs, each node indicates a requirement of the workpackage, and labeled edges indicate the type of interaction between requirements. Circles around the graph indicate the workpackage from which the requirements originate. We used requirements graphs to discuss and prioritize the requirements of each WP. The final visualization and evaluation were validated by the corresponding partners.

2.4.2 Inter-WP Requirements Interaction (I.2)

To integrate the WP viewpoints into a monolithic consistent requirements document, we asked WP partners to document the interactions of requirements across workpackages, from now on referred to as the inter-WP requirements interaction. We used the same controlled vocabulary used for the inner workpackage interactions. We added ”A is similar to B” to the controlled vocabulary for inter-WP interaction analysis, as recommended by [1]. We did this in order to determine overlapping or redundant requirements across work packages. The inter-WP interactions were then captured using a template (See Template 2 in Appendix A).

We tried to visualize the inter-WP requirements interactions, but these visualizations actually did not enhance readability. Hence, we included the templates as provided by the partners according to their viewpoints, then modeled the interactions as a graph and used this graph to look for inconsistency candidates. We describe our approach to inter-WP interaction analysis in more detail in Section 2.4.4 .

2.4.3 Requirements interaction with Architecture (I.3 and I.4)

In addition to the Inter-WP interaction analysis among the different partners, we asked the architecture team to map the requirements of the different WPs to the architecture. We asked them to fill a simple template mapping each requirement to a component of the architecture, including an explanation of how the component will fulfill that requirement. The architecture team also documented redundancies and requirements that are out of the scope of the architecture. The results were communicated back to the WPs and the necessary updates were conducted in the requirements list in the first iteration of D1.2.

2.4.4 Reiteration of Inter-WP Requirements Interaction (I.5)

As mentioned earlier, graphical models for analysis often suffer scalability issues, depending on the granularity of the analysis needed. In our case, the direct visualization of inter-WP requirements interactions fell apart after 20 requirements. Hence, simple visualization is not appropriate for representing inter-WP interactions between the 163 requirements in Deliverable 1.2. To address the scalability issues, we developed our own automated analysis tool that detects inconsistency candidates and visualize only the relevant parts of the requirements graphs. We used the initial round of input with respect to inter-WP interactions to

study the type of inconsistencies that occur among the requirements of the different WPs and to develop an inconsistency detection tools.

The inconsistency detection tool is used to find inconsistency candidates. Inconsistency candidates include groups of requirements that are indicated by the WP partners to either be conflicting or similar. Further, we developed a catalog of patterns which may point to further inconsistency candidates. These patterns detect:

- *homogeneous interaction cycles*: cycles with the same interaction type, e.g. "A depends on B", "B depends on C" and "C depends on A";
- *heterogeneous interaction cycles*: cycles which are not homogeneous and may be unreasonable, e.g. if "A depends on B" and "B abstracts A", it means that a requirement depends on its abstraction.
- *non-cyclic interactions*: these patterns identify the combinations of unacceptable multiple edges, e.g. "A supports and depends on B", as well as unreasonable combinations comparable to heterogeneous interaction cycles, e.g. "A supports and abstracts B".

After repeating the elaboration of requirements and capturing all the new, edited and deleted requirements of the WP, we re-iterated the inter-WP requirements interaction analysis using the inconsistency detection tool.

We first asked the partners to address requirements that were indicated as similar or conflicting. At the end of this activity, similar requirements were either merged or their differences were better articulated, and conflicting interactions between requirements were resolved.

We then used our inconsistency detection tool to generate requirements graphs of inconsistency candidates. These become our *inconsistency graphs*. We integrated the inconsistency graphs into the Trac Wiki system using GraphViz DOT. The partners were then asked to comment on the inconsistencies, to suggest changes to interactions between requirements or to change the requirements. The suggested changes are then validated by the partners. The results were then fed back into the inconsistency detection tool to check if new inconsistencies surfaced as a result of the changes.

A preliminary analysis using the inconsistency detection tool, following the resolution of similarities and conflicts, revealed 20 similarities, 62 homogenous cycles and 3 heterogenous cycles. These inconsistency candidates based on patterns were discussed and resolved with the partners during a requirements interaction analysis workshop with all partners.

This interaction analysis activity requires multiple synchronization steps among the partners with a high communication overhead. The intermediary synchronization between steps have to be well planned since changes provided by any WP may affect the interactions with other requirements. In addition, inconsistency analysis can be reiterated infinitely. Knowing when to stop the analysis requires balancing the level of requirements consistency with partners' time and motivation. Trac wiki provides an environment to analyze and resolve inconsistencies collaboratively. However, it can lead to confusion, especially if unexpected edits are executed by partners. In the following paragraphs we explain the rest of the interaction analysis activities, including details on how we deal with problems of scalability and completeness during interaction analysis activities.

2.4.5 Interaction of Legal and Technical Requirements (I.6 and I.7)

The interaction of legal requirements with technical requirements is an under-researched matter where the accumulation of past experience is minimal. Previous work in this field focuses on the articulation of data protection legislation as requirements [**?**] but not on how legal and technical requirements can be consolidated during requirements engineering. However, due the nature of legal requirements, the relationship between legal and technical requirements need to be expressed differently than technical requirements among each other. Further, in the second iteration of WP6, the legal requirements were refined from 17 requirements to over 60 legal requirements, and this required a systematic approach to interaction analysis between legal and technical requirements.

We identified the following steps in order to complete an analysis of the interaction of legal requirements with technical requirements:

1. identify data protection requirements that can be fully or partially technically satisfied
2. identify data protection requirements that cannot be technically satisfied
3. identify legal requirements elaborated by other WP partners

Further, in order to complete this partitioning, we designed the following interaction template:

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.X	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		

In this template, the vocabulary is to be interpreted as follows:

- is fulfilled by: 1-on-1 (exact match) OR technical requirement covers more than the legal requirement
- is partially fulfilled by: technical requirement covers a part of legal requirement
- conflicts with: in case the implementation of the technical requirement would violate the legal requirement
- comment: used to describe why it is not yet sufficiently supported (but should be) and states whether for the fulfillment of the legal requirement additional work is needed, and if so, which work packages would be responsible to articulate the requirements or develop the necessary components.

After the technical requirements interaction analysis was completed, WP6 reviewed the (revised) requirements list to evaluate the extent to which legal requirements were sufficiently addressed, as well as to evaluate whether or not there were any legal requirements missing. The extent of fulfillment (complete, partial, not at all) of the legal requirements through the technical requirements was documented by WP6 in the legal-technical requirements interaction analysis template. Where it was found that there was no adequate technical counterpart to satisfy the legal requirement, WP6 documented which items were still missing (under the comment section of the template with the title requires additional work)

Once all of these items requiring additional work were documented, a workshop was organized to discuss and decide which WP shall be responsible for ensuring that a given legal requirement will be satisfied. This proved to be a useful exercise not only for completing the interaction analysis, but also to raise awareness with technical partners with respect to the legal requirements relevant to their work. Only in a limited number of instances was the satisfaction of a legal requirement considered to be out of scope. In all these cases, this was due to the fact that the objective of TAS^3 is not to develop a final end-product. For such requirements, this was indicated with an N/A where normally the WP responsible for the requirement would be indicated.

During the WP6 interaction analysis workshop WP6 also identified a number of technical requirements which might benefit from some further editing. Proposals for changes to these tecnical requirements were made to the respective WPs. WP6 also identified certain redundancies (overlap) among the legal requirements and these were resolved by integrating these requirements into separate new requirements.

As a follow-up to the requirements interaction analysis workshop, to further promote the integration of legal requirements with work by the technical WPs, WP6 provided each WP individually with the list of the requirements which are particularly relevant to their work. In other words, each WP was presented with a report in which they would only have to look at a subset of the WP6 total requirements list relevant to their technical objectives.

A number of additional legal requirements were identified during the workshop. Further, some of the requirements were added to avoid overlapping requirements and better address the complexities of the TAS^3 project. Further, some of the requirements were deleted, again to avoid overlapping legal requirements. The new, edited and deleted requirements are documented in Section B. The final refined list of requirements can be found in the Annex IV of Deliverable 6.1.

2.4.6 Validation of Requirements with the Architecture (I.8 and I.9)

The mapping of requirements to the architecture was repeated after the re-iteration and the completion of the interaction analysis. There is a danger in viewpoint oriented requirements analysis that global requirements are neglected in the process of consolidating the different viewpoints. The global requirements of TAS^3 were initially defined by WP2 and were not included in the Inter-WP interaction analysis. Hence, in a preliminary step of the mapping of requirements to the architecture we studied the mapping of global requirements to the TAS^3 architecture. We defined a template through which we mapped each of the global requirements to components in the architecture and identified gaps. The results of this mapping is documented in Section 7.

Finally, once the inter-WP requirements interactions and the legal-technical requirements

interactions were completed we validated all of these requirements by mapping them to the architecture. This activity consisted of reviewing each technical requirement for corresponding components in the architecture. During this activity gaps in the architecture, missing requirements and overlapping requirements were also identified. Further, the architecture team indicated where legal requirements were addressed in the different architecture components, identified gaps in the legal requirements and made suggestions for additional legal and technical requirements.

To conclude, we produced multiple viewpoints of the requirements of TAS^3. These viewpoints we used to scrutinize our requirements [4]; discover discrepancies between understandings of the different WPs, their responsibilities and interactions; and, most importantly, to identify the requirements that demand extra communication among the partners. Through these interaction analyses activities, we consolidated the different WP viewpoints and the architecture and finalized our technical, legal and application domain requirements.

2.5 Structure of the Document

The remainder of this document is organized as follows. We first define the overall objective of the TAS^3 project and state the objectives of each of the work packages with respect to the scope TAS^3 in Section 3. Next, we analyze the requirements interactions within each work package in Section 4 (see Appendix C and B for the requirements themselves). Following, we analyze the interaction of the requirements among the different work packages in Section 5. This is followed by the results of the analysis of the interaction of legal and technical requirements in Secion 6. In Section 7 we map the global requirements and in Section 8 we map the WP technical requirements to the architecture, and show which components will fulfill them. The inter-WP interaction analysis sections each include also references to gaps and assigns WPs to these where possible. In Section 9 we list existing solutions and the requirements that they fulfill, as well as an overview of the justifications for selecting specific solutions for the project. A detailed description of all the solutions that were candidates for use in TAS^3 are listed in Appendix D. In Section 10 we list the necessary steps to close the gap between those requirements that can be fulfilled using existing technology and research; and, those requirements that require further research and development and should be fulfilled within the TAS^3 project. Last, in the Conclusion, we summarize our findings and discuss plans for the next iteration of the Deliverable 1.2.

Part I

Deliverable 1.2: Requirements Assessment Report

3 Objectives of TAS^3 revisited

Today's globalized and interdependent economy is supported by distributed information systems and dispersed business functions and workforces. Society is changing fast as a result of fluctuating labor markets with shorter term contracts and increasing mobility. The concept of developing technologies according to the requirements of a specific environment – its application domain – is more important than ever, and yet, a greater challenge than ever. Previously a technology was defined to work in a specific environment. Now, the increased pace of change in technologies as well as in the environments in which those technologies are embedded requires an iterative and collaborative development process. Such processes have to consider both such changes from the beginning.

As a consequence of the increasing dependence of business and personal transactions on service-oriented technology, a key exigency for networks and service platforms is to be made trustworthy. According to the ICT Work Programme 2009-10[1] of the European Commission a trustworthy system is qualified as being "secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in security management". All the above aspects of trustworthiness are relevant in TAS^3 and find their place in the composing WPs.

Each of the above topics relies on a body of work that is surveyed in [25]. A key innovation in TAS^3 is the holistic approach that is taken. The approach combines trust concerns that are traditionally addressed within separate contexts in a unifying framework . Thus, for instance, because we take a user-centric approach, we need to consider access control mechanisms and functional compliance, trust and usability aspects together.

The key interacting parts of the TAS^3 ecosystem are technology, law and policy. Therefore, it is the objective of this document to start with the overall goal of the TAS^3 to develop a secure and trusted ecosystem and to refine that goal for each of the workpackages. The aim of this process is to document the interaction of the technical, legal and application requirements that make up such an interdependent ecosystem .

The overall objective of TAS^3 is defined in the Description of Work as follows:

> The overall objective of the TAS^3 project is to specify a trusted services network that advances the current state of the art of isolated solutions. These solutions are to respond to the challenges listed in the Description of Work. The scientific and technological objective of the project is to research and develop (1) a generic and fully published trusted architecture for securely shared personal data services and (2) a full implementation thereof using adaptable business processes.

In the following, we refine the objective of TAS^3 shortly summarized above for each of the workpackages. The objective of each work package is articulated with respect to the scope of the project also as they are defined in the Scenarios in Deliverable 1.4 [22] For each work package we also describe related solved and unsolved problems in the field of trust and security in service-oriented open and distributed environments. In some work packages the scope of the research and development questions are different i.e. WP9, WP10, WP12.

[1] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/ict-wp-2009-10en.pdf

The demonstrators have to address how to set up pilots so that they can link application domains to the TAS^3 architecture, such that they can test the feasibility of using TAS^3 in those domains, and elaborate new requirements to be addressed by the TAS^3, WP10 is concerned with the development of automated validation testing, while WP12 is concerned with integration activities. Hence, for these work packages the unsolved problems specific to their WP objectives are described.

3.1 Objectives of WP2

WP2 is made up of two teams, the Architecture Team and the VUB based team working on ontologies. The Architecture team, which is part of the WP2 has the objectives to normatively specify what it means to be TAS^3 compliant to the extent that the compliance can be technically specified. WP2 also has the objectives to describe technology in sufficient detail for a diligent implementer of ordinary skill, possibly even an implementer not participating in the TAS^3 consortium, to be able to implement the components of TAS^3 such that they interoperate; and, to configure the components into a working system that is TAS^3 compliant. The architecture will provide a framework and articulation that allows TAS^3 research topics to interrelate, communicate. Ultimately it will provide useful modules that integrate into a common whole that is TAS^3 compliant. Last, the architecture will satisfy general TAS^3 requirements as well as those requirements defined in this deliverable and Deliverable 1.4 [22] that are necessary to a complete secure and feasible system.

The objective of the VUB team, whose activities are also within the scope of WP2, is to develop an ontology on Security, Privacy and Trust for interoperability. The role of this ontology is to provide semantics that can then be attached (through annotations) to web services and business processes. Although several ontologies on security have been developed (e.g. NRL Security Ontology [1]), none of these have been developed on the basis of IT security standards (e.g. ISO standards). We believe that such standards provide a terminology and conceptualisation, which has been agreed upon by domain experts. Furthermore, none of these ontologies have included the aspect of Trust and Privacy within their framework.

3.2 Objectives of WP3

WP3 will provide a secure and flexible platform for business processes by developing process-oriented security concepts and an integrated model-driven approach to process management, involving both modelling and execution. WP3 will build on a stable modelling and execution framework of business processes in a service-oriented environment.

TAS^3 applications are based on executing business processes like the given example processes of APL or Mass-Layoff scenario [22]. Human actors such as coaches or employment candidates are involved in the process. The process cooperates with changing subprocesses (such as the selection of employability providers adequate to the candidates reputation or rank), or services (which provide access to shared personal data, e.g. certificates of a candidate in the APL scenario). We will provide security concepts, model elements and runtime enforcement mechanisms to support business processes that process personally-identifiable information in a privacy-preserving way. Further, we will provide concepts and mechanisms which support altering and adapting the schemas of running process

instances. These mechanisms will take into account properties of the process itself and of the available infrastructure, e.g., data involved in the process; privacy requirements of the user; quality requirements on the the outcome of the process. Thus processes will leverage the flexibility and openness of the TAS^3 architecture while staying secure.

In order to provide interoperability within the TAS^3 architectures, ontologies will semantically underpin the specifications of business processes, including their security properties and requirements.

Business Process Management in service-oriented environments is well supported by standards in this area. A standardized modelling language is given by BPMN, execution of business processes with web services are handled in a standardized way by BPEL (Business Process Execution Language (see D1.1 [25]). There exist first implementations of such business process management systems, mostly vendor-specific, but also a few open-source solutions.

Secure processes are still beyond the state-of-the art. Distinct standards in the web service area exist, like WS-Security, WS-Trust, etc. (see D1.1 [25]) but these are only for securing web services to a limited degree. Process security is not yet available in a sufficient manner (see for more details D1.1 [25] and D3.1 [23]). TAS^3 will support business processes in an open agile application environment that requires flexible and adaptable processes in a challenging manner. In particular, using security issues to guide and support adaptations of processes is a novel and promising approach. Modeling of business processes as means to capture security rules at the business level and deriving policies for the enforcement level is not yet sufficiently supported by existing tools. Model-driven-development as a general approach in software development will be applicable to tackle these issues. Adaptation of processes is a vivid research area but existing solutions only provide preliminary solutions. Some research approaches based on specialized theoretical process modelling languages with proprietary prototype systems exists, but these are mostly not for processes in service-oriented architectures. Overall, the TAS^3 architecture will be the first to provide a coherent solution for the security, adaptability and semantic interoperability requirements of business processes.

3.3 Objectives of WP4

The objective of WP4 is to propose the mechanisms that are necessary to successfully guarantee that information can be processed in a secure fashion that provides end-to-end security and end-to-end trustworthiness of the whole information processing process. These objectives will be achieved through the introduction of information containers with sticky policies that are stored in an authoritative repository that commit to enforcing these policies. We will also introduce audit and logging functions in order to enable oversight and recognize breaches of policies. Further mechanisms to map and identify information containers, policies, services, service consumers will support the objectives of the work package. Users will be supported in making decisions with respect to revealing their person information to trusted parties through mechanisms to discover service providers that meet and commit to adhere to privacy policies.

WP4 addresses the gap in research and development in existing service discovery mechanisms. These often only allow users to discover the functionality of potential service providers, but do not take into account their trustworthiness or their ability to commit to

enforce certain policies (e.g., authorization and obligations). Currently existing service oriented architectures are not able to deal with privacy enhanced identifier mappings. We will attend to these open problems in the activities of Work Package 4.

3.4 Objectives of WP5

The objective of WP5 is to create an expressive, flexible Trust Management (TM) framework, which leads to the following concrete objectives: (1) define a flexible TM architecture; (2) create an efficient TM policy evaluation engine; (3) provide Trust feedback mechanisms based on the evaluation of behavior, policy compliance and key performance indicators.

Services in the employability and eHealth setting rely heavily on personally identifiable information. To build user trust in such services, it must be possible for the users to select from a wide range of trust policies. Users' trust can be based on the credential presented by an entity on the past performance of the entity. Existing TM systems can be divided into two main categories: structural and behavioral. Credential based Trust Management (CTM) is a structural, rule based approach to managing authorization in environments where authority emanates from multiple sources. Session Trust Management (STM), which fits within the CTM setting, is an approach to dynamically manage authentication in distributed environments, where users may be authenticated by different mechanisms at different Identity Providers. Reputation Trust Management (RTM) is an approach to manage and dynamically update reputations based on the behavior of participants. Key Performance Indicators based Trust Management (KPITM) capture past behavior and can be used to build a novel behavioral trust metric. However, no existing framework combines these categories of TM systems.

Our aim is to create a trust policy framework, within the TAS^3 architecture, which is able to efficiently enforce a broad range of trust policies by combining CTM, STM, RTM and KPITM based trust metrics. As a basis for supporting structural trust we propose to use TuLiP [13]. This framework is flexible and provides guarantees for credential chain discovery, one of the main issues in this domain. Though the system provides a sound basis open issues exist ranging from technical, e.g. the support for standardized attribute credential formats, to foundational, e.g. delegation control; what does delegating a decision imply. As a basis for supporting behavioral trust we propose to use computation of centrality measures within a database setting such as the Oracle database. Centrality measures [28, 16, 19, 20, 24] are graph algorithms which can be used to find the most trustworthy participants based on the feedback [17, 29]. What is missing is a flexible framework which allows the user to select their preferred metric. We plan to create this by defining an algebraic language with support for centrality measures along with methods to evaluate this on a database of feedback data.

3.5 Objectives of WP6

The objective of Work Package 6 is to enable trust through developing a contractual infrastructure that supports and binds technology platforms with organizational policies and defines, supports and binds organizational as well as individual obligations. The contractual framework is designed to meet or exceed requirements of the relevant privacy and sectoral laws. The Framework will be composed of Infrastructure or ecosystem level requirements

as well as requirements at the individual and transaction level. The latter will be divided between service providers with a direct relationship to the individual and those that only interact with other service providers.

The need to enable trust requires that individuals have faith in their service providers to properly manage and secure their information. Previous attempts to do this purely in technology, P3P, EPAL have met with limited success and provided limited scope solutions. Purely contractual solutions have likewise met with limited success at the individual level because of the difficulty in understanding legal drafting. On the business side, todays more global infrastructures make maintaining complex contractual infrastructures and ever increasing and untenable burden. These problems remain at best partially addressed in both the contract and technology realms.

The TAS^3 infrastructure addresses these problems by collaboratively developing contracts, policies and technology and allowing them to interface in a manner that is designed to be mutually supportive. This collaborative development model, which reaches down to contractually enabling sticky policies, provides a significant evolution in both contractual and technology development models. It must be recognized that this level of interdependence and planning at the design stage increases complexity and burden of development but should yield significant benefits in operation and compliance. Furthermore, this collaborative model enables requirements needed for legal compliance to be prebuilt into technology (audit trails etc) while addressing limitation of some technical implementations in policy and contract. These are the solution basis of work package six which will be elaborated in the contractual frameworks.

3.6 Objectives of WP7

The overall objective of WP7 is to build a fully dynamic privacy preserving authorization infrastructure that allows credentials to be dynamically created, revoked, delegated and aggregated as necessary between users, administrators, and processes. This infrastructure should be easy to use for service oriented applications in order to achieve wide deployment of the TAS^3 architecture. The infrastructure should enable the dynamic management and update of authorization and privacy policies. It is our goal to incorporate sophisticated real-life authorization requirements such as Break the Glass policies, dynamic separation of duties, state based decision making, resolution of conflicting policies and adaptive audit controls. And last but not least, WP7 wishes to contribute to international standards development in the area of IdM and authorization protocols and profiles and authorization ontology.

Partial solutions exist in the field of service oriented authorization. For example SAML allows short lived credentials to be dynamically created but does not support long lived credentials or revocation. PERMIS supports credential aggregation, but only when the user has the same name at the different credential issuing sites. PERMIS, SAML and X.509 support credential delegation but not in a privacy preserving manner. PERMIS supports state based decision making and separation of duties but the policy language is not standardized. None of the solutions above have implemented the Break the Glass policies in an application independent manner.

Many papers have been published on dynamic delegation of authority between users and processes [2, 3, 7, 9, 11] but no open source software currently exists that provides this general purpose functionality for service oriented architectures. Further, a standardized lan-

guage for expressing obligation policies is still lacking, and no general purpose obligation enforcement infrastructure exists. There is no recognized model, architecture or infrastructure for the support of sticky policies. This includes the lack of a standard protocol for passing policies to PDPs along with authorization decision requests. Such a standard is necessary to enforce sticky policies, an important stepping stone for implementing an authorization infrastructure that enables flexible and easy implementation of data protection obligations.

3.7 Objectives of WP8

The main objective of WP8 is to provide a uniform interface to allow service providers and service requesters to access TAS^3 in a standardized manner. WP8 builds the gateways for applications like business process engines, web front-ends or repositories to access the TAS^3 infrastructure. We also deliver the base components for the pilots; so that they can connect to TAS^3 and exchange information in a TAS^3 secured and trusted way. This also means that our two gateway services on service requester and on service provider side need to be TAS^3 aware and hence they also have to cope with authentication and authorization protocols. Those gateways will not only route things from one side to the other. They will als transform, aggregate and disaggregate the sent payload and attached policies.

In the first iteration or phase of TAS^3 the interface will be experimental. Later on well divide this component in an application dependent and application independent part (WP7 is working on the application independent part of the Requester and Responder PEP). The application dependent part is necessary to support special classes of applications (BPEL engines, Repositories). This gateway will be provided as web service because the whole TAS^3 infrastructure is based on the SOA (Service Oriented Architecture) approach. Beside those mentioned gateways, Risaris (partner in WP8) will extend and adapt their SOA gateway to allow legacy systems (especially legacy databases) to be integrated in TAS^3 . By that, it will be possible to access also older datasets.

Another task in Work Package 8 is the adaptation of a repository, so that it can handle person related data. This is something new in the world of repositories, because normally repositories store digital assets that belong to the domain of libraries. The storage and modification of person related data brings new requirements to a conventional repository, which have to be taken into account and need further implementation and adaptation of existing repository functions.

3.8 Objectives of WP9

The objective of the three demonstrators in Work Package 9 is to prove the generic applicability of the TAS ^{3} trust infrastructure for exchanging personal information in different domains. More specifically it is the objective of the pilots to demonstrate the trust, security and privacy services required to deliver major reforms of vocational education and lifelong skills development through partnerships of education/training providers and employers and required to enable information exchange within eHealth and ensure patient empowerment. In the pilots the TAS ^{3} infrastructure as a whole and the different components specific to each pilot will be tested in relation to the needs, demands and concerns of both end-users and the registered service providers.

Until now personally identifiable information (PII) has been mainly used by and stored on behalf of corporate, institutional and service provider driven processes. We are entering a world however, where the emphasis is shifting from organization to the individual, and the control of users data is following suit.

In general, users perception of trust and security of the internet and electronic data exchange has decreased in recent years. Several significant episodes of loss, theft and abuse of personal sensitive data in different EU countries (see details in [25] Chapter 13.2)), have aroused mistrust in users who might otherwise see the benefits of sharing PII in this way. In Holland 2.6% (438,000 as of March 2009) of citizens have lodged objections to participation in the EPD (Electronic Patient Record). While most opponents do not object to data exchange per se, they do not trust the security of the systems used and consider that they have insufficient control over their PII. It is to be anticipated that similar issues will arise with the increasing use of ePortfolios not only to support educational processes but also to support lifelong employability. See also [25] Chapter 13.2. Until now there have not been significant or successful attempts to resolve the issue of mistrust in security on the use and exchange of employability-related personal data. Work Package 9 will benefit from the work of other partners to build a trustworthy and secure infrastructure for the exchange of highly sensitive personal data in employability and healthcare. Conversely, the other work packages will benefit from the WP09 demonstrations to prove their trust and security solutions and empower restoration of trust to users and other stakeholders.

3.9 Objectives of WP10

Work Package 10 aims at ensuring quality and trustworthiness of the handled business processes and of service provision. The goal of WP10 is thus to develop and implement a comprehensive validation methodology of the TAS^3 platform and its offered services. In particular, WP10 will work towards validating the functional and QoS compliance of services that participate in a TAS^3 choreography and will contribute to enhance the trustworthiness of the TAS^3 ecosystem with:

- a novel framework for on-line service testing that will be seamless embedded within the TAS^3 architecture; such a framework will strengthen service registration by a preliminary verification session and will enforce services to abide by their manifested policies by periodic compliance testing and negative/fuzz testing;
- support for verification of compliance to manifested access policies by automated derivation of XML documents (maybe XACML) from XML Schemas

The fulfilment of the above objectives requires research and development in model-based automated testing of service-oriented compositions and in XML-based modelling and transformations.

From an end-user perspective, the objective of WP10 is to develop measures to ensure Perceived Quality and Trustworthiness of the TAS^3 platform and its offered services. In particular,

- Measure usability and trust levels of TAS^3 architecture.

- Measure perceived quality of service in terms of usability, security, privacy, satisfaction and trust.
- Analyze the influence of previous concepts on the end-user intention to use the system.
- Measure accessibility levels of TAS^3 architecture.

The success of any information system architecture must be based not only on technology schemes, standards and protocols, but also on users' perceptions [5]. Indeed, services are used by a wide spectrum of end-users, who will probably have a diverse expertise, so that the correct measurement of end-user perceptions has acquired a great relevance in this context. Thus, in order to convince end-users to use a given infrastructure, their perceptions regarding ease of use, trust and performance must be taken into proper account [12]. Also the capability to easily access services becomes important for trustworthiness [14]. Broadly speaking, in any service-oriented applications, also in the eHealth and in the employability context, the provided services must be developed according to the user perspective [6]. However, to date, most of research on quality of service and trust is technologically oriented. It is at this point where Unizar contribution to WP 10 becomes especially relevant. In particular, Unizar can provide TAS^3 a non-technical approach; that is, specific methodologies to measure end-users perceptions (usability; service quality and global trust perceptions), as well as understanding precursory factors and outcomes of all these aspects. As a result it will be possible to establish guidelines in order to increase the levels of usability and end-users trust. Moreover, accessibility will be considered as a fundamental requirement of TAS3.

3.10 Objectives of WP12

The main objective of WP12 is to assure that there will be a coherent end result of all the development work, instead of ten incompatible mini systems. Specifically, it is the objective of WP12 to ensure that all developed software modules, and all work performed by WP110, maintain a close fit and integrate with the overall TAS^3 project. WP12 activities will also define, document, implement, and manage interfaces between the core technical modules (i.e., trust layer: WP3-7, application layer: WP8); integrate the trust layer with the employability and eHealth application layers (WP89); and test the TAS^3 system as a whole on functionality, performance and manageability, usability and effectiveness, and adaptivity.

It follows that WP12 is not a design or development work package. As such, it does not bring core components, models, interfaces, architectures, or prototypes to the project. These tasks are in the scope of WP1 – WP10.

A major activity to assure coherence is that the primary WP12 contributors thoroughly study nearly all components and the complete system. This is an underground task which does not lead to any visible deliverable, so it is very unrewarding. A good understanding allows WP12 management to question and direct the contributions for easier and better integration. This is one of the major reasons to have both Architecture and Integration under the same cluster lead. At the same time it allows WP12 to keep a close eye on the proper documentation of interfaces, requirements, components, and test beds. It is expected that WP12 needs to monitor the central issue registration as well, and even moderate it and

assure proper feedback to and from developers. When demonstrators come online, WP12 will be the core WP to bridge the gap between the demonstration and a loose collection of security components.

4 Requirements interaction in TAS^3 Work Packages

In this Section, we do an analysis of the requirements from each of the work packages. As we mentioned in the Introduction, we sent a template out to the TAS^3 partners, in which we asked them to also provide us with a refined set of requirements for their activities in their work packages. These requirements are now listed in Appendix C. The requirements template is in Appendix A. Specifically, we will analyze the interactions among the work packages requirements in order to partition the requirements into related clusters, determine the requirements of higher priority, and to become aware of singular requirements and possible missing interactions or requirements. We have asked all partners to do interaction analysis when they elaborated their work package requirements.

We visualize the requirements interactions using directed graphs. Further, we denote the responsible teams for each of the requirements. We do the latter by drawing circles labeled with the name of the team around the requirements that belong to each team in the work package. In case there is only one team in the work package, we label the circle simply with the number of the work package.

The interactions between the requirements are denoted on the edges of the graph. The labels of the edges denote the kind of interaction: source requirement depends on target requirement is denoted with a D, where the head of the arrow points to the target requirement. Further labels using the same reading direction are S for supports, I for implements, A for abstracts and C for conflicts with. We especially wanted partners to articulate possible conflicts, since we see them as a way of discovering either under-specification, communication needs, or improved design needs.

When we received the interaction analysis results, we did notice different interpretations of our controlled vocabulary. That a requirement A supports another requirement B did not always mean that B is dependent on A. Therefore, supports was sometimes used in the sense of ”strengthens” rather than ”is a condition for”. Further, a requirement could implement many other requirements, or a requirement could abstract many implementing requirements. We will integrate this knowledge into the next iteration of the Deliverable 1.2. For now, this means that the interactions between the requirements are not bi-directional e.g. supports does not imply depends and vice versa.

4.1 Requirements Interaction in WP3

The analysis of requirements interaction shows that one of the main requirements of WP3 is to make it possible for process designers to specify the assignment of tasks to actors in a business process in a sufficiently abstract, flexible and secure way, using roles for grouping tasks and responsibilities (D1.2-3.5), which is implemented by the requirement D1.2-3.6 which states that business process providers (in general: coordinators of a complex service) must be able to control who performs a task, by binding authorization to perform a task and access necessary resources to roles. D1.2-3.6 also implements the tools to define (graphical) models of their business processes including the interactions of the process with external components, i.e. web services and human activities (web interfaces), and other business processes (D1.2-3.1).

Another requirement which is important for WP3 activities is about the recovery of busi-

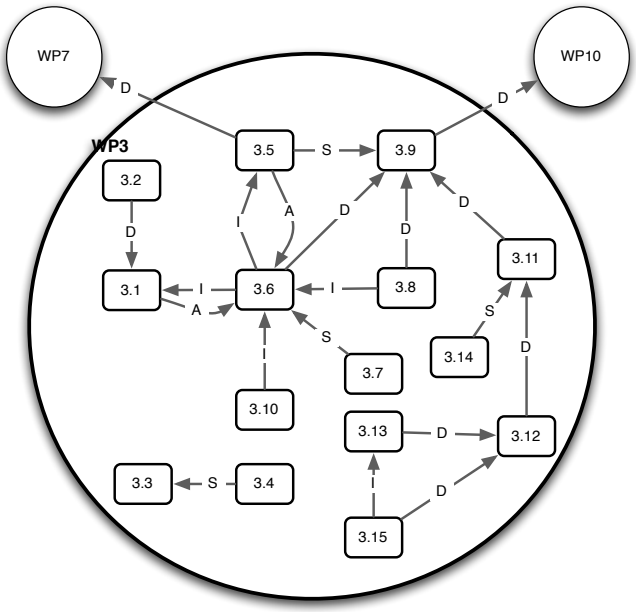

Figure 4.1: WP3 requirements interaction

ness processes from error situations (D1.2-3.9). The errors that may be generated by the security requirements such as authorization for tasks (D1.2-3.6), mutual exclusion between roles (D1.2-3.8), and, user access control on PII including service provider compliance with it (D.2-3.11) need to be handled properly and hence depend on D1.2-3.9. The fulfillment of this requirement also depends on interactions with the requirements of WP10.

Further dependencies exist between the requirements in order to provide secure (D1.2-3.15) adaptable processes (D1.2-3.13) and the requirements for business processes to receive interoperability information with respect to services and business processes as well as privacy policies of other service providers (D1.2-3.12). The latter is also dependent on the ability of users to specify on which of their PII the process should have access, and, the service providers abilities to discover for a particular piece of PII which user settings apply and whether the PII is particularly sensitive (D1.2-3.11).

Further interactions of the WP3 requirements with the requirements of other WPs is analyzed in Section 5.

4.2 Requirements Interaction in WP4

According to the interaction analysis, the possibility to demonstrate to lay users the complex security and trust features of the TAS^3 (D1.2-4.3) and the ability of providers to prove that they processed the information and services in accordance to the required policies (D1.2-4.4) are the two central high-level requirements of the work package. These two requirements depend on all the other requirements in the work package.

Most central with respect to dependencies are the requirement to make the discovery service and policy management system user friendly and easy to configure and use (D1.2-

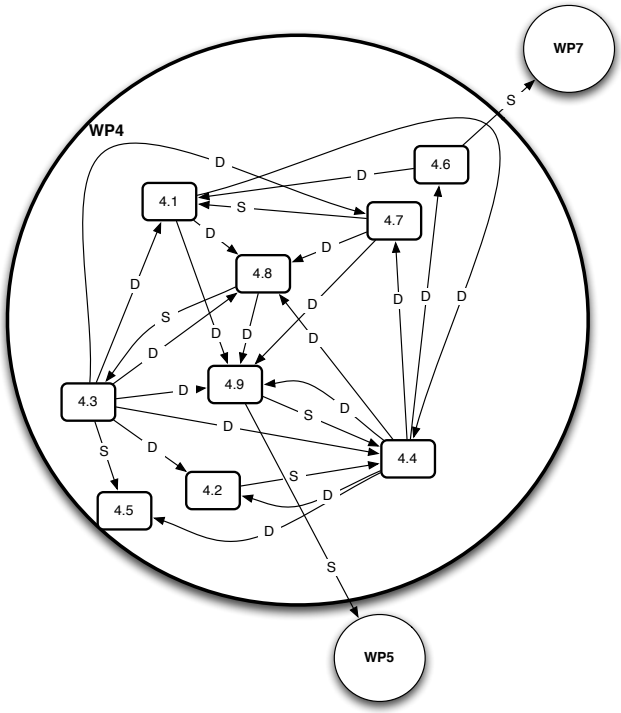

Figure 4.2: WP4 requirements interaction

4.8) and the requirement to take trust and reputation scores of both service consumers and providers into account in the discovery service (D1.2-4.9). Since so many of the other requirements and the two high-level requirements depend on these two requirements, they should be prioritized in the WP.

D1.2-4.9 supports the trust management system in WP5 while the requirement on access under exceptional situations (D1.2-4.6) interacts with the requirements of the break the glass functionality as implemented by WP7. Further interactions of the work package are defined in the inter-WP requirements interaction analysis in Section 5.

4.3 Requirements Interaction in WP5

The requirements of WP5 are strongly interdependent, see also Figure 4.3. Requirement D1.2-5.1 is the higher level requirement that states that the trust management system shall answer to trust policy evaluation requests which can use different sources of trust. Most other requirements support D1.2-5.1 or are refinements thereof. User authentication is also a central requirement which is a pre-condition for the fulfillment of all the WP5 requirements. The development and implementation of secure and privacy preserving user authentication within the TAS^3 architecture is the responsibility of WP7. Hence, WP5 has a strong dependency on WP7 and the authentication solution they provide.

Another important requirement is D1.2-5.3 which describes the need for a reputation based trust management system. This is supported with requirements regarding business

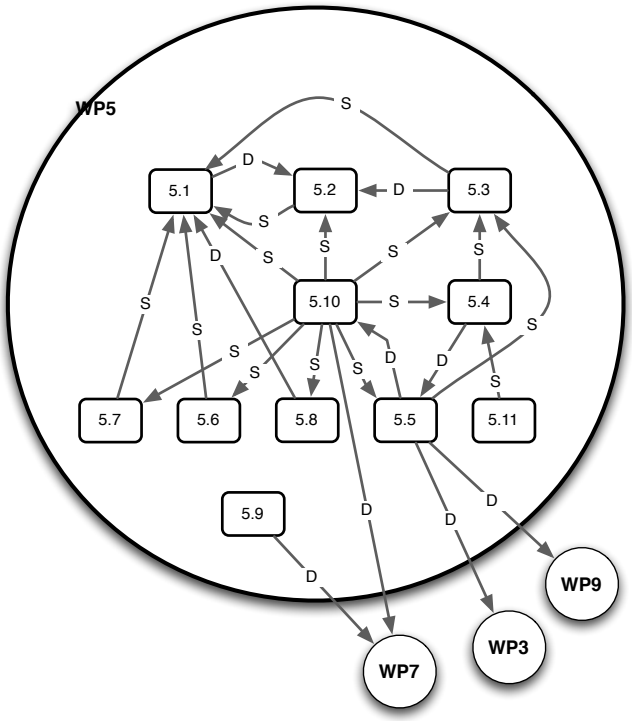

Figure 4.3: WP5 requirements interaction

processes that provide trust feedback opportunities (D1.2-5.5), support for gathering reputation feedback (D1.2-5.4) and legal/contractual models to support the feedbacks and recommendations of the trust management system.

The work package has two other requirements which have dependencies on the requirements of other work packages. Specifically, the fulfillment of D1.2-5.9, which is about trust policy formulation support, depends on the research and development activities in WP7. Requirement D1.2-5.5 on trust feedback opportunities within the business processes will depend on activities of WP3 and the domain specific needs of the demonstrators in WP9. The detailed relationships between those requirements and the requirements in WP7 and WP9 will be presented in Section 5.

4.4 Requirements Interaction in WP6

WP6 requirements are divided into three sections: Intake, Legal Requirements and Contract Fraemwork.

- D1.2-6.1 – 6.2 are the intake and qualification requirements these are the processes for qualifying/verifying prospective users and screening/validating service providers to assess their ability to comply.
- D1.2-6.3 – 6.12 are the basic legal requirements that either emanate from the Data Protection Directive or a needed to give effect to those requirements (complaint handling, compliance, etc)
- D1.2-6.13 – 6.17 are those sections that provide for or give effect to aspects of the contractual and policy framework.

The Intake processes are needed to assure that individuals are validated in the architecture and there is a mechaism to provide them with notices and an opportunity to develop their privacy polices and exercise choices. In this aspect, the intake process will work in conjunction with the user interface. The organizational or service provider intake process is of a more rigorous nature and goes beyond just idetifying organizations to the system, but rather assists in qualifying their ability to comply. Both of these elements are necessary predicate functions to assure that both legal requirements will be complied with and that the contract framework will be honored.

The requirements of the Directive are interlinked and both support and depend on each other by defintion. All the bidirectional edges in Figure 4.4 stand for this interdependency and are not labeled for readability reasons.

When data is going to be collected, then data subjects need to consent (D1.2-6.6, D1.2-6.7) to the data that is going to be collected. The consent is usually limited to the use of the data for a specific purpose (D1.2-6.5). The collected data should not be more then necessary to complete the business function (D1.2-6.4). This all needs to be enveloped in a notice (D1.2-6.3). Further, audits will be put in place so that activities that are not compliant with respect to the collected data can be captured (D1.2-6.9), the necessary redress processes can be put into place (D1.2-6.10). An underlying helping mechanism here enables the users to make requests for access (D1.2-.8).

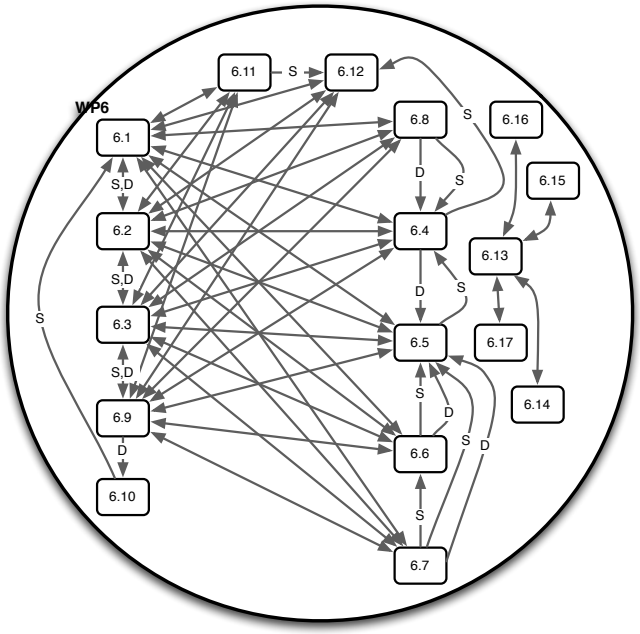

Figure 4.4: WP6 requirements interaction

The notice requirement (D1.2-6.3), together with the Intake Process requirements, through which all users (D1.2-6.1) and organizations (D1.2-6.2) are identified are overarching requirements that depend on and support all other requirements for data protection and legal compliance to be executed. All of these requirements are supported through two horizontal security requirements with regard to confidentiality, integrity and availability of data(D1.2-6.11, D1.2-12).

The legal requirements as identified above while madated by law need to be made operational. TAS^3 has tried to create an innovative development model by coordinating and integrating the development of technology, policy and contract. All three elements play a role in compliance with the identified legal requirements. The policies help define minimum practices that service providers will comply with and the contractual framework will bind all the parties to their obligations and enable individual rights.

A focal point of this compliance is thus the execution of the contract creating the binding (D1.2-6.13). The contract requires the use of TAS^3 technology (D1.2-6.14) and acceptable policies (D1.2-6.15) and evidences the acceptance of the agreement to be bound in general (D1.2-6.16) and pursuant to technical elements and process (D1.2-6.17).

The legal and Contract Framework requirements interact with all the other work packages of the TAS^3 project. These interactions will be picked up later in Section 5. Futher, the requirements for WP6 have been refined after the completion of this deliverable. These refinements can be found now in D1.4 [22] under the legal requirements in Section 6. We will integrate these changes in the next iteration of this deliverable.

4.5 Requirements Interaction in WP7

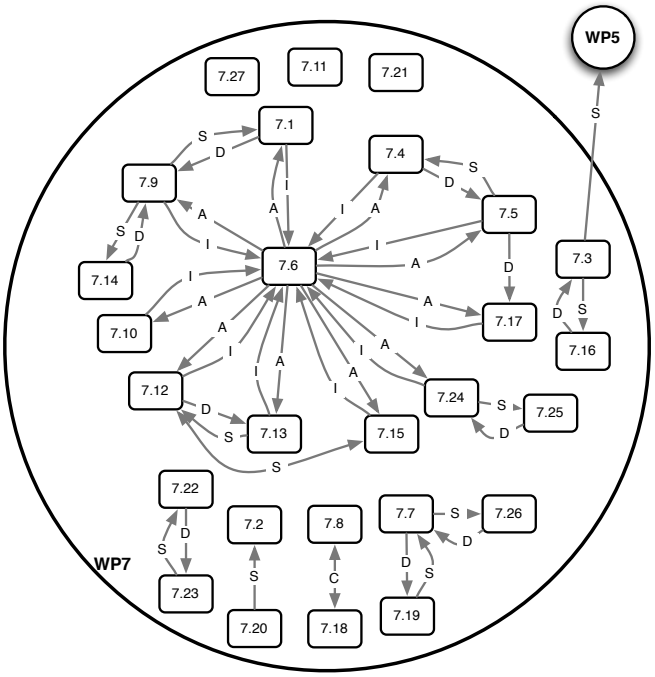

Figure 4.5: WP7 requirements interaction

Most of the activities in WP7 are focused on the authorisation of user activities (D1.2-7.6) in TAS^3 based on trust and privacy policies. There are many dependencies among the requirements that implement the authorisation. The ability for users to delegate activities to other users (D1.2-7.1), and comparably, the ability of service providers to delegate activities to other service providers (D1.2-7.14) depend on the feasibility of revoking the delegation credentials (D1.2-7.9). In order to be able to pull user credentials on demand (D1.2-7.12) depends on the ability of the service providers to locate those credentials (D1.2-7.13). This process is further supported by the ability of users to push credentials to the system dynamically (D1.2-7.15).

Implementing audits is part of WP7's activities. The audits need to be adaptive to changes in the system (D1.2-7.25) which depends on the secure implementation of the authorisation audits (D1.2-7.24). The authorisation system will also implement a break the glass policy (D1.2-7.22) that requires the authorisation system to make decisions based on the current state of the application or system (D1.2-7.23).

Users must be able to provide consent for the use of his private data and credentials in TAS^3 (D1.2-7.26). In order to achieve this, the user must be able to dynamically set his/her privacy policies (D1.2-7.7) which depends on the service providers being able to update their policies dynamically without having to bring down their systems (D1.2-7.19).

User in TAS^3 should be able to use different pseudonyms in order to protect their privacy (D1.2-7.16) and each of these pseudonyms should be implemented such that it should be possible for users to prove who s/he is to any service provider (D1.2-7.3). The opposite, the

authentication of the service provider (D1.2-7.3) to the user and other service providers is also a requirement of WP7.

The work package members have also noted a potential conflict between two requirements. The first requirement states that service providers should not be able to link together the sequential requests of a user without the users consent (D1.2-7.18). When there is a consent, the requirement may conflict with another requirement which states that different service providers should not be able to collude together to determine who a pseudonymous user is without the users consent (D1.2-7.8).

The authorisation mechanisms developed by WP4 are central to TAS^3. There is also a close interaction between the trust management system provided by WP5 and the requirements of WP7. The detailed relationships between those requirements and the requirements in WP5 and other related WPs will be presented in Section 5.

4.6 Requirements Interaction in WP8

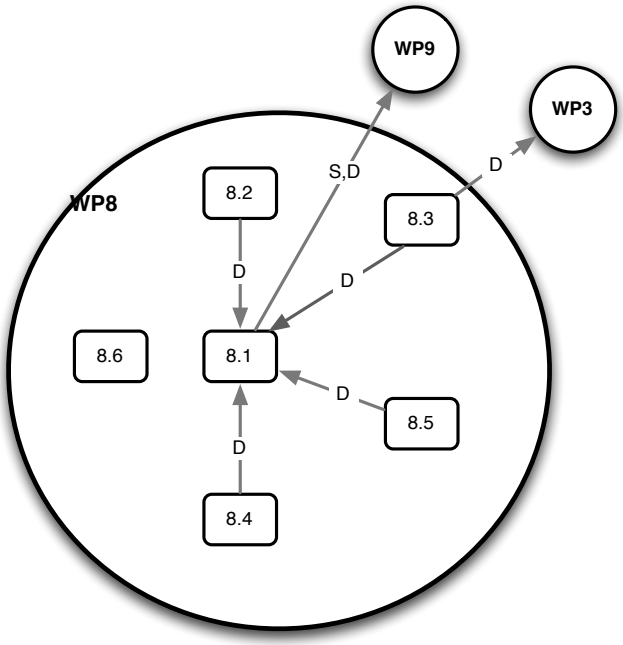

Figure 4.6: WP 8 requirements interaction

The central requirement for WP8 is to build a gateway for the demonstrators to be able to access TAS^3 (D1.2-8.1). All further requirements depend on this specification of the gateway.

These other requirements are as follows: on the legacy side, there is a requirement for an interface so that legacy databases can provide their data and service to TAS^3 (D1.2-8.2). On the user side the requirements are to allow end users to access TAS^3 functionality through a business process (D1.2-8.3) and through a generic client (D1.2-8.4); to make it possible for end-users to access and manage their policies (D1.2-8.5); and, to store and modify their

data stored in repositories in TAS^3.

The WP8 will support requirements of WP9, while it will also depend on their requirements. The business process related requirements will require interaction with WP3. The detailed relationships between those requirements and the requirements in WP9 and any other related work packages will be presented in Section 5.

4.7 Requirements Interaction in WP9

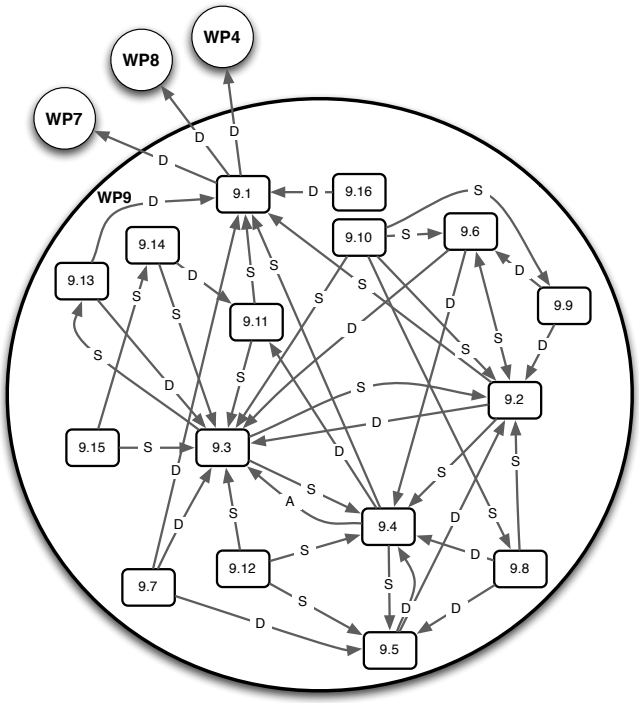

Figure 4.7: WP9 requirements interaction

The main requirements of WP9 are focused on the needs of the user and the protection of his/her data. The demonstrators will make use of TAS^3 to make sure that processes used in the demonstrators have secure access to data drawn from a variety of distributed sources, and are only be able to access the specific data they need (D1.2-9.1). They will make use of the TAS^3 architecture to enable users to set, view, control and change policies for their data at a variety of levels, down to the lowest (field) level, from accepting clearly-formulated preset policies to adding fine-grained policies to specific sets of data; the users must clearly understand the implications of this policy choice (D1.2-9.2).

Further, users have to be securely authenticated and authorised before any access to data is allowed (D1.2-9.4) and the access to the system must be easy, without the need for overly complex authentication and authorization processes (D1.2-9.3). And, in line with data protection measures, the demonstrators will require a secure and reliable audit trail showing who accessed user PII, when and for what purpose, and whether any changes were

made (D1.2-9.5). All other requirements of the work package support or depend on these requirements. The detailed relationships between these requirements and the requirements in WP8 or other related work packages will be presented in Section 5.

4.8 Requirements Interaction in WP10

WP 10 is made up of two groups whose requirements are not interdependent. For UNIZAR all the requirements are related to user evaluation of different quality aspects of the TAS^3 architecture. Since they need an interface to do the user studies they are dependent on the user interfaces that will be developed by the demonstrators in WP 9. In further refinements of the requirements it is possible that UNIZAR delivers specific requirements to WP9 with respect to building testable interfaces and vice versa. Changes made to the interfaces of the WP9 are likely to effect the user tests executed by UNIZAR and need to be communicated.

The requirements of the CNR team have internal dependencies. An analysis of the dependencies shows that the accompaniment of services that are to participate in a TAS^3 choreography with models describing their characteristics (D1.2-10.8) is of greatest importance. All other CNR requirements, except D1.2-10.3, depend on D1.2-10.8. It is important to note that the fulfillment of requirement D1.2-10.8 itself depends on the rest of the TAS^3 WPs. Another dependency is between the requirement for identifiable error messages (D1.2-10.3) and other TAS^3 work packages, with a strong interaction with WP2.

An analysis of inter-WP requirements interaction will reveal the exact requirements interaction between the requirements of WP10 and the requirements of other work packages.

4.9 Requirements Interaction in WP 12

The WP12 is responsible for the integration of the TAS^3 architecture work packages. Hence, it is a requirement to provide all project partners with a single, central place where all known issues and defects of all components are administrated (D1.2-12.23) and where all developers, testers, and users can test and understand signicant parts of the complete system at least at the conceptual level (D1.2-12.1). This also means that change management will have to be enforced on core integration resources (D1.2-12.21). Requirements D1.2-21 and D1.2-2.23 have to be balanced out with the needs of participants to choose when and how to perform their contractual duties (D1.2-12.3). In cases of conflict and important and/or urgent events there will be a hierarchical escalation to raise these to organisational levels above non-responsive ones (D1.2-12.4).

In order to support the integration objectives, all developers, testers, and users must have access to all project documentation regardless of origin, target audience, or assumed relevance (D1.2-12.2). All participants must also check released components for correct operation in the network environment and developers must be kept up to date as of the performance of their released component. All other requirements of WP12 support or depend on these requirements.

The WP interacts with all other work packages hence we have left out the interaction of the requirements with other work packages.

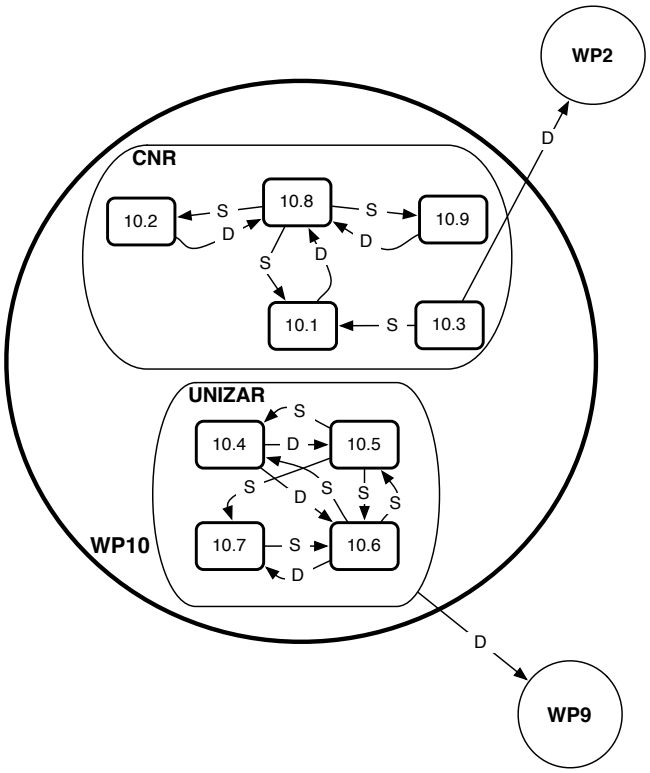

Figure 4.8: WP10 requirements interaction

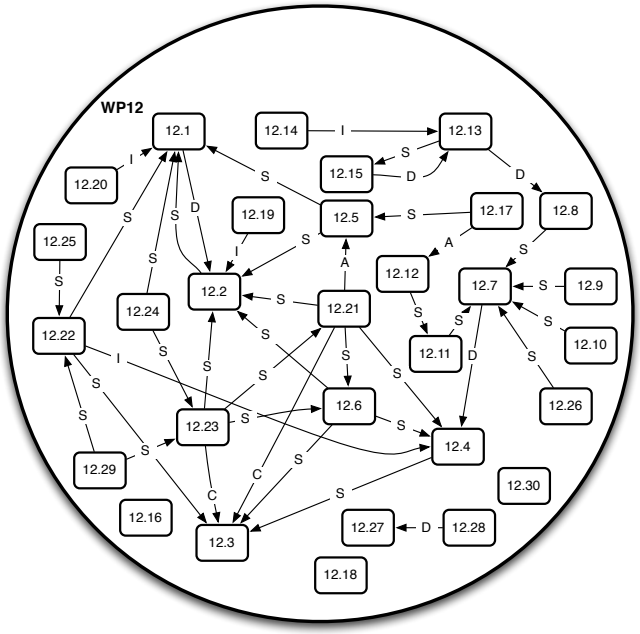

Figure 4.9: WP12 requirements interaction

5 Inter-Work Package Technical Requirements Interactions

It is our objective to complete interaction analysis so that we can consolidate the viewpoints of the WPs, and check for completeness with respect to the global requirements, legal requirements and the architecture. The analysis maps out the interdependencies between the work packages, and hence helps to find the inconsistencies between the WP requirements viewpoints. This chapter provides an overview of the activities that technical WPs completed with respect to the interaction of the technical requirements. Later in Chapter **??** we present the results of the analysis of legal and technical requirements interaction and the final mapping of legal and technical requirements to the architecture.

We completed the following activities for inter-WP technical requirements interaction analysis (the number refer to the overview of interaction analysis activities depicted in Figure 2.1:

Elicit inter-WP requirements interactions (I.2): for the inter-WP requirement interaction analysis we asked each WP to complete Template 2 in Appendix A. The results were included in the first iteration of D1.2, we have now moved them to Appendix E.

Map WP requirements to architecture (I.3 and I.4): we mapped all the technical and legal requirements to the architecture and captured inconsistencies. The results of this first mapping are now in Appendix E.

Reiteration of inter-WP requirements interactions (I.5): we used the first iteration of the inter-WP requirements interaction and mapping of requirements to the architecture as input for the second iteration of the inter-WP requirements interaction analysis. We started with the analysis of requirements that were indicated as being ”similar” and asked WP partners to communicate with each other to determine whether the similarity is due to a requirements overlap or due to differences that were not clear from the formulation of the requirement. The details of this activity are described in Section 5.1. We then updated the requirements list according to the results of the similarity analysis. We also updated the legal and technical requirements list after the re-iteration of the requirements elaboration. We then asked the partners to re-iterate the requirements interaction analysis. We then analyzed the results for inconsistency candidates and these were then discussed and resolved during a workshop with all partners. The details of these activities are in Section 5.2.

5.1 Similarity Analysis

In order to complete the similarity analysis, we first used the DOT language to represent the interactions between the requirements. These are in the following format:

“Requirement 1” → “Requirement 2” [label = “Type of interaction”]

We call ‘Requirement 1’ the source and ‘Requirement 2’ the target requirement. The interaction is indicated by the owner of Requirement 1, i.e., the WP from which the requirement originates. Below is the DOT format representation of the similarities identified during the first iteration of the Inter-WP requirements interaction analysis.

"D1.2-3.12" → "D1.2-2.14" [label = "Sim"];
"D1.2-9.11" → "D1.2-2.23" [label= "Sim"];
"D1.2-3.12" → "D1.2-2.23" [label = "Sim"];
"D1.2-9.8" → "D1.2-2.22" [label= "Sim"];
"D1.2-9.13" → "D1.2-2.18" [label= "Sim"];
"D1.2-9.13" → "D1.2-2.19" [label= "Sim"];
"D1.2-5.10" → "D1.2-3.4" [label = "Sim"];
"D1.2-3.12" → "D1.2-4.7" [label = "Sim"];
"D1.2-9.4" → "D1.2-5.10" [label= "Sim"];
"D1.2-9.7" → "D1.2-6.8" [label= "Sim"];
"D1.2-9.8" → "D1.2-6.8" [label= "Sim"];
"D1.2-9.3" → "D1.2-7.5" [label= "Sim"];
"D1.2-5.10" → "D1.2-7.3" [label = "Sim"];
"D1.2-9.4" → "D1.2-7.3" [label= "Sim"];
"D1.2-9.4" → "D1.2-7.6" [label= "Sim"];
"D1.2-9.9" → "D1.2-7.7" [label= "Sim"];
"D1.2-9.8" → "D1.2-7.11" [label= "Sim"];
"D1.2-9.5" → "D1.2-7.24" [label= "Sim"];
"D1.2-9.2" → "D1.2-8.5" [label= "Sim"];
"D1.2-9.7" → "D1.2-8.6" [label= "Sim"];
"D1.2-3.11" → "D1.2-8.5" [label = "Sim"];
"D1.2-3.11" → "D1.2-9.6" [label = "Sim"];
"D1.2-5.10" → "D1.2-9.12" [label = "Sim"];
"D1.2-9.10" → "D1.2-3.3" [label= "Sim"];
"D1.2-9.10" → "D1.2-4.8" [label= "Sim"];
"D1.2-9.10" → "D1.2-8.4" [label= "Sim"];
"D1.2-9.13" → "D1.2-7.6" [label= "Sim"];

In order to resolve these similarities, we took the following steps:

Step 1: ask the owner of the target requirement to state whether they agree with the similarity between the two requirements

Step 2: If the owner of the target requirement agreed, then the two requirements are declared redundant and one of the requirements is deleted. If no agreement is available, then the owner of the target requirement is asked to propose changes they found necessary to avoid the redundancy. The partners could also indicate if they had a justification for the redundancy.

Step 3: ask the owner of the source requirement to validate the proposed solution.

Once these four steps were concluded, we updated the requirement set with their conclusions and the second iteration of the requirements elaboration. Then the partners were asked to re-iterate the interaction analysis. The results of the second iteration of the inter-WP interactions analysis is provided in Appendix F in DOT notation.

5.2 Inconsistency Analysis

Once the second iteration of the requirements interaction analysis was completed, we used our inconsistency detection tool to look for inconsistency candidates due to the patterns described in Section 2. Figure 5.1 provides a screenshot of one round of results from the inconsistency detection tool. The figure shows homogenous interaction cycles with the relationship type “support”. The existence of multiple edges between two nodes indicates that there are multiple support cycles. During the requirements interaction workshop all partners analyzed the set of requirements that produced the cycles and negotiated the re-definition of the requirements so that the inconsistencies were resolved.

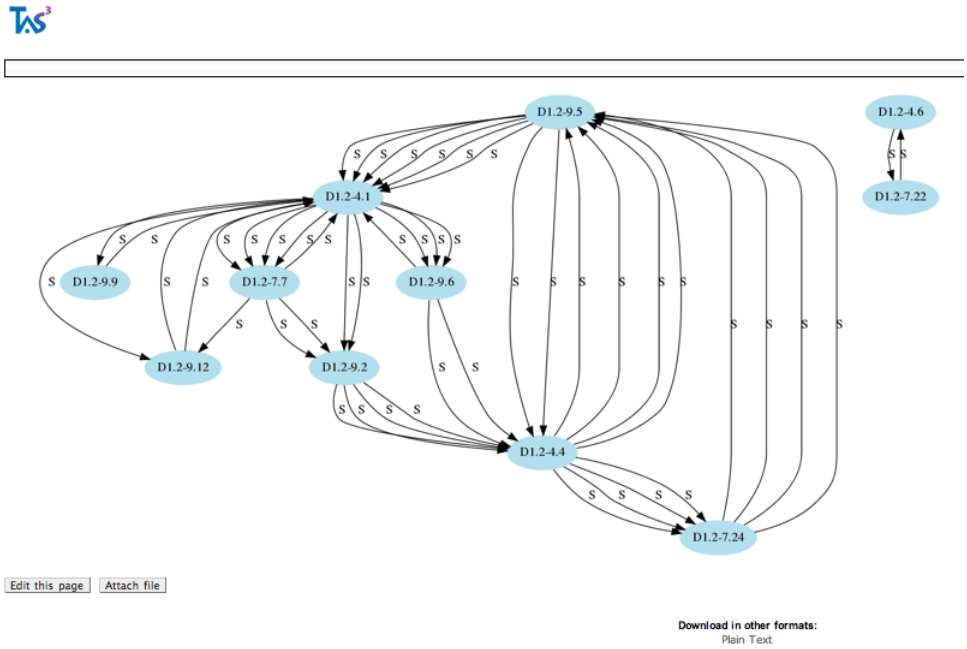

Figure 5.1: A screenshot of the interaction graph with inconsistencies as produced by the inconsistency detection tool.

Inconsistency resolution consisted of changing the semantics of the requirements to be more precise, merging or splitting requirements, and in some cases the deletion of the requirements.

After each round of negotiation and editing of the requirements and interactions, we ran the inconsistency detection tool again to see if further inconsistencies appeared. In approximately three rounds all of the inconsistencies based on the different patterns were eliminated. Once the inconsistency analysis was completed, we updated the list of requirements and presented it to the legal requirements team in WP6 to complete their interaction analysis.

6 Legal and Technical Requirements Interaction Analysis

Within the last year, the legal requirements were refined by WP6. Once the refinement of the legal requirements were completed, we prepared an interaction analysis template, as discussed in Section 2, that was filled out by WP6. Later a workshop was organized where the other WPs discussed with WP6 the interaction of the legal requirements with the technical requirements and identified gaps in both sets of requirements. The analysis of the gaps often led to immediate updates to the technical and legal requirements. in a few of the cases gaps that have to be addressed in the future were captured. We document the results of the legal and technical requirements interaction analysis in this chapter. For the list of the legal requirements used in the interaction analysis, please refer to Annex IV of Deliverable 6.2.

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.1	is fulfilled by	
	is partially fulfilled by	9.25 (documentation provisioning)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Complete outline intake process user/data subject (see also 6.4 and 6.5) b. Enrollment of users LoA needs to be specified c. Pilots need to take into account intake process as defined in D6.2 (tailoring to context might be necessary) d. Specification of technical user interface
This requirement will be fulfilled by WPs		WP6 (6.1.a), WP7, 9 (6.1.b), WP9 (6.1.c) WP2, 8, 9 (6.1.d).
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.2	is fulfilled by	
	is partially fulfilled by	10.8, 10.12, 10.13 (documentation provisioning by organization) 10.9 (verification of technical capacity to comply)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Complete outline intake process organization b. Enrollment of organizations LoA needs to be specified c. Pilots need to take into account intake process as defined in D6.2 (tailoring to context might be necessary) d. Specification of technical interface for enrolment of organizations e. Technical specifications organizations must meet in order to become TAS^3 participants
This requirement will be fulfilled by WPs		WP6 (6.2a), WP7, 9 (6.2.b), WP9 (6.2.c, d), WP2 (6.2.e)

Source Requirement	**Interaction Type**	**Target Requirements**

D1.2-6.3, D1.2-6.3.1, D1.2-6.3.2, D1.2-6.3.3	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work (but only for actual deployment)
This requirement will be fulfilled by WPs		N/A
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.4	is fulfilled by	
	is partially fulfilled by	9.25 (prior information)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Ensure agreement to use specified technologies is obtained during intake process b. See also 6.1.d and 6.2.e
This requirement will be fulfilled by WPs		WP6 (6.4.a).
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.6, D1.2-6.6.1, D1.2-6.6.2, D1.2-6.6..3, D1.2-6.6.4, D1.2-6.6.5, D1.2-6.6.6	is fulfilled by	4.1 (enforcement of sticky policies), 4.5 (policy compliance) 9.24 (immediate effect of changed policies) for 6.6.1
	is partially fulfilled by	9.25 (prior information - for 6.6)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Ensure agreement to be bound by use of specified technologies is obtained during intake process (6.6) b. Communication and commitment to usage directives (sticky policies), even when information exits (6.6.3 6.6.5) c. Non-repudiation of agreement (6.6.2) d. Easy accessibility and usability/clarity of policies (6.6.4 - 6.6.6)
This requirement will be fulfilled by WPs		WP6 (6.6.a), WP4 (6.6.b), WP6, 2 (6.6.c), WP9 (6.6.d)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.7	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Overview of policies which must be implemented b. See also 6.69 with regards to verification of implementation
This requirement will be fulfilled by WPs		WP6 (6.6.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.8	is fulfilled by	
	is partially fulfilled by	ALL
	not fulfilled	
	conflicts with	

	comments:	
This requirement will be fulfilled by WPs		ALL
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.9, D1.2-6.70, D1.2-6.72	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Identification of which actors within the TAS^3 network shall assume these tasks (taking into account separation of duties)
This requirement will be fulfilled by WPs		WP2, ALL (6.9.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.10	is fulfilled by	
	is partially fulfilled by	3.11 (ability to express privacy preferences wrt to which data to be used in particular business process) 3.13 (adaptation of business processes in light of privacy preferences), 9.24 (ability to dynamically set policies with immediate effect), 9.2 (ability for user to set privacy preferences for objects/data, and presentation in an understandable manner), 9.6 (ability for user to set privacy preferences wrt recipients), 4.1 (enforcement of privacy preferences, even when aggregated from different sources), 7.7 (ability to dynamically set privacy policies), 7.26 (consent for use of credentials and other personal data)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how legitimate bases other than consent shall be recognized and incorporated in authorization decisions.
This requirement will be fulfilled by WPs		WP7 (6.10.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.10.1	is fulfilled by	
	is partially fulfilled by	9.25 (inform user about implications expression privacy preferences)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be ensured that consent is freely given, informed and unambiguous
This requirement will be fulfilled by WPs		WP6 (6.10.1.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.10.2	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	

	comments:	Requires additional work: a. Specification of instances in which consent in writing is required b. Specification of how requirement of consent in writing shall be satisfied.
This requirement will be fulfilled by WPs		WP6 (6.10.2.a, 6.10.2.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.11	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which consent cannot be freely given. b. Specification of how to accommodate those instances in authorization decisions.
This requirement will be fulfilled by WPs		WP6 (6.11.a), WP7 (6.11.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.13	is fulfilled by	D1.2-3.11, D1.2-3.13, D1.2-4.1, D1.2-7.7, D1.2-7.26,D1.2- 9.2, D1.2-9.6 D1.2-9.24
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.14	is fulfilled by	
	is partially fulfilled by	2.20 (only authorized disclosures and actions), 7.6 (authorization required for any action), 4.1 (enforcement of user-centric policies on aggregated information sets), 7.7 (ability to dynamically set privacy policies), 9.2 (ability for user to set privacy preferences for objects/-data, and presentation in an understandable manner), 9.6 (ability for user to set privacy preferences wrt recipients), 9.24 (ability to dynamically set policies with immediate effect)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. See 6.11.b
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.15	is fulfilled by	
	is partially fulfilled by	Requires additional work: a. Specification that data controllers must specify the purposes of the processing prior to initiating the processing
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		WP6 (6.15.a)

Source Requirement	Interaction Type	Target Requirements
D1.2-6.16	is fulfilled by	
	is partially fulfilled by	D1.2-7.7
	not fulfilled	
	conflicts with	
	comments:	Requires additional work by technical partners: a. Specification of mechanism to determine compatibility of purposes b. Specification of mechanism enabling consent capture for new or changed use (user call-back), except where processing is legitimate pursuant to another basis (see 6.10)
This requirement will be fulfilled by WPs		WP3, 7 (6.16.a), WP2 (6.16.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.17	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for TAS^3 participants to have a privacy policy that articulates restrictions and obligations with regards to subsequent use of personal data it has under its control
This requirement will be fulfilled by WPs		WP6 (6.17.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.18, D1.2-6.18.1, D1.2-6.18.2.3	is fulfilled by	
	is partially fulfilled by	2.15 (accountability), 4.1 (enforcement of privacy preferences within TAS^3)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be ensured that when personal data is transmitted to a non-TAS^3 participants or is exported from the network, the recipient shall be informed of the restrictions and obligations of use (for 6.18) b. Specification of how non-TAS^3 participant shall be legally bound to respect such restrictions and obligations (for 6.18.2) c. Specification of how it shall be ensured that data subject is aware that data recipient is not a TAS^3 participant (for 6.18.3)
This requirement will be fulfilled by WPs		WP 2, 7 (6.18.a) (within the network), WP6 (6.18.b), WP6, 9 (6.18.c)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.19	is fulfilled by	
	is partially fulfilled by	4.1 (enforcement of privacy preferences)
	not fulfilled	
	conflicts with	

	comments:	Requires additional work: a. Specification of how compatibility with specified purposes shall be technically enforced. b. See also 6.16.a
This requirement will be fulfilled by WPs		WP7 (6.19.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.20	is fulfilled by	D1.2-9.5
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.21, D1.2-6.22	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be ensured that processed personal data is not excessive in relation to the specified purpose
This requirement will be fulfilled by WPs		WP6 (6.21.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.23	is fulfilled by	3.11 (privacy preferences, granular access control and business process), 2.20 (only authorized disclosures and actions), 7.6 (authorization required for any action), 9.21 (different levels of authorization), 9.23 (granular access by processes)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.24	is fulfilled by	
	is partially fulfilled by	7.5 (only provide minimum of credentials needed), 9.12 (user identification only possible after appropriate authentication and authorization), 7.8 (prevent collusion to determine identity user without consent), 7.16 (user choice of pseudonyms)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how unnecessary leaking of identifiers shall be avoided
This requirement will be fulfilled by WPs		WP2
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.24.1	is fulfilled by	
	is partially fulfilled by	7.5 (only provide minimum of credentials needed), 7.26 (consent for use of personal data and credentials)

	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how user will be able to choose among IdPs
This requirement will be fulfilled by WPs		WP7 (6.24.1.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.25, D1.2-6.25.1, D1.2-6.25.2, D1.2-6.25.3	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which data must be anonymyzed or deleted (for 6.25) b. Specification of how storage duration shall be determined (as part of the service/process definition) and enforced (for 6.25.1) c. Specification of data life cycles and their management (for 6.25.2) d. Specification of technical obligation languages which stipulate after which time-span deletion is mandatory (for 6.25.3)
This requirement will be fulfilled by WPs		WP6, 9 (6.25.a), WP4, 7 (6.25.b) (for enforcement), N/A (6.25.c), WP2 (6.25.d)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.26, D1.2-6.27, D1.2-6.28, D1.2-6.29	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be determined which entities are authorized to act as data providers for which data sets (designation of authoritative sources) (for 6.26) b. Specification of how trustworthiness of information shall be ensured, including review and update procedures (for 6.27) c. Specification of procedures on how to deal with suspected inaccuracies (for 6.28) d. Specification of procedures on how data subject will be able to verify accuracy of data prior to further processing (where appropriate) (for 6.28)
This requirement will be fulfilled by WPs		WP2 (discovery service), WP7 (for credentials) (6.26.a), WP2 (rectification process) (6.26.b), WP2 (dashboard), 9 (6.26.c), WP2 (dashboard) (6.26.d)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.30, D1.2-6.30.1	is fulfilled by	
	is partially fulfilled by	2.20 (only authorized actions), 9.19 (means to guarantee data integrity and authenticity)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification on how modification rights shall be determined (need-to-modify).
This requirement will be fulfilled by WPs		WP9 (6.30.a)

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.31	is fulfilled by	9.19 (means to guarantee data integrity and authenticity)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.32.1	is fulfilled by	(See also comments from architecture team)
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		WP6 (6.32.a), WP2, 4, 7 (6.32.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.33, D1.2-6.34	is fulfilled by	2.20 (only authorized disclosures and actions), 3.10 (permissions only valid when needed), 9.20 (confidentiality during transmission), 7.6 (authorization required for any action), 9.19 (means to guarantee data integrity and authenticity), 9.21 (different levels of authorization), 9.23 (granular access by processes)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.35	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of an organizational framework for information security management
This requirement will be fulfilled by WPs		N/A (6.35.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.36, D1.2-6.36.1, D1.2-6.36.2, D1.2-6.36.3, D1.2-6.36.4, D1.2-6.36.5	is fulfilled by	2.18 (credible authentication), 7.3 (proof of identity), 7.4 (presentation of multiple credentials), 7.5 (only provide minimum of credentials needed), 7.9 (revocability of credentials), 7.12 (pull of additional user credentials as required), 7.13 (ability to determine where additional credentials must be pulled from), 9.21 (different levels of authentication)
	is partially fulfilled by	
	not fulfilled	

	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37	is fulfilled by	2.20 (only authorized disclosures and actions), 3.11 (privacy preferences, granular access control and business process), 7.6 (authorization required for any action), 9.21 (different levels of authorization), 9.23 (granular access by processes)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.1	is fulfilled by	
	is partially fulfilled by	9.1 (secure access to data from a variety of sources)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how a directory of resources shall be populated b. Specification of how categories of potential data recipients shall be defined
This requirement will be fulfilled by WPs		WP2, 7 (6.37.1.a, 6.37.1.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.2	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how personal data shall be categorized (type, sensitivity)
This requirement will be fulfilled by WPs		N/A
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.3	is fulfilled by	
	is partially fulfilled by	9.23 (processes may only access data needed to execute successfully)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how privileges of (all) entities shall be determined
This requirement will be fulfilled by WPs		WP7 (6.37.3.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.4, D1.2-6.37.6	is fulfilled by	
	is partially fulfilled by	7.29 (mapping of external attributes to authorization attributes)

	not fulfilled	X
	conflicts with	
	comments:	a. Specification of how a list of valid recipients for each object that qualifies as personal data shall be definable upon request b. Specification of how authorization profiles shall be defined (indicating which resource is accessible to which type of entity in which capacity, time, etc)
This requirement will be fulfilled by WPs		WP 7 (6.37.4.a, 6.37.4.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.5	is fulfilled by	
	is partially fulfilled by	4.6 (override of ordinarily denied access)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how acceptable purposes for access to any given data type shall be definable upon request
This requirement will be fulfilled by WPs		WP 7 (6.37.4.a, 6.37.4.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.5	is fulfilled by	
	is partially fulfilled by	4.6 (override of ordinarily denied access)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how acceptable purposes for access to any given data type shall be definable upon request
This requirement will be fulfilled by WPs		WP4, 7 (6.37.5.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.7	is fulfilled by	
	is partially fulfilled by	10.3 (detect failures in granting or denying access to resources with respect to policies)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of instances which qualify as a security breach b. Specification of instances in which security breach notification shall be required c. Specification of which entities must be notified in case of a security breach d. Specification of follow-up of security breaches by notified entities
This requirement will be fulfilled by WPs		WP2, 10 (6.37.7.a), WP2 (abstract) (6.37.b), WP2, ALL (6.37.7.c, 6.37.7..d)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.38	is fulfilled by	9.19 (means to guarantee data integrity and authenticity), 9.20 (confidentiality during data transmission)
	is partially fulfilled by	

	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.39	is fulfilled by	
	is partially fulfilled by	7.8 (prevent collusion to determine identity user without consent), 7.16 (user choice of pseudonyms), 7.18 (avoid linkage of sequential requests)
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		WP2, 3, 4
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.40	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of in stances in which physical access control is appropriate b. Specification of how physical access control shall be realized
This requirement will be fulfilled by WPs		N/A
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.41	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for TAS^3 actors to adopt internal privacy policies documenting security measures b. Specification of technical measures which must be adopted within internal privacy policies c. See also 6.2.e
This requirement will be fulfilled by WPs		WP6 (6.41.a), WP2 (6.41.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.42	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for TAS^3 actors to institute confidentiality agreements where required by law or appropriate
This requirement will be fulfilled by WPs		WP6 (6.42.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.43	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	

	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to determine, for each data processing operation: the controller, what data shall be collected and how, for what purpose, how it will be used, who it might be shared with, and how it will be managed
This requirement will be fulfilled by WPs		WP6 (6.43.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.44	is fulfilled by	
D1.2-6.44.1, D1.2-6.44.2, D1.2-6.44.3, D1.2-6.45,	is partially fulfilled by	2.11 (functionality of TAS^3 must be transparent), 4.3 (capability to demonstrate security and trust features of TAS^3 to users), 9.25 (prior information concerning implications privacy preferences) for 6.44
D1.2-6.45.1,	not fulfilled	
D1.2-6.45.2,	conflicts with	
D1.2-6.45.3, D1.2-6.46, D1.2-6.46.1, D1.2-6.46.2, D1.2-6.46.3, D1.2-6.47, D1.2-6.47.1, D1.2-6.47.2, D1.2-6.48, D1.2-6.48.1, D1.2-6.48.2, D1.2-6.49	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to notify the data subject of: -identity of the controller; -purposes of processing; -(categories of) recipients -obligatory or voluntary nature of reply (where appropriate), and consequences of failure to reply -right of access and rectification -in the event of indirect collection: categories of data concerned b. Specification on how this information shall be communicated to the data subject
This requirement will be fulfilled by WPs		WP6 (6.45.a), WP6, WP9 (6.45.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.51	is fulfilled by	
D1.2-6.52, D1.2-6.53, D1.2-6.54, D1.2-6.55, D1.2-6.55.1, D1.2-6.55.2, D1.2-6.55.3, D1.2-6.56, D1.2-6.57, D1.2-6.59, D1.2-6.60,	is partially fulfilled by	7.7 (ability to dynamically set privacy policies), 8.6 (ability to store and modify personal data), 9.2 (ability for user to set privacy preferences for objects/data, and presentation in an understandable manner), 9.6 (ability for user to set privacy preferences wrt recipients), 9.24 (ability to dynamically set policies with immediate effect) for 6.52 (blocking and modification) 7.28 (summary audit trails), 9.8 (ability for data subject to see which entity has requested access and whether granted or denied) for 6.53 and 6.60 (past recipients)
D1.2-6.61,	not fulfilled	
D1.2-6.62	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to accommodate data subject requests to access, amend, block or erase personal data b. Specification of how such requests shall be accommodated and which criteria shall be applied (e.g., when should request for modification be granted automatically, when is additional assurance necessary, when does an overriding interest exist, etc) c. Specification of how data subject shall be informed of how to request access, amendment, blocking or erasure

This requirement will be fulfilled by WPs		WP6 (6.51.a), WP2 (dashboard), WP7 (authorization), WP9 (pilots) (6.51.1.b, 6.51.c)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.58	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to communicate modifications or blocking pursuant to data subject request to third parties to whom data have been disclosed b. Specification of how such notice shall be communicated to third party recipients
This requirement will be fulfilled by WPs		WP6 (6.58.a), WP2, 7 (6.58.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.63, D1.2-6.64, D1.2-6.64.1, D1.2-6.64.2, D1.2-6.64.3	is fulfilled by	9.5 (audit trail of who accessed personal data, when and for what purpose), 9.18 (journaling of data) for 6.63 4.4 (proof of processing in compliance with policies) for 6.64.1-2-3
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.65	is fulfilled by	
	is partially fulfilled by	2.17, 7.24 (untamperable audit trail)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how completeness of the audit trail shall be ensured
This requirement will be fulfilled by WPs		WPs 2, 7, 8, 9, 10 (6.65.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.66	is fulfilled by	
	is partially fulfilled by	2.11 (functionality of TAS^3 must be transparent)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. See 6.43.a, 6.45.a, 6.45.b
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.67, D1.2-6.68.1, D1.2-6.68.2	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	

	comments:	Requires additional work: a. Specification of how log information shall be stored, in particular which format (pseudonymized y/n) it shall be processed b. Specification of how separation of duties (and corresponding privileges) shall be organized
This requirement will be fulfilled by WPs		WP 2, 9 (6.67.a), WP2, ALL (6.67.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.68	is fulfilled by	7.24 (confidentiality of audit trail)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.69	is fulfilled by	D1.2-10.1, D1.2-10.2, D1.2-10.9, D1.2-10.10
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.71	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for TAS^3 participants to co-operate with entities in the TAS^3 network charged with oversight and audit
This requirement will be fulfilled by WPs		WP6 (6.71.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.73, D1.2-6.73.1, D1.2-6.73.2	is fulfilled by	
	is partially fulfilled by	D1.2-2.15, D1.2- 4.4
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how non-repudiation shall be ensured b. See also 6.6.c
This requirement will be fulfilled by WPs		WPs 2, 7 (6.73.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.74	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	

	comments:	Requires additional work: a. Specification of instances in which automated notification shall be instituted b. Specification of how such notifications should be followed up c. See also 6.37.7.a-d
This requirement will be fulfilled by WPs		WP2, 7, ALL
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.75	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of procedures which enable identification of the source of personal data upon request, as well as the purpose for processing
This requirement will be fulfilled by WPs		WP2 (6.75.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.76	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation to ensure that data recipients outside the TAS^3 are bound to adhere to the usage directives and policies articulated by the TAS^3 network
This requirement will be fulfilled by WPs		WP6 (6.76.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.77, D1.2-6.77.1, D1.2-6.77.2, D1.2-6.78	is fulfilled by	
	is partially fulfilled by	2.15 (accountability), 5.4 (trust feedback mechanism)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Definition of complaint capture system and follow-up procedures (in addition to reduction of trust score), including processes for providing redress
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.79	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Ensure that TAS^3 participants provide evidence of notification of their DPA during intake process
This requirement will be fulfilled by WPs		WP6 (6.79.a)

6.1 Interaction Analysis of New Legal Requirements

After the analysis of the interaction between the legal and technical requirements, WP6 and the other WPs noticed the need for further legal requirements. The complete list of new, edited and deleted requirements are captured in Appendix B. The final list of legal requirements are listed in Deliverable 6.1. The interactions of the new requirements are documented in the following template.

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.80	is fulfilled by	
	is partially fulfilled by	D1.2-7.27
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Further specification of actors, roles and responsibilities b. See also Req 6.9
This requirement will be fulfilled by WPs		WP2, ALL (6.80.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.81	is fulfilled by	9.9 (ability for users to modify privacy preferences), 9.24 (act on dynamically set privacy policies with immediate effect)
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.82	is fulfilled by	
	is partially fulfilled by	D1.2-3.4 (consistent identification throughout the execution of a business process instance)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how unambiguous identification shall be ensured across service providers (beyond business process instances)
This requirement will be fulfilled by WPs		WP2 (6.82.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.83	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which delegation might be restricted b. Specification of how it shall be ensured that delegation will only executed where permitted by the appropriate policy
This requirement will be fulfilled by WPs		WP6, 7 (6.83.a, 6.83.b)
Source Requirement	**Interaction Type**	**Target Requirements**

D1.2-6.84	is fulfilled by	D1.2-7.3
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.85	is fulfilled by	D1.2-4.6
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
This requirement will be fulfilled by WPs		
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.85.1	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of which entities should be notified in case the glass is broken b. Specification of how notification of these entities shall be ensured c. Specification of follow-up procedures
This requirement will be fulfilled by WPs		WP2, 7, ALL (6.85.1.a) WP7 (6.85.1.b), WP2, 7 ALL (6.85.1.c)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.86	is fulfilled by	
	is partially fulfilled by	D1.2-9.16
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which (temporary or permanent) duplication shall be deemed necessary
This requirement will be fulfilled by WPs		WP2, 9 (6.86.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.7, D1.2-6.87.1	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how user will be able to set privacy preferences with regards to use of feedback information b. Specification of how operator of Trust Reputation Server shall be bound to only process feedback information in accordance with the policy expressed by the user c. See also 5.11

This requirement will be fulfilled by WPs		WP2 (6.87.a.), WP6 (6.87.b)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.88, D1.2-6.88.1, D1.2-6.88.2	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which outsourcing or delegation is restricted b. Specification of how it shall be ensured that TAS^3 participants are contractually bound to only select processors which offer sufficient guarantees in terms of organizational and technical measures c. Specification of how it shall be ensured that TAS^3 participants are contractually bound to conclude a contract with their processors containing the elements required by art. 17 of Directive 95/46/EC
This requirement will be fulfilled by WPs		WP6 (6.88.a, 6.88.b, 6.88.c)

6.2 Mapping of Legal Requirements to Architecture

In the mapping of the legal requirements to architecture we first asked the WP6 to identify requirements that specifically interact with WP2. These interactions were than commented by the WP2 architecture team. The architecture team indicated whether the legal requirement could be addressed in the architecture and if so, whether it already had been addressed or there was a gap.

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.9, D1.2-6.70, D1.2-6.72	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Identification of which actors within the TAS^3 network shall assume these tasks (taking into account separation of duties)
Comments of WP2		This requirement may only be fulfilled in a concrete implementation of TAS^3 in a given context. This can be done for the demonstrators but will have to remain open for future contexts or will be specific to an implementation of TAS^3.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.16	is fulfilled by	
	is partially fulfilled by	D1.2-7.7
	not fulfilled	
	conflicts with	

	comments:	Requires additional work by technical partners: a. Specification of mechanism to determine compatibility of purposes b. Specification of mechanism enabling consent capture for new or changed use (user call-back), except where processing is legitimate pursuant to another basis (see 6.10)
Comments of WP2		This matter is addressed in D1.2-2.4 Section 2.7.4 User Interaction
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.18, D1.2-6.18.1, D1.2-6.18.2.3	is fulfilled by	
	is partially fulfilled by	2.15 (accountability), 4.1 (enforcement of privacy preferences within TAS^3)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be ensured that when personal data is transmitted to a non- TAS^3 participants or is exported from the network, the recipient shall be informed of the restrictions and obligations of use (for 6.18) b. Specification of how non- TAS^3 participant shall be legally bound to respect such restrictions and obligations (for 6.18.2) c. Specification of how it shall be ensured that data subject is aware that data recipient is not a TAS^3 participant (for 6.18.3)
Comments of WP2		This is currently not addressed in the architecture of TAS^3
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.24	is fulfilled by	
	is partially fulfilled by	7.5 (only provide minimum of credentials needed), 9.12 (user identification only possible after appropriate authentication and authorization), 7.8 (prevent collusion to determine identity user without consent), 7.16 (user choice of pseudonyms)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how unnecessary leaking of identifiers shall be avoided
Comments of WP2		this requirements is addressed in D2.1 Section 3.2.1 Attribute Pool Model
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.25, D1.2-6.25.1, D1.2-6.25.2, D1.2-6.25.3	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	

	comments:	Requires additional work: a. Specification of instances in which data must be anonymyzed or deleted (for 6.25) b. Specification of how storage duration shall be determined (as part of the service/process definition) and enforced (for 6.25.1) c. Specification of data life cycles and their management (for 6.25.2) d. Specification of technical obligation languages which stipulate after which time-span deletion is mandatory (for 6.25.3)
Comments of WP2		addressed in D2.4 Section 2.10 Simple Obligations Language (further languages can be extended to specify this, but currently it is only SOL that we have made sure addresses this specification).
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.26, D1.2-6.27, D1.2-6.28, D1.2-6.29	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how it shall be determined which entities are authorized to act as data providers for which data sets (designation of authoritative sources) (for 6.26) b. Specification of how trustworthiness of information shall be ensured, including review and update procedures (for 6.27) c. Specification of procedures on how to deal with suspected inaccuracies (for 6.28) d. Specification of procedures on how data subject will be able to verify accuracy of data prior to further processing (where appropriate) (for 6.28)
Comments of WP2		This requirement still needs to be refined to be addressed by the architecture. It is possible that this requirement may only be fulfilled in a concrete implementation of TAS^3 in a given context.The dashboard will also partially address this requirement.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.32.1	is fulfilled by	D1.2-9.19, D1.2-9.20
	is partially fulfilled by	
	not fulfilled	
	conflicts with	
	comments:	
Comments of WP2		this requirements is addressed in D2.4 Section 2.2.2 Liberty and ID-WSF Profile, D2.1 Section 3.8 Properties of Web Service Binding. It is also addressed in the above mentioned requirements from WP9.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.1	is fulfilled by	
	is partially fulfilled by	9.1 (secure access to data from a variety of sources)
	not fulfilled	
	conflicts with	

	comments:	Requires additional work: a. Specification of how a directory of resources shall be populated b. Specification of how categories of potential data recipients shall be defined
Comments of WP2		This requirement may only be fulfilled in a concrete implementation of TAS^3 in a given context.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.37.7	is fulfilled by	
	is partially fulfilled by	10.3 (detect failures in granting or denying access to resources with respect to policies)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of instances which qualify as a security breach b. Specification of instances in which security breach notification shall be required c. Specification of which entities must be notified in case of a security breach d. Specification of follow-up of security breaches by notified entities
Comments of WP2		This requirement is addressed in the annexes on Threat analysis and Risk assessment in D2.1.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.39	is fulfilled by	
	is partially fulfilled by	7.8 (prevent collusion to determine identity user without consent), 7.16 (user choice of pseudonyms), 7.18 (avoid linkage of sequential requests)
	not fulfilled	
	conflicts with	
	comments:	
Comments of WP2		This requirement is addressed in D4.1 Section 1.1 Format and Properties of Identifiers which is also implemented by the architecture team.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.41	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for TAS^3 actors to adopt internal privacy policies documenting security measures b. Specification of technical measures which must be adopted within internal privacy policies c. See also 6.2.e
Comments of WP2		This requirement is addressed in D2.1 Annex Compliance Requirements and in the Annex CR251-OpsManual of the same deliverable.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.51 D1.2-6.52, D1.2-6.53, D1.2-6.54, D1.2-6.55, D1.2-6.55.1, D1.2-6.55.2, D1.2-6.55.3, D1.2-6.56, D1.2-6.57, D1.2-6.59, D1.2-6.60, D1.2-6.61, D1.2-6.62	is fulfilled by	

	is partially fulfilled by	7.7 (ability to dynamically set privacy policies), 8.6 (ability to store and modify personal data), 9.2 (ability for user to set privacy preferences for objects/data, and presentation in an understandable manner), 9.6 (ability for user to set privacy preferences wrt recipients), 9.24 (ability to dynamically set policies with immediate effect) for 6.52 (blocking and modification) 7.28 (summary audit trails), 9.8 (ability for data subject to see which entity has requested access and whether granted or denied) for 6.53 and 6.60 (past recipients)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to accommodate data subject requests to access, amend, block or erase personal data b. Specification of how such requests shall be accommodated and which criteria shall be applied (e.g., when should request for modification be granted automatically, when is additional assurance necessary, when does an overriding interest exist, etc) c. Specification of how data subject shall be informed of how to request access, amendment, blocking or erasure
Comments of WP2		This requirement is addressed in D2.4 Section 2.7 Realization of the Audit and Dashboard Function.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.58	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of obligation for relevant TAS^3 actors to communicate modifications or blocking pursuant to data subject request to third parties to whom data have been disclosed b. Specification of how such notice shall be communicated to third party recipients
Comments of WP2		This is discussed but not properly addressed in D2.1 Section 6.2 Right of Access Rectification and Deletion.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.65	is fulfilled by	
	is partially fulfilled by	2.17, 7.24 (untamperable audit trail)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how completeness of the audit trail shall be ensured

Comments of WP2		This problem has two parts 1)you do not delete what is there (this is addressed in D2.1 Section 6.1 Dashboard and D2.4 Section 2.7 Realization of the Audit and Dashboard Function, 2) more difficult to guarantee that things are logged in the first place, and this requires human audit. Human audit comes in two categories i) the end-user self-audit which is facilitated through the Dashboard, and ii) Audit Analysis which is done by external auditing organizations, this is mentioned in D2.1 Section 2.1. There is also a D2.1 Section 6.5 Formal Compliance Audits
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.67, D1.2-6.68.1, D1.2-6.68.2	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how log information shall be stored, in particular which format (pseudonymized y/n) it shall be processed b. Specification of how separation of duties (and corresponding privileges) shall be organized
Comments of WP2		6.67.a requirement is addressed in D2.1 Annex Enumeration of Audit Events (although this does not go into detail). WP2 finds it more appropriate that 6.67.b is addressed by WP7.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.73, D1.2-6.73.1, D1.2-6.73.2	is fulfilled by	
	is partially fulfilled by	D1.2-2.15, D1.2- 4.4
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how non-repudiation shall be ensured b. See also 6.6.c
Comments of WP2		This is a gap which will be addressed by WP2.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.74	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which automated notification shall be instituted b. Specification of how such notifications should be followed up c. See also 6.37.7.a-d
Comments of WP2		WP2 addresses this requirement in D2.1 Section 6.2 Right of Access Rectification and Deletion
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.75	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X

	conflicts with	
	comments:	Requires additional work: a. Specification of procedures which enable identification of the source of personal data upon request, as well as the purpose for processing
Comments of WP2		WP2 D2.4 Section 2.10.2 Matching Pledges to Sticky Policies and Obligations addresses that what the policies are conveyed. D2.1 Section 2.4.3 Using Sticky Policies to Protect Data, potentially this is also addressed in D2.1 Section 4.1 Protocol Support for Conveyance of Sticky Policies , also in D2.4 Section 2.11 Realization of Sticky Policies. These address the policies, but the data aspect is addressed in D2.1 Section 6.2.1 Identification of Originating Authority (6.75.a)
Source Requirement	**Interaction Type**	**Target Requirements**
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.80	is fulfilled by	
	is partially fulfilled by	D1.2-7.27
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Further specification of actors, roles and responsibilities b. See also Req 6.9
Comments of WP2		WP2 addresses this requirment in D2.4 Section 1.2 Composition and Co-location of Architectural Components, this section discusses the types of conflicts of interest e.g., why you should not be an SP and IdP at the same time.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.82	is fulfilled by	
	is partially fulfilled by	D1.2-3.4 (consistent identification throughout the execution of a business process instance)
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of how unambiguous identification shall be ensured across service providers (beyond business process instances)
Comments of WP2		WP2 addresses this requirement in D4.1 in Section 1.1. (6.82.a)
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.85.1	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of which entities should be notified in case the glass is broken b. Specification of how notification of these entities shall be ensured c. Specification of follow-up procedures

Comments of WP2		WP2 states that this is a business/legal definition and not a technical one.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.86	is fulfilled by	
	is partially fulfilled by	D1.2-9.16
	not fulfilled	
	conflicts with	
	comments:	Requires additional work: a. Specification of instances in which (temporary or permanent) duplication shall be deemed necessary
Comments of WP2		WP2 addresses this requirement in D2.1 Section 3.2.1 Attribute Pull Model which also includes a plan to avoid duplication.
Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-6.7, D1.2-6.87.1	is fulfilled by	
	is partially fulfilled by	
	not fulfilled	X
	conflicts with	
	comments:	Requires additional work: a. Specification of how user will be able to set privacy preferences with regards to use of feedback information b. Specification of how operator of Trust Reputation Server shall be bound to only process feedback information in accordance with the policy expressed by the user c. See also 5.11
Comments of WP2		WP2 thinks that WP5 should state their fulfillment of this requirement.

7 Mapping Global Requirements to the TAS^3 Architecture

Requirements elaboration in D1.2 is based on viewpoints elicitation and analysis. There is always a danger that when the focus is on the viewpoints that global requirements are not properly addressed. In order to address this problem, we have asked the architecture team to identify global requirements during the requirements elaboration activities. Later, the requirements team was asked to map these requirements to the different architecture components developed by the TAS^3 WPs. The results of this mapping as well as the accompanying gap analysis is listed below using a mapping template:

ReqID	**D1.2-2.1**
Requirement	TAS^3 Architecture MUST be feasible to implement
Evaluation	The reference implementation in form of ZXID is a feasibility proof given that it was implementable within the architecture is a feasibility proof. Further, several of the components have been implemented in a reasonable amount of time and guarantee good performance.
To do	
ReqID	**D1.2-2.2**
Requirement	TAS^3 Architecture MUST be feasible to deploy
Evaluation	The IDP implemented (that will be implemented) at demo.tas3.eu shows that it is feasible to deploy TAS^3. By month 27 we will be able to say that it is fully deployable. The demos prepared by Custodix, Risaris and Nottingham will also be used to validate the deployability. This is work in progress although early experiences show that it is feasible to deploy TAS^3.
To do	The demonstrators are still to be completed and evaluated with respect to the validation of the fulfillment of this requirement.
ReqID	**D1.2-2.3**
Requirement	TAS^3 Architecture MUST support plurality of service business models
Evaluation	TAS^3 contains a discovery service. This is implemented in the component T3-IDP-Map There is a ZXID implementation of the discovery service. Plurality of service business models cannot only be guaranteed technically. It also depends on the business model of TAS^3 which is still to be completed. In the combination of the technology and the business model will this requirement be fulfilled.
To do	The business model has to be completed. This needs to be in a manner with enables plurality of business models.
ReqID	**D1.2-2.4**
Requirement	TAS^3 Architecture MUST support multiple software suppliers

Evaluation	TAS^3 is currently compliant with existing standards. Therefore it is conducive to enabling a multi-vendor market. This is also validated in the different components which are developed using different identity management standards in the components T3-IDP-ZXID and T3-IDP-SHIB. In that sense, we have a multi-vendor experience. In the case of the PDP authorization component we also have multi-vendor experience. The PERMIS PDP, SUN PDP and Trust PDP simulate a multi-vendor situation. There is also a dummy PDP which was Sampo's own authorization client. There are though problems with the multi-vendor requirements: TAS^3 in its current form TAS^3 is very much ZXID dependent. There is a possibility that Custodix software is not. This needs to be checked. Currently we also do not have a second implementation of the stack. In deliverable 2.4 there is a TAS^3 (official) API section. Once completed, we will have an out-of-the-box specification of the TAS^3 API for several programming languages.
To do	Find out if Custodix is also ZXID dependent or if they are using different standards. Confirm that the API is the multiple programming language solution that it claims to be.
ReqID	**D1.2-2.5**
Requirement	TAS^3 Architecture MUST be platform independent
Evaluation	ZXID has been imported to both linux and windows. So currently it is a multi-platform architecture.
To do	
ReqID	**D1.2-2.6**
Requirement	TAS^3 Architecture MUST be programming language agnostic
Evaluation	2.6 We have implementations in PHP and java. These can be found in the following components: T3-SSO-ZXID-JAVA T3-SSO-ZXID-MODAUTHSAML T3-SSO-ZXID-PHP The reference implementation supports JAVA, PHP, C and C++. The last two were not part of the TAS^3 requirements but were desirable by Sampo. Hence, the architecture is programmable using multiple programming languages. It is not a JAVA only architecture. In Deliverable 2.4 there is a TAS^3 (official) API section, out-of-the-box TAS^3 will specify for several programming languages the API.
To do	Check end-results of Deliverable 2.4 definition of API.
ReqID	**D1.2-2.7**
Requirement	TAS^3 Architecture MUST be fail safe, i.e. failure should not lead to security breach
Evaluation	This requirement is currently not demonstrated/fulfilled.
To do	Fail-safe design implementation and related security checks have to be systematically done in many parts of the architecture. Can WP10.CNR do compliance checking for a fail-safe architecture. Or, is WP10.CNR just a test frame? Then, how is this systematic check going to be completed?
ReqID	**D1.2-2.8**
Requirement	TAS^3 Architecture MUST be available
Evaluation	A lot of the services in the architecture can be backed up. An alternative IDP can easily be found. The storage persistent parts on the other hand are not easy to replace if they fail on availability. In Deliverable 2.4 Section 5 starts addressing availability issues. It is called resilient deployment architecture. Currently this section does not contain much detail. Even the TAS^3 wiki has a number of single points of failure. Possibly it is not in the scope of this project to demonstrate the fulfillment of this requirement.
To do	Decide if this requirement is within the scope of TAS^3 project.

ReqID	D1.2-2.9
Requirement	Implementation MUST correctly implement TAS^3 Architecture
Evaluation	The integration testing demonstrates interoperability between vendors. But, this is a weak demonstration of correctness, but it is better than nothing. But, how do you demonstrate correctness. A tough thing to do is to provide software proofs. You can also do some correctness checks at the interface level, or using unit testing and some compliance testing. The complexity of a constellation like TAS^3 may be such that you cannot test it exhaustively. Even testing a component like the PDP is complex.
To do	This is a currently unaddressed requirement which demands additional communication and planning. If WP10.CNR is not doing this sort of testing needs to be clarified?
ReqID	**D1.2-2.10**
Requirement	TAS^3 MUST appear to the users to work correctly
Evaluation	This is a quality requirement. Ideally, this is part of what UNIZAR should be testing. But, it is likely that UNIZAR will only look at the interface and say if it is friendly or not. This requirement is not addressable in the architecture. Some end-to-end testing is also conceivable: The end-users of the demonstrators can be part of such testing and may also state the functionalities that they do not understand. This will require cooperation between WP9 and WP12. With respect to the specification, if we specify some (work) flows, the flows have to be within reasonable expectation of what the users think will happen. But, where do we specify flows? Who will do the specification of what the user experience looks like. Maybe this should be part of the pilots. These matters to not get addressed or specified in the architecture although they probably should. This is a gap in the project. We state that user interaction and experience is important but nobody is addressing this. The dashboard interface prototype Lex showed in Budapest could be one of the matters addressed to fulfill this requirement. Is the dashboard a part of any specific WP?Is it going to be part of WP9?
To do	This requirement is currently not addressed. Possible candidates are UNIZAR, WP9 or others?? addressing the user experience and correctness of functionality. The work on the Dashboard interface can be seen as fulfilling this requirement partially. Responsibilities for this requirement have to be distributed.
ReqID	**D1.2-2.11**
Requirement	The functionality of TAS^3 must be transparent to the users (user can see what is going on)

Evaluation	A large part of this requirement is fulfilled with the development of the dashboard. This requirement is an overall guiding principle for the user interface. We need to define how the dashboard is going to make the system transparent to the user. Koblenz is developing part of the dashboard including an audit trail search tool. The module is called: T3-LOG-GUI And, part of the functionalities in the component: T3-DASH fulfill this requirement. The business process modeling could also be used to provide more transparency. If the users are aware of the business processes, then they can then understand how it is supposed to work, and understand if there are anomalies in the system. If it is explained and understood, this is the process, then the user can inform herself and make a well informed decision. which means the business processes have to be modelled properly in an understandable manner. Sampo thinks T3-BP-GUI is responsible for this. Let's take for example the TAS^3 service selection. The user has a processing need, and once the candidates for the service have been filtered for suitability by using the trust engines and other criteria, and more than one candidate remains, the user needs to make a choice (informed). Essentially, TAS^3 should guarantee that the ones ranking low on the trust model are eliminated. But there is a point where the machine should not make a decision. In some cases, it may be appropriate to have a policy driven selection, but human interaction selection may often be desirable. This is the service selection dilemma. How does that selection happens, and how it is user centric and controlled by the user is part of comprehensibility and transparency, too. From the legal side it is probably also very important that the user can make an informed decision and can judge appropriately what the system is doing.
To do	Is the component/WP T3-BP-GUI addressing the problem of making the system/business process transparent to the user? Is it necessary, legally, to make anything transparent to the user? What is the sufficient standard of transparency and comprehensibility from a legal perspective? Are there different requirements for different application domains?
ReqID	**D1.2-2.12**
Requirement	TAS^3 MUST be comprehensible to the user. The user MUST be able to understand what has happened, what should have happened, and what will happen.
Evaluation	see D1.2-2.11
To do	
ReqID	**D1.2-2.13**
Requirement	TAS^3 MUST be easy to use

Evaluation	This requirement should be split into three with respect to the different "user" groups: for users, deployers/clients, and for developers. TAS^3 ease-of-use for users: The ease-of-use for the users is a matter of the GUI packages which are dealt with in the following components: T3-BP-GUI T3-LOG-GUI T3-POL-GUI TAS^3 ease-of-use for deploying clients: This is the case as a result of a lot of the automatic configuration features, e.g., the SAML 2.0 well known location method of meta-data exchange. For two entities in the TAS^{3}3 infrastructure to communicate, they need to know where the certificates, end-points and other configuration parameters are located. In D2.4 this kind of exchange is prescribed. We assume that if there are readily available products, then it will be easy to deploy TAS^3. Last, the architecture documentation is comprehensible and makes it easy to understand and deploy TAS^3 (this is to be validated). TAS^3 ease-of-use for programmers: TAS^3 provides a reference implementation. T3-IDP-ZXID T3-SSO-ZXID The programmers are also provided with a standardized API.
To do	We need validation of the ease-of-use concepts listed above: including ease of use of documentation, the ease-of-use of GUIs, and the IDP and SSO implementations.
ReqID	**D1.2-2.14**
Requirement	TAS^3 MUST appear to the user to be privacy protective
Evaluation	The privacy protection has to provide the user with control while not being intrusive e.g., the user has to be asked for consent when this is necessary, but there should be also some automation available if the user prefers to automate some of the decisions or consent is not necessary. Matters of a similar kind are addressed in different parts of the architecture: Mechanisms for minimal disclosure: There are ways to negotiate what you reveal in our system. This is especially addressed when doing trust and privacy negotiation. Mechanisms for control and data protection: The authorization component like the sticky policies play an important role in providing users with control. The relevant components are: T3-POL-GUI T3-POL-NLP T3-POL-WIZ T3-PEP-AI: provides the enforcement of sticky policies and obligations. Mechanisms for developing privacy practice: The trust components help the users in developing practices with respect to their privacy with trusted parties. T3-TRU-FB T3-TRU-RTM It is currently unclear, if we need a separate service for conveying the trust, or if it can be conveyed through the audit bus. Users, through their ranking and feedback trigger trust and reputation related events. If these events go through the bus, some of these interesting events, like audit trail items, could be considered as events part of the trust formation. Communicating trust feedback over the bus means the user has to send the feedback once. If not, then the user has to send the feedback a second time to a separate service. This means that the user has to bother to send a message to the service provider. In comparison, an audit trail is necessary and mandatory. Legally an audit trail is expected. At the same time, most of the trust feedback is in the audit trail. So, there is an existing economy from which to develop the trust management service. in any case, both audit bus and the dashboard are important components of privacy as practice. T3-DASH T3-BUS-AUD

To do	What else can we say about the trust and privacy negotiation component? Clarify if a separate trust service provider is necessary, and if/how it can be integrated with the audit information that flows over the bus.
ReqID	**D1.2-2.15**
Requirement	TAS^3 MUST make it possible to hold people and companies accountable for the activities with respect to personal data
Evaluation	The audit trail is the main tool with which we achieve oversight and accountability. There is a requirement for everybody to keep audit trail. The TAS^3 audit trail is spread throughout the architecture. It touches every component of the architecture that needs to be audited. The audit trail also has a number of facilitating components: T3-LOG-SAWS T3-LOG-WRAP-SAWS T3-LOG-WRAP-ZXID T3-LOG-ZXID T3-DASH Another aspect of accountability is temper proof and non-repudiation. These properties can be addressed in the stack. The stack is addressed in the component: T3-STACK But, a lot of the functionality of the TAS^3-stack is integrated into a number of ZXID modules. Therefore, temper resistance and non-repudiation also needs to be addressed in this component: T3-SSO-ZXID In general, both properties are addressed in the design and implementation.
To do	It needs to be validated in the future if temper-resistance and non-repudiation have been addressed in T3-Stack and T3-SSO-ZXID.
ReqID	**D1.2-2.16**
Requirement	TAS^3 MUST mitigate risks or prevent risks to the trust and security of the architecture.
Evaluation	The current threat model/risk model part of the architecture has not been completed (Task 2.8) There are some components that mitigate some of the risks that would be discovered in the threat and risk analysis model. The operation monitoring component has intrusion detection, protection against viruses, and buffer overflows. General network security would apply, but is not part of the research project. Nevertheless, you cannot address this requirement without having done such an analysis.
To Do	The threat and risk analysis is to be completed in Task 2.8. Responsible are Sampo and SAP. Completion in month 27.
ReqID	**D1.2-2.17**
Requirement	TAS^3 MUST provide an untamperable audit trail
Evaluation	2.17 The temper-resistant audit trail is taken care of in: T3-LOG-SAWS within the secure auditing web services T3-LOG-ZXID which in principle aim to address the same matter in a parallel implementation. The issue is also addressed in: T3-DASH The bulk of untemperability is done by SAWS. SAWS has a vulnerability that an attacker cannot modify but might be able to find a way to omit or delete audit trails. At certain check points audits will become undeletable, but in between attacks are possible. Sampo is not convinced about the absolute undeletability of the audits with SAWS. Hence, Sampo proposes a back to the dash to protect against the types of deletion attacks that SAWS and ZXID cannot fully mitigate.
To Do	T3-DASH has to implemented in such a way to mitigate the tempering/deletion risks not addressed by SAWS.
ReqID	**D1.2-2.18**
Requirement	Authentication in TAS^3 MUST be credible

Evaluation	Authentication of the end-users: The following components address the credibility of authentication for the end-users: T3-IDP-ZXID: supports both client ceritificates (e-id) and the hardware tokens such as yubikey. T3-IDP-SHIB: they also support something better than password Authenticating the end-user is convincingly implemented by the hardware tokens. One could easily also implement RSA and other authentication tokens. Authentication of system entities: By system entities we mean entities, such as the idp and service providers, etc. Their authentication is done by the use of client certificates issued to a server at TLS and using digital signatures. Both of these mechanisms are checked and validated using the following components: T3-STACK: creates and checks TLS and digital signatures. T3-ACBS: provides an authorization credential validation service.
To Do	Check what kind of authentication Shibboleth provides to complete the evaluation of the authentication requirement for users.
ReqID	**D1.2-2.19**
Requirement	Authorization in TAS^3 MUST be credible
Evaluation	2.19 This may currently be a weak spot in the architecture. It may prove difficult to develop rule sets that are correct. Nevertheless, the problem is addressed in all components starting with: T3-PDP-* packages. And, in the: T3-PEP-* In general, the following two rules have to be satisfied: 1) the right authorization decisions are being made 2) and the decisions are enforced We are developing mechanisms to put both in place
To Do	When and how do we evaluate the liminations of the PEP and PDP components?
ReqID	**D1.2-2.20**
Requirement	TAS^3 MUST guarantee only authorized disclosures and actions
Evaluation	This is the enforcement part of requirement 2.19. It is addressed in: T3-PEP-* This requirement is also related to the obligations management. University of Kent has an obligations manager, but we currently do not have a module in our component list addressing this problem. The likely candidate where this is happening is: T3-PEP-AI
To Do	Check and confirm that either T3-PEP-AI is addressing this requirement or delegate to another component the fulfillment of this authorization requirement.
ReqID	**D1.2-2.21**
Requirement	TAS^3 MUST implement data protection legislation in technology.
Evaluation	
To Do	2.21 The evaluation of this requirement will be completed with Brendan and Joe.
ReqID	**D1.2-2.22**
Requirement	TAS^3 MUST permit access to the audits for legitimate authorities if this is legally necessary.
Evaluation	The access to the audit is generally made possible with: T3-LOG-SP This component exposes the audit trail to authorized parties, depending on what legitimate authorization is defined as. But, guaranteeing that only those with legitimate authority use this functionality is not only a matter of technology, but also needs to be defined though organizational policies. It would be nice to have a library of default policies that address such law enforcement measures.

To Do	A discussion is necessary as to if a new component named: T3-DEFAULT POLICY should be added in which a library of reusable policies that address data protection issues and legitimate access policies are collected. Brendan and Joe should be consulted with respect to the feasibility and desirability of such a component.
ReqID	**D1.2-2.23**
Requirement	Semantic interoperability should be achieved across web services and business processes.
Evaluation	We achieve semantic interoperability by trying to avoid divergent semantic vocabularies. D2.4 specifies the appropriate trust levels that can be used. Ontology activities to improve the semantics and hence the use of a common vocabulary between the partners will be addressed in the following components: T3-ONT-LCO T3-ONT-SO T3-ONT-UCO This ontology task is at a very high level. There is no single other component that is integrating machine readable ontology into their system. There is no commitment from quentin that the LCO and UCO are machine readable. They are also not actionable. Current implementers see great utility in mapping or translating credentials and attributes and this is realized by Credential Validation Service (T3-ACVS). However, this module is currently using simple mapping table approach and does not really integrate to the ontology components (T3-ONT-*).
To Do	The integration of the ontology components with the semantic needs of the rest of the components should be addressed.

8 Mapping WP Requirements to the TAS^3 Architecture

The following is a mapping of the requirements to the TAS^3 architecture. The mapping is not yet complete. Some of the requirements for WP5, WP7, WP8, WP9 are missing, unless they were redundant requirements. The mapping of the requirements of WP10 are missing completely. Further, our legal experts have started commenting on all the requirements individually and the mapping of the requirements to the architecture. Both of these activities are underway and will be completed in the next iteration of D1.2. Here we present the latest version of the requirements mapping to the architecture.

The mapping of the requirements to the architecture also documents redundant requirements, requirements that are out of the scope of the architecture, and any conflicts between requirements from the perspective of the architecture team.

Req.	**Primary Responsibility**	**Architecture Component**	**Explanation of how component fulfills requirement**
D1.2-2.1-FeasImp	WP2, WP12	General	Only a correct architecture is feasible. Correctness is to be ensured by editorial excellence and review. Sufficient architecture documentation is a second enabler of feasibility. WP2 will work in close interaction with WP8 and WP9 to ensure knowledge transfer. Availability of ready made solutions, especially open source solutions, for the components of the architecture that are not in research scope, is fundamental for implementation feasiblity. Architecture has been designed to be standards aware and operational with existing software libraries.
D1.2-2.2-FeasDep	WP2, WP12, WP8	General	All “hows” of D1.2-2.1-FeasImp apply. Further, the architecture and software documentation must address how to configure the modules correctly. Deployment feasibility also means that algorithms that are used, either through architecture choice or implementation choice, must be efficient enough to run in a production environment. Of particular concern are the number of public key operations required (e.g. digital signature generation and verification as well as TLS connection establishment) and the number of authorization decisions that need to be made. The general approach has been to emphasize correct, no short cuts, implementation of functionality with minimum number of expensive operations. However, in no case has functionality been traded for efficiency. Such trade-off may eventually be made in a future release of the architecture, based on pilot experience (WP9). Of particular importance from the feasibility perspective is that the architecture does not require PKI to be deployed to the end users (however PKI for end users can be deployed in context of the TAS^3 architecture).

D1.2-2.3-BMs	WP2, WP7	D4.1, Discovery, ID Mapper, Registry Server	Service business models can range from hardwired monopoly environment to fully dynamic competitive environment. Generally the latter is more demanding. So, the architecture specifies the discovery family of functionality to support this. The monopoly case is handled as a special case where only one provider can be discovered.
D1.2-2.4-MultiVendor	WP2, TAS^3 CA	Annex A: Protocols	Standards based architecture is inherently easier for multiple vendors to implement. Another multivendor feature is the Royalty Free licensing of included Project Background and the Project Foreground, as foreseen in the TAS^3 Consortium Agreement. The CA also foresees use of BSD style Open Source licenses in the project deliverables, further permitting commercial reuse of project deliverables.
D1.2-2.5-Platform	WP2	Annex A: Protocols	Multiplatform support is mainly a matter of not using solutions that are available on just one platform. TAS^3 architecture specifies standards a based approach so multiplatform support requirement is well addressed.
D1.2-2.6-Lang	WP2	Annex A: Protocols	Most important way to support multiple programming languages is to specify all APIs and interactions on wire protocol terms rather than in programming language specific API terms. All standards referenced by the Architecture Protocols annex shall be wired protocol standards rather than programming APIs. Another way to support multiple programming languages is using libraries that provide multiple interfaces, e.g. by using SWIG [SWIG] to translate C interfaces to a number of scripting languages.
D1.2-2.7-Safe	WP2	Annex F Threats, New section TBW	The Threats section specifies some Denial of Service attacks and strategies for surviving them. Architecture does not currently (May 2009) address Fail Safety adequately. This will be addressed by a special analysis section that will be included in the next architecture deliverable. See also Req. D1.2-7.21-Safe.
D1.2-2.8-Avail	WP2	Annex B: Resilient Deployment Architecture, Annex F Threats	Architecture discusses several availability techniques (cf. Annex B). These techniques have been taken in consideration and enabled by the architecture by avoiding constructs that would block their use. In particular, attention has been paid to making horizontal scaling and load balancing possible. While these are mainly performace techniques, they also serve as fail safe mechanisms, ensuring availability.

D1.2-2.9-Correct	WP10, WP8, WP9, WP12, WP2	Annex F Threats	Architecture has to specify what "correct" means. This is ensured by reviewing the architecture documents. Further, some secure, i.e. correct, programmin aspects are handled in Annex F Threats. Correctness of implementation is verified through certification, which is a research topic of WP12. WP12 will also implement continued compliance validation procedures. Correctness of software modules is ensured and verified by WP8 using unit testing. Correctness of configuration is ensured and verified by WP9, again by testing. Sufficient test coverage is ensured by WP8 in the unit testing. Correctness is further ensured by code review, in which WP2 may participate. WP12 will perform overall validation of correct implementation by performing integration tests. Following the quality procedures specified in WP13 all parties contribute to provide adequate documentation of the correctness. If there is any doubt about correctness, and the ability of quality procedures to assess it, arises, external audits should be used to check to what degree the correctness is actually achieved and whether internal controls are sufficient.
D1.2-2.10-SeemsCorrect	WP10, WP12	n/a	Perception of correct behaviour is important for adoption. However, this topic is not addressed by the architecture. End-to-End human testing and surveys can be used to assess user's perception of the correct behaviour. Such surveys are WP10 responsibility.
D1.2-2.11-Transp	WP2, WP3	Sec 3.8 Properties of Web Service Binding; Sec 6. Oversight and Monitoring; and D.3 User Uses Dashboard	Transparency is supported by various oversight and monitoring features of the architecture. In particular, the Dashboard functionality provides transparency. Another transparency measure is provision of digitally signed receipts for each significant transaction.
D1.2-2.12-Compr	WP10, WP2, WP3	Secs 6. Oversight and Monitoring and D.3 User Uses Dashboard; WP3 modeling	User comprehensibility refers to making what is supposed to happen understandable. This is a problem of communcating business process model to the user. It can be addressed by WP3 through creating succinct and comprehensible models, and by WP2 through visualizing the business process and where the user stands in the Dashboard. The transparency and audit features of WP2 further add to the user comprehension. End-to-End human testing and surveys can be used to assess user's comprehension of the business processes and system behaviour. Such surveys are the responsibility of WP10.

D1.2-2.13-Easy	WP10, WP8, WP9	Annex E: Generalized Use Cases	Once mechanisms are in place for system to operate correctly and user to comprehend what is happening, the focus will shift to ease of use. Of course easy of use can also contribute to comprehension. Architecture can not contribute much to this requirements. Most of the work in this area needs to be done in the scope of WP8 and WP9.
D1.2-2.14-Priv	WP2, WP7	Sec 2.4.1 Data Model for Core Security Architecture; Sec 3.1 Core Security Architecture - Flows; Sec 3.2.1 Attribute Pull Model; D4.1 Identifiers and Discovery	Privacy preception can be enhanced through user interface design (WP9, WP8) and measurement of the preception will be completed by WP10. The contractually available privacy protections, as drafted by WP6, can further contribute to the privacy perception. Hard privacy protection rests on avoidance of correlation handles and of unnecessary collection of data (minimal disclosure). These are addressed in various parts of the architecture.
D1.2-2.15-Resp	WP2, WP6	Sec 3.1 Core Security Architecture - Flows; Sec 3.8 Properties of Web Service Binding CR212-Trail	Holding people responsible and accountable for their actions is addressed in various ways by the architecture. There is a long trail of proof starting from authentication and proceeding through the steps, such as concent, that are taken to authorize a transaction. Digitally signed protocol messages and signed audit train play a very significant role in ensuring nonrepudiation and supporting any law suits that may arise in this regard.
D1.2-2.16-Mitigate	WP2	Sec 6 Oversight and Monitoring	Architecture achieves risk mitigation mainly through depth of defence measures such as intrusion detection, monitoring, and audit. Another important way to mitigate risks is to follow strict operating procedures. Some of these are specified as compliance requirements while others may be achieved through well designed business processes, especially for implementing security critical functions.
D1.2-2.17-AuditUntamp	WP2	Sec 6.3 Log Audit; CR212-Trail	The architecture mandates digital signing of critical logs.
D1.2-2.18-AnCredi	WP2	Sec 3.1 Core Security Architecture - Flows; A.1 Supported Authentication and Login Systems	Credibility of Authentication hinges mainly on the use of technically strong solutions (one time passwords, tokens, appropriate crypto), and on the original registration of the user. Conveyance of authentication must happen in a secure fashion as well. See also Reqs. D1.2-7.3-An

D1.2-2.19-AzCredi	WP2, WP7	Sec 2.2.3 Authorization Subcontinent; Sec 3.1 Core Security Architecture - Flows; A.3 Authorization Systems	Credibility of Authentication hinges mainly on use of technically strong solutions and convincing the users that the solutions are applied in the right level of granularity. See also Reqs. D1.2-7.6-Az
D1.2-2.20-Az	WP2, WP7	Sec 2.2.3 Authorization Subcontinent; Sec 3.1 Core Security Architecture - Flows; A.3 Authorization Systems	Authorization is pervasive in TAS^3 architecture. Policy Enforcement Points appear at multiple points and they connect to the Master PDP. WP7 addresses the internal structure and operation of the Master PDP.
D1.2-2.21-DataProtLaw	WP2, WP6	Sec 2.4.3 Using Sticky Policies to Protect Data; Sec 3.2.1 Attribute Pull Model; CR213-Backup; CR26-SSL	The architecture addresses the data protection law issues by first ensuring minimal disclosure using a data pull model to obtain PII attributes on a strictly need-to-know basis; then, by ensuring that confidentiality of data is preserved, and that user designated policies are enforced.
D1.2-2.22-GovtAccess	WP2, WP7, WP6	6.3.1 Log Collection and Storage	Legitimate government access is granted by issuance of appropriate tokens or decryption keys to the authorities upon presentation of a valid court order. Alternatively the plain text can be surrendered.
D1.2-2.23-SemIOP	WP2, WP7	D2.1 Sec 3.7.3 Semantic Interoperability Engine; D7.1 sec Semantic Handler	The semantic interoperability is a requirement at two levels: for authorization and associated vocabularies, such as roles or credentials, and for data. The Semantic Handler component addresses practical mapping. It is integrated with Credentials Validation Service.

D1.2-2.24-NoPanopt	WP2	General	The architecture supports multiple data sources (and their discovery) so there is no need to aggregate too mauch sensite data in any one place. Even where some aggregation happens, we recommend using pointers to the data rather than aggregating the data itself. The most sensitive aglomeration of correlation handles occurs in Identity Provider, Discovery Servive and ID Mapper service. To some extent also Delegation service is in position to have database that allows cross referencing and correlation. The fact that such services have to exist, is a limitation of the current (2010) architecture. The mitigating factors include: (i) there can be multiple instances of each of the said services, thus avoiding single entity that knows everything about everybody (however there could still be single entity that knows everything bout somebody, (ii) we separate architecturally these entities to avoid single entity knowing everything about somebody. Such separation, is somewhat difficult due to similarity of the data requirements of the said services. Generally if the separation is implemented, cumbersome data synchronization arrangements are needed, which arrangements themselves can pose security threat. It would appear that mitigation (ii) may be in conflict with req D1.2-2.2-FeasDep. Another possibility is to consciously not implement mitigation (ii) and instead implement additional vigilance and mitigation steps such as enhanced access controls and host security on the database server. See also Reqs. D1.2-3.8-Separate and D1.2-7.27-Separate
D1.2-3.1-BPMTools	WP3	n/a	The architecture has nothing applicable at the tool level.
D1.2-3.2-ModelDrivenCfg	WP3, WP2, WP10	Sec 5 Using Business Process Modelling to Configure the Components	WP3 is responsible for developing the business models. WP2 will provide help in determining what should be modelled and how, and it will develop the configuration layer that exploits the models and derives the actual configurations.
D1.2-3.3-Dash	WP3, WP2	Sec 2.2.1 Major Components; Sec 6.3 Log Audit; D.3 User Uses Dashboard;	The dashboard, especially when driven directly by the BPM, can provide a user interface for visualizing the ongoing business processes.

D1.2-3.4-UID	WP2, WP3	D4.1, Discovery, ID Mapper, Registry Server	The identity in the business process can be more or less a local affair. By no means should it introduce a globally unique identifier requirement. More likely, a pseudonym will be used for each Service Provider. However, the pseudonym given to any given participant of the business process will stay fixed for the duration of the business process. See also Reqs. D1.2-5.10-UID and D1.2-9.12-UID
D1.2-3.5-TaskAssign	WP3, WP7	n/a	From an architectural point of view, the dynamic reassignment of roles is reduced to an update of an attribute at an attribute authority. The inherent limitation is that any attribute statement or claim remains valid until it expires. The expiry time should be relatively short, but if it is not, the increased window of opportunity should be factored-in to the risk assessment.
D1.2-3.6-CoordAz	WP3, WP2	GAP	The roles-to-actions mapping is expected to be defined already at the time when the business process is defined. This means that the only variable is the users to roles mapping. The binding of a user to a role can be fairly dynamic, i.e. evaluated each time a credential or token is requested. However, once a token is issued, it tends to stay valid until expiration.
D1.2-3.7-Deleg	WP2, WP7	D2.1 Sec 3.3 Delegation	Delegation is handled by issuance of delegation tokens. These tokens can express both minor delegation where user instructs the system to act on his behalf, and major delegation where user gives a power-of-attorney to another user or business process (modelled as a type of juridical person). Other forms of delegation involve role editing and policy editing to authorize the delegatee. Narrowing the delegation to per process instance level requires additional mechanisms. The delegation tokens can be created with usage limitations that narrow the use to one business process instance, e.g. “use once” token or token that specifies the business process instance identifier. See also Req. D1.2-7.1-Deleg
D1.2-3.8-Separate	WP3	n/a	The separation of business roles depends on the business process definition. For Trust Network administrative processes these are defined at the Trust Network level. See also Reqs. D1.2-7.27-Separate and D1.2-2.24-NoPanopt.

D1.2-3.9-BPRecover	oWP2, WP7	GAP; D2.1 Sec 3.5 Break-the-Glass Authorization; D2.1 Sec 3.8 Properties of Web Service Binding	Recovery from a business process fault is generally implemented by retrying the operation after some adjustments are made. This could mean rediscovering a provider for faulting service, interacting with a user to gain consent, or invoking a Break-the-Glass scenario and obtaining a new credential capturing the Break-the-Glass status. GAP: Architecture does not expressly describe the retry, although such possibility is implicit in ID-WSF. See also Req. D1.2-4.6-BrkGlass
D1.2-3.10-JITPerm	WP2, WP7	A.1.1 SAML; D2.1 Sec 3.2.1.3 Back Channel, Simple; GAP	SAML token format supports NotOnOrBefore and NotAfter constraints. This allows the access credentials, expressed as SAML tokens, to be constrained in duration. The attribute pull model and the discovery funtionality support just-in-time issuance of the credentials. GAP: Credential revocation in general may need more architectural specification.
D1.2-3.11-UPAPD	WP2	GAP; D4.1 [TAS3D41ID]	This requirement really has two facets: policy editing by user (UPA) and policy discovery. GAP: Architecture has to specify the Policy Authoring interface. The Policy Discovery is supported using general discovery and Credentials and Privacy Negotiation mechanisms. Once the discovery and negotiation are done, there may still be need to consult the user. This can be achieved by the Interaction Service. See also Reqs. D1.2-7.7-UPA, D1.2-9.2-UPA.
D1.2-3.12-SPManifest	WP3, WP2	D2.1 Sec 5 Using Business Process Modelling to Configure the Components; D4.1	It is not clear what is meant by “user” in this requirement. It seems nonsensical that the end users would be able to edit the business process nilly willy. The business modelling will (GAP 2010) use IGF techniques such as CARML to describe the data needs, data available, and the associated policies. Discovery functionality and Trust and Privacy Negotiation allows data sources to be located according to available data and the policies under which the data is offered.
D1.2-3.13-BPAdapt	WP3, WP2	D4.1, D4.3, D3.1 Sec 4.4.3 Substitution of Parts of BP	Architecture provides many mechanisms for adaptation, such as Discovery functionality and Credentials and Privacy Negotiation functionality. They are used in setting up an adapted business process instance and they may also be used during the business process process for further adaptation. Business Process Engine uses these facilities to select parties that are invoked by the instance and to coordinate the course of action that the application takes.

D1.2-3.14-PIIPolicyDisco	WP2, WP3	3.5.3 Semantic Interoperability Engine; D4.1, D4.3	Discovery functionality can be keyed on acceptable policies and also on the Credentials and Privacy Negotiation. Static knowledge of some of the policy properties can be modelled and represented using IGF CARML. The ontologies of policies can interoperate using the Semantic Interoperability Engine.
D1.2-3.15-SecPreserve	WP3, WP8, WP2	D4.1; D8.2; 3.5.3 Semantic Interoperability Engine	Security and policy preservation in business process adaptation involves discovering (using Discovery or IGF CARML): policies and security properties of the available services. It then requires applying policy merging (see D8.2) and ontological techniques to ensure that the security and policy properties are preserved.
D1.2-4.1-EnfUCPol	WP7, WP2	2.4.3 Using Sticky Policies to Protect Data; D.8 Consenting to PII Release or Manipulation	The Sticky Policy and PII Consent Service features allow enforcement and attachment of the user centric policies.
D1.2-4.2-BPPrivacy	WP2, WP3	D4.1; Sec 3.1 Core Security Architecture - Flows; Sec 6.3.3 Privacy Issues: What to Collect and What to Report	Privacy of the user in a business process is fundamentally ensured by use of pseudonyms and other measures to avoid correlation handles. A tricky problem will be the avoidance of correlation handle in the audit trail as here privacy protection is in conflict with accountability. This will be researched and incorporated to section 6.3.3 in future versions of the Architecture deliverable [18].
D1.2-4.3-SecDemo	WP11, WP9, WP12	GAP; Sec 3.1 Core Security Architecture - Flows	Demonstrating the security features requires effectively a use case, a sequence or choreography of actions to be performed by a user, and some observation points that would allow the spectator to peek inside TAS^3 at some critical points, e.g. to see that different pseudonyms are used, or that the data is encrypted. The choreography can be partially based on the Flows described in the Architecture. The WP9 scenarios should provide useful material for developing the demonstration.
D1.2-4.4-CourtProof		Sec 3.1 Core Security Architecture - Flows; Sec 3.8 Properties of Web Service Binding CR212-Trail	Proof for nonrepudiation of transaction is generally catered for. Proof of fulfilment of obligations like data non-retention may be very hard to support, except perhaps through human audit. No technical solution is known. See also Req. D1.2-6.17-TechBind.
D1.2-4.5-ComplyPolicy	WP7, WP2, WP10	Sec 2.2.3 Authorization Subcontinent	Full compliance of, e.g. data retention policy, can be difficult to prove. However, a large measure of compliance can be imposed through the Authorization process.

D1.2-4.6-BrkGlass	WP7, WP2	Sec 2.2.3 Authorization Subcontinent; Sec 3.5 Break-the-Glass Authorization	Break the Glass scenario is addressed as part of the authorization process. See also Reqs. D1.2-3.9-BPRecover
D1.2-4.7-PolicyDisco			Similar to D1.2-3.14-PIIPolicyDisco. Propose to merge requirements.
D1.2-5.4-RepuFB			See also Req. D1.2-6.9-Complaint.
D1.2-5.10-UID	WP2, WP5	D2.1 sec 3.8 Properties of Web Service Binding; D2.4 sec 2.2 Supported Identity Web Services Systems; D4.1 sec 1.1 Format and Properties of IDs	The general TAS^3 plumbing conveys user's (pseudonymous) identity sufficiently to provide accountability to the Trust Feedback process. See also Reqs. D1.2-3.4-BPIdent and D1.2-9.12-UID.
D1.2-5.12-TrustRank	WP5, WP2	D2.4 Sec 2.7 "Using Trust Scoring in Discovery"	The plumbing for passing the trust scores around is based on special XACML status responses.
D1.2-6.1-IntakePers	WP2, WP3		The intake processes for individual users will be highly dependent on the nature of the Trust Network and the services that are offered in it. The Trust Network level modelling is used to describe these processes and they are implemented using Trust Network Process Manager.
D1.2-6.2-IntakeOrg	WP2, WP3, WP10		The intake process for organizations is modelled at Trust Network level and executed using Trust Network Process Manager. Some aspects of the intake process will involve certification, which should be addressed by WP10.
D1.2-6.3-WhatHowWhyWho	WP3, WP2	Sec 5 Using Business Process Modelling to Configure the Components; D.8 Consenting to PII Release or Manipulation	The specification may happen in two ways: (i) as a model, in which case it is handled by business process modelling using technologies like IGF and CARML; (ii) as a user interface to the user. This can be done using the PII Consent Service.

D1.2-6.4-Min	WP2, WP3, WP9	Sec 2.2.3 Authorization Subcontinent; Sec 3.2.1 Attribute Pull Model; Sec 5 Using Business Process Modelling to Configure the Components	Data collection minimization starts from business process modelling in which the data is actually needed is identified. The needs can be expressed using IGF techniques, such as CARML. The configuration can be propagated such that the minimal collection is enforced through the authorization system. The authorization features can be used to limit the access to the data on the basis of need. The pull model helps to minimize the exposure of the data. As a result only the data that is actually needed by the business process instance will be shared (i.e. do not send data just in case the business process might need it). The pilots are responsibile for identifying meaningful minimal disclosure policies for their industries. See also Reqs. D1.2-7.5-Min, D1.2-9.23-Min
D1.2-6.5-Purpose	WP2	Sec 2.4.3 Using Sticky Policies to Protect Data	Purpose can be seen as a usage constraint attached to the data. Sticky policies are our main method for addressing this.
D1.2-6.6-Consent	WP3, WP2	D.8 Consenting to PII Release or Manipulation	User's consent can be structural, this should be considered in the business models; or it can be explicitly gathered using PII Consent Service or other user interfaces.
D1.2-6.7-Reconsent	WP2, WP3	D.8 Consenting to PII Release or Manipulation	Main vehicle for capturing user's consent will be the PII Consent Service. However, business process modelling should capture whether consent is needed, e.g. if information changes due to administrative needs.
D1.2-6.8-UAc	WP2, WP3	Sec 2.4.3 Using Sticky Policies to Protect Data	The main vehicle for user access is the Dashboard. The processes for the access can be modelled at Trust Network level and implememented in Trust Network Process Manager. The data origin requirement can be addressed using sticky policies. See also Reqs. D1.2-8.6-UAc and D1.2-9.7-UAc.
D1.2-6.9-Complaint	WP2, WP5	CR30-GA; D.3 User Uses Dashboard	Complaint capture will be handled in several ways: the business processes should have an explicit feeback stage (see Req. D1.2-5.4-RepuFB). The Dashboard functionality integrates a way to raise concerns, and finally the audit function of the Trust Network will handle any (serious) complaints.
D1.2-6.10-Redress	WP6, WP2	CR212-Trail; CR30-GA; Sec 6.3 Log Audit; Sec 6.5 Administrative Oversight; E.5 How should the governance be organized?	The redress is based on proving that a bad thing happened. This is pervasively handled by use of digital signatures and by the auditing and monitoring functions of the architecture; and being able to hold organizations and people responsible. The latter is handled by the legal and contractual framework that the Trust Network adopts.

D1.2-6.11-Confid	WP6, WP2	CR26-SSL; CR213-Backup; CR30-GA; E.5 How should the governance be organized?	Establishing duties on processors is done contractually in Trust Network Governance Agreement. Technical protections, such as encryption are addressed pervasively in the architecture.
D1.2-6.12-Sec	WP2, WP7	Sec 2.5 Authorization Process; Sec 2.6 Enforcement Process; Sec 3.1 Core Security Architecture - Flows; A.1 Supported Authentication and Login Systems	The architecture specifies numerous security features that aim at preventing unauthorized access. These include credible authentication and credible authorization. See also Reqs. D1.2-2.18-AnCredi and D1.2-2.19-AzCredi.
D1.2-6.13-Contract	WP6	CR24-File	The architecture does not specifically address the contract work, but we list it as a compliance requirement CR24-File.
D1.2-6.14-Compat	WP10	CR30-GA; Sec 6.1 On-line Compliance Testing	Use of compatible software is a certification requirement. While there probably needs to be a clause to this effect in the Trust Network Governing Agreement. The On-Line Compliance Testing certainly addresses this concern.
D1.2-6.15-MinPolicy	WP3, WP10	CR30-GA; Sec 6.1 On-line Compliance Testing	The required set of policies should be modelled at Trust Network Level. Since they are expected to be the same across all organizations, they are the prime candidate for On-line Compliance Testing.
D1.2-6.16-Bound	WP6	CR30-GA	This matter has to be addressed legally, in the Governance Agreement for example. There is no technical solution.
D1.2-6.17-TechBind	WP2, WP6	CR30-GA; CR212-Trail; Sec 3.1 Core Security Architecture - Flows; A.1 Supported Authentication and Login Systems	The legal binding has to be addressed in the Governing Agreement. However, the architecture contains numerous features. Namely, these are use of digital signatures and credible authentication. They facilitate forning and proving the binds. See also Req. D1.2-4.4-CourtProof.
D1.2-7.1-Deleg	WP2, WP7	Sec 3.2.2.1 N-Tier Linking Service Model; Sec 3.3 Delegation	Delegation is handled by issuance of delegation tokens. These tokens can express both minor delegation where user instructs the system to act on his behalf, and major delegation where user gives a power-of-attorney to another user or business process (modelled as a type of juridical person). See also Req. D1.2-3.7-Deleg

D1.2-7.2-RoleSig	WP2	GAP	Signing in a role can be viewed as a form of auhtorization in some cases. Thus if the user authorized something and the system entity signed it, then it could be argued that the user is bound. Thus the net effect of user signing is achieved. However, if the user is really expected to sign with his own private key, the Architecture does not offer any specific solution. We could document use of DSS or DSS-X as a way to do this. We could also invent a sophisticated client side solution to get the signetures to happen.
D1.2-7.3-An	WP2	CR216-EntAn; Sec 3.1 Core Security Architecture - Flows; A.1 Supported Authentication and Login Systems	The architecture supports both user authentication and entity authentication. See also Reqs. D1.2-2.18-AnCredi.
D1.2-7.4-MultiCred	WP2	D3.2 Sec 3.2 Tokens, Access Credentials	The notion of "credential" is squishy here. It could mean authentication credential, or it could mean claim of some attribute. Multiple authentication credentials and step-up authentication are supported by SAML. Multiple attribute claims can be obtained either using push or pull model, see Architecture sec 3.2 Tokens, Access Credentials.
D1.2-7.5-Min	WP2	D2.1 Sec 3.2.1 Attribute Pull Model	Minimum credential release principle is best implemented by pull model where the business process requests only the credentials it actually needs. See also Reqs. D1.2-6.4-Min, D1.2-9.23-Min.
D1.2-7.6-Az	WP2, WP7	D2.1 2.2.3 Authorization Subcontinent	The architecture foresees several authorization points (PEPs)s. See the authorization subcontinent, which addresses this requirement exhaustively.
D1.2-7.7-UPA	WP2, WP3	GAP; D2.1 Sec 4.2.5 Anatomy of an Audit and Dashboard Provider, Event Infrastructure; D2.1 Annex D.3 User Uses Dashboard	o GAP: Architecture has to specify the Policy Authoring interface. The Dashboard may be of some help in defining this interface. For on demand ad-hoc policy setting the PII Consent service may also be useful. See also Reqs. D1.2-3.11-UPAPD, D1.2-9.2-UPA.
D1.2-7.8-NoColl	WP2	2.4.1 Data Model for Core Security Architecture; D2.1 Sec 3.1 Core Security Architecture - Flows; D2.1 Sec 3.1.1.1 Authentication Request	Collusion prevention is most convincingly achieved by ensuring that no correlation handle is leaked. Avoidance of correlation handles has been a major motivation in the Core Security Architecture data model and flows. Essentially the problem is solved by making sure that every pair-wise federation relation uses a different and ungueassable user ID. See also Req. D1.2-2.14-Priv.

D1.2-7.9-Revoc	WP2, WP7	GAP	The current model of the architecture is that if a token is emitted, then it is valid for its validity period and no further checks will be made. Thus this requirement adds an additional burden that was not foreseen in the beginning. The solutions are similar to public key certificate revocation: online check (perhaps using SAML or OCSP stype protocol) or vigorous circulation of revocation lists.
D1.2-7.10-Target	WP2	A.1 Supported Authentication and Login Systems	The ID-WSF security mechanisms and SAML tokens support AudienceRestriction which is intended exactly for this type of targeting.
D1.2-7.11-PolMerge	WP7, WP4	GAP; D7.1 Sec 7 Dynamic Management of Policies Infrastructure	Policy Merging is the cousin of attribute merging. At runtime the policy merge is done by Master PDP. GAP: At data access time, the data aggregation function must also address policy aggregation.
D1.2-7.12-CredStepUp	WP2	Sec 3.2.1 Attribute Pull Model	The credentials step-up is supported by the attribute pull model.
D1.2-7.13-CredDisco	WP2	Deliverable 4.1 [TAS3D41ID]	The attribute pull model is complemented by the discovery function to ensure that the location of the needed attributes can be determined.
D1.2-7.14-Sub	WP2	Sec 3.1 Core Security Architecture - Flows	Subdelegation is fully supported through the token passing scheme described in the Core Security Architecture.
D1.2-7.15-PushCred	WP2	Sec 3.2.2 Linking Service: Attribute Push Model	The push is in addition to the ability to pull. In the push model, the user introduces additional credentials in an unsolicited fashion. In the pull model only the credentials that the process requests are supplied. Thus in the push model the user can volunteer more than would be strictly necessary.
D1.2-7.16-Nym	WP2, WP4, WP7	Sec 2.4.1 Data Model for Core Security Architecture; Sec 3.1 Core Security Architecture - Flows	Fully preudonymous operation is supported by the architecture and the protocols that have been chosen (e.g. SAML SSO and ID-WSF web services).
D1.2-7.17-Increm	WP2, WP4	Sec 3.6 Trust and Privacy Negotiation; Deliverable 4.1 [TAS3D41ID]	The incremental credential release is part of the Trust and Privacy Negotiation. This function is mainly implemented by the discovery functionality.
D1.2-7.18-Seq	WP2	3.2 Tokens, Access Credentials	Linking sequential requests can happen at many levels. On session level the architecture does not (and probably can not) prevent linking. However, a lot of effort has been spent on whether sessions can be linked together or not. To satisfy this requirement, Transient NameIDs should be used.

D1.2-7.19-DynaUpd	WP8, WP12, WP2	D.1 Zero Downtime Updates	Dynamic update of policies is a desireable deployment time feature. This has only tangential influence to the architecture, see Annex B. Mostly dynamic update support will depend on implementation capabilitities and the way the software is deployed and managed.
D1.2-7.20-PADeleg	WP2	GAP	GAP: The architecture does not currently have clear description of how Policy Authoring is to be accomplished, much less how it could be distributed to various players. For the users some facilities exist in PII Consent Service and the Dashboard.
D1.2-7.21-Safe	WP2, WP5	Sec 3.1 Core Security Architecture - Flows; Sec 6.3 Log Audit	Resilience against fraud is mainly achieved by stringent authentication of the actors, followed by a good audit trail that allows everybody to be held responsible for their actions. Additional resilience against fraud is provided by the reputation based trust mechanism, which should prevent repeated instances of detected fraud. Resilience against mistakes is much more difficult to achieve. See also Req. D1.2-2.7-Safe.
D1.2-7.27-Separate	WP3	D2.4 sec 1.2 Composition and Co-location of Architectural Components	The separation of business roles depends on the business process definition. For Trust Network administrative processes these are defined at the Trust Network level. See also Reqs. D1.2-3.8-Separate, D1.2-2.24-NoPanopt, D1.2-6.80-Separate.
D1.2-7.28-Audit	WP2	D2.1 Sec 6.1 Dashboard; D2.1 Sec 6.4 Log Audit; D2.4 Sec 2.7 Realization of the Audit and Dashboard Function	The components of the system send to the Audit Bus individual audit records. Generally these will summarize one access or attempted access. Summarization across multiple accesses is done at the Dashboard.
D1.2-7.29-RoleMap	WP7, WP2	D7.1 Sec 6.4 Design of a Credential Validation Service; D7.1 Sec “Ontology Handler”	The Credentials Validation Service (CVS) is responsible for checking the credentials, such as roles and attributes, for authenticity and then mapping them to the vocabulary used in the rules configured to the PDP. The CVS uses Ontology Handler (a.k.a. Ontology Mapper) to map the validated roles and attributes to the vocabulary used by the rule set.
D1.2-8.6-UAc			See also Reqs. D1.2-6.8-UAc and D1.2-9.7-UAc.
D1.2-9.1-SecData	WP2	D2.1 sec 3.2.1 Attribute Pull Model	TAS3 core security architecture flows, and in particular Attribute Pull model ensures secure access. The discovery functionality further facilitates use of multiple sources.

D1.2-9.2-UPA	WP7	GAP	Policy editing is supposed to solve this, but currently (2010) we do not have satisfactory solution. The achievable granularity of control will greatly depend on the abilities of the underlying data model and Policy Enforcement Point (PEP). Especially in case of legacy systems it is unrealistic to expect fully granular control. It may also be unrealistic to expect users to comprehend the full detail of the fully granular data and policies. Finally, determining and visualizing the full consequences of a policy choice is a difficult problem. See also: D1.2-9.25-Consequences
D1.2-9.3-SSO	WP2	D2.4 sec 2.1 Supported Authentication and Login Systems	The core security architecture flows include Single Sign-On.
D1.2-9.5-Trail	WP2	D2.4 sec 2.7 Realization of the Audit and Dashboard Function	The Audit Bus collects summary of all the accesses. This summary will allow the user to use Drill In interface to access the detail of the audit trail. Access controls and authorization are applied in terms of who can post to audit bus as well as who can listen to the audit events. Access controls also determine whether drill down is available. Access controls ensure that only the user has access to his dashboard.
D1.2-9.6-UPADetail	WP7	GAP; D2.4 sec 2.1.1 System Entity Authentication	Satisfying this requirement is a very tough policy editing job. Granularity down to organizational or server level is easily achieved by the architecture and its System Entity Authentication mechanims. If granularity needs to progress to level of individual users, we encounter the issue of properly identifying the user when pseudonymous identifiers are used. Generally same solution as in delegation needs to be adopted: use invitations to pseudonymously introduce the users to each other.
D1.2-9.7-UAc			See also Reqs. D1.2-6.8-UAc and D1.2-8.6-UAc.
D1.2-9.8-UAudit	WP2	D2.4 sec 2.7 Realization of the Audit and Dashboard Function	The Dashboard and audit drill down service provide this functionality, subject to access controls.
D1.2-9.9-UPADyn	WP7, WP2	D2.1 sec 4.1 Protocol Support for Conveyance of Sticky Policies; D2.1 sec 6.2.3 Propagation of Rectifications by the Originating Authority	The policy enforcement dynamically queries Policy Decision Points. This requrement is satisfied if the privacy policies can be made dynamically available to the PDP with immediate effect. A mechanism of such dynamic policy distribution is Sticky Policies. Another is the Subscription and Notification Pattern. See also: D1.2-9.24-UPADyn

D1.2-9.12-UID	WP2	D4.1 sec 1.1 Format and Properties of IDs	The pseudonymous properties of the identifiers ensure that the identification of users is only possible with user consent (e.g. user says who he is) or by consulting the detailed audit trail of the IdP or Discovery Service. Such drill down is controlled by appropriate access controls. See also Reqs. D1.2-3.4-UID and D1.2-5.10-UID.
D1.2-9.17-PolicyComb	WP7	D7.1 Sec 5.3 Conflict Resolution Policy; D7.1 Sec 7 Dynamic Management of Policies Infrastructure	The Master PDP will dispatch authorization request to a number of PDPs depending on policy languages employed as well as multiple policy authorities. If multiple PDPs are consulted, the Master PDP will combine the results according to combination policies.
D1.2-9.18-Journal	WP2	D2.1 sec 6.1 Dashboard; D2.1 Annex NN Enumeration of Audit Events; D2.4 sec 2.7 Realization of the Audit and Dashboard Function	!!TAS3 addresses journaling in the audit sense in that each operation is logged in summary form to the audit bus. However, this does not log the actual data to the Audit Bus. This is to avoid Panopticon threat centered around the Audit Bus and Dashboard seeing too much data and becoming fat target. Thus the journaling requirement may be in conflict with req D1.2-2.24-NoPanopt. The !!TAS3 audit trail does not attempt to address journaling in the sense that database inconsistency could be recovered.
D1.2-9.19-Integ	WP2, WP4	D2.1 sec 3.8 Properties of Web Service Binding; D2.4 sec 2.2.2 Liberty ID-WSF Profile; D2.4 sec 2.2.1 Framework; D4.2; D8.1	The protocol bindings of the architecture apply digital signatures and authentication at appropriate places to ensure this. The repository services ensure the integrity and authenticity of of the data while in storage and when delivered from storage.
D1.2-9.20-Confid	WP2	D2.1 sec 3.8 Properties of Web Service Binding; D2.4 sec 2.2.2 Liberty ID-WSF Profile; D2.4 sec 2.2.1 Framework	The protocol bindings of the architecture apply encryption and access control at appropriate places to ensure this.
D1.2-9.21-AnLvl	WP2	D2.4 sec 2.1 Supported Authentication and Login Systems; D2.4 sec 2.7 Using Trust Scoring in Discovery	The authentication levels are expressed during SSO as Authentication Context Class Reference, which can express the authentication technology as well as the intitial strength of user intake, registration, identity proofing, and vetting. The approach taken by !!TAS3 is compatible with major international standards and trends in eGovernment authentication and identity proofing. Authorization is performed based on authentication and presented credentials. Concept of “level” is not applicable to authorization. Levels of trust can be conveyed using the XACML special status returns.

D1.2-9.22-TrustEst	WP6, WP5, WP2	D6.2 sec 8.1 Intake process; D5.1 sec 4 Trust Services; D2.4 sec 2.1.2 SAML item 11	A very basic level of trust is established at the partner intake phase. On technical level initial trust is established at the metadata exchange phase. Afterwards, the trust is managed using Trust and Reputation engine.
D1.2-9.23-Min	WP3, WP7, WP2	Sec 2.2.3 Authorization Subcontinent; Sec 3.2.1 Attribute Pull Model; Sec 5 Using Business Process Modelling to Configure the Components	The business process modelling captures the data needs of a business process. These needs are usually satisfied by discovering an authority that can supply the data, and then querying this athority to obtain the data (pull model). Occasionally the push model may be used aw well, but it is difficult to organize minimality of data access in push scenario. All data releases are subject to authorization, which is driven by policies. The flexibility of policy formulation allows any scenario to be catered (but wrong policies can lead to inadvertent release of data). See also Reqs. D1.2-6.4-Min, D1.2-7.5-Min
D1.2-9.24-UPADyn	WP7, WP2	D2.1 sec 4.1 Protocol Support for Conveyance of Sticky Policies; D2.1 sec 6.2.3 Propagation of Rectifications by the Originating Authority	The policy enforcement dynamically queries Policy Decision Points. This requrement is satisfied if the privacy policies can be made dynamically available to the PDP with immediate effect. A mechanism of such dynamic policy distribution is Sticky Policies. Another is the Subscription and Notification Pattern. See also: D1.2-9.9-UPADyn
D1.2-9.25-Consequences	WP2	D2.1 sec 6.1 Dashboard	Ideally an identity mirror concept should be implemented. Currently (2010) the best approximation that allows the user to see where the data propagates is the Dashboard. See also: D1.2-9.2-UPA

Requirements from D1.2 First iteration that have not been changed * D1.2-2.1 : TAS^3 Architecture MUST be feasible to implement * D1.2-2.2 : TAS^3 Architecture MUST be feasible to deploy * D1.2-2.3 : TAS^3 Architecture MUST support plurality of service business models * D1.2-2.4 : TAS^3 Architecture MUST support multiple software suppliers * D1.2-2.5 : TAS^3 Architecture MUST be platform independent * D1.2-2.6 : TAS^3 Architecture MUST be programming language agnostic * D1.2-2.7 : TAS^3 Architecture MUST be fail safe, i.e. failure should not lead to security breach * D1.2-2.8 : TAS^3 Architecture MUST be available * D1.2-2.9 : Implementation MUST correctly	WP2, WP10	D2.1 sec 6.1 Dashboard; D2.4 sec 2.7 Realization of the Audit and Dashboard Function	The primary means of reporting authorization failures is via Audit Bus. The Trust Network operator should listen to these events.

D1.2-10.11-AzFailNotifTrust	WP2, WP10, WP5	D2.1 sec 6.1 Dashboard; D2.4 sec 2.7 Realization of the Audit and Dashboard Function	The primary means of reporting authorization failures is via Audit Bus. The Trust and Reputation Infrastructure should listen to these events.
D1.2-10.12-ModelIf	WP2, WP10		Typical Service Provider that joins Trust Network will describe its services in terms of (i) SAML Metadata, (ii) Registration of EPR, and (iii) WSDL. Currently (2010) no facility to register or distribute WSDL is provided.
D1.2-10.13-ModelAz	WP7, WP10, WP2		Current (2010) we do not adequately capture authorization model. It is expected that the WP10 test case generation activity can use the actual policies to derive the test cases. No facility to register authorization model is provided either.
D1.2-12.1-Grok	WP11	n/a	This is not a requirement addressable in architecture. In general, TAS^3 should provide training so that everybody can comprehend it.
D1.2-12.2-DokuAc	WP11	n/a	Project requirement, not an architecture requirement. Ideally should be addressed by the dissemination work package (WP11).
D1.2-12.3-WorkLoad	WP13	n/a	Project requirement, not an architecture requirement. Fundamentally this is a project management issue.
D1.2-12.4-Escalate	WP13	n/a	Project requirement, not an architecture requirement. Fundamentally this is a project management issue.
D1.2-12.5-DokuCVS	WP12, WP13, WP8, WP9	n/a	Project requirement, not an architecture requirement. Fundamentally this is a project management issue.
D1.2-12.6-ProjComm	WP13	n/a	Project requirement, not an architecture requirement. Fundamentally this is a project management issue.
D1.2-12.7-CompChk	WP12, WP8, WP9, WP10	n/a	Project requirement, not an architecture requirement. Fundamentally this is an integration issue. WP10 work, although focussed on the On-line testing, can provide some regressing testing framework as well (for module developers to use before they submit the modules to certification).
D1.2-12.8-CtlEnv	WP12, WP10	n/a	Project requirement, not an architecture requirement. Fundamentally this is an integration issue. WP10 needs to define what are the controlled production environements that software should be tested against.

D1.2-12.9-MadTest	WP10, WP12, WP8, WP9	n/a	The On-line Compliance Testing functionality requires negative testing and sometimes the only way to achieve this is to have in every component a known, triggerable, way to fail.
D1.2-12.10-MultiEnv	WP12, WP10	n/a	WP10 test suites should specify the secnarios, WP12 should be ready to support these scenarios.
D1.2-12.11-KickStart	WP12	n/a	The ability to recreate test conditions is immensely important. Some techniques that can be used towards this end are Kick Start and instantiation of canned virtual hosts.
D1.2-12.12-SubInst	WP8, WP9, WP12	n/a	Sub-component installation scripts are good practise as they document what is component specific.
D1.2-12.13-Vfy	WP2	Sec 6 Oversight and Monitoring; A.2.2 Liberty ID-WSF	User triggered verification of system's correct functioning depends on every system component implementing a "dry-run" feature, such as ID-WSF ¡ProcessingContext¿ urn:liberty:sb:2003-08:ProcessingContext:Simulate SOAP header. Further assurance of correct functioning can be obtained from the Dashboard.
D1.2-12.14-Case	WP8, WP9, WP12, WP10, WP3, WP7, WP2, WP5	n/a	Provision of specific evil test cases is mainly responsibility of the particular software developers. However, designers of the business processes, identity management, architecture, and reputation are well positioned to generate particularly insidious test cases and simulated attacks. These resources should be used to make sure all known attacks are covered in the testing.
D1.2-12.15-Valid	WP2, WP10	Sec 6 Oversight and Monitoring	User triggered validation can be implemented to some degree using the Dashboard. However, it does not seem feasible to allow each and every user to audit everything about the system at will. Therefore, beyound the Dashboard functionality, most users will have to content themselves with trusting the Trust Network level audits and On-line Compliance Testing.
D1.2-12.16-OnlineTst	WP10, WP2	Sec 6.1 On-line Compliance Testing; A.2.2 Liberty ID-WSF	Continuous On-line testing is principally supported by "dry-run" features of the architecture. The actual implementation of the testing is carried out by WP10.
D1.2-12.17-Doku	WP8, WP9, WP7, WP2	n/a	The architecture will strive to deliver most clear documentation feasible.
D1.2-12.18-ExtDoku	WP12, ZXID, etc.	n/a	To the extent that the "external" dependencies are actually projects of TAS^3 participants, we expect them to deliver documentation up to the project standard.

D1.2-12.19-ReadersGuide	WP8, WP9	n/a	The architecture will attempt to implement a reader's guide, but this quite likely is not going to be compliant with this requirement, neither should it be.
D1.2-12.20-Train	WP11, WP2	GAP	Training sessions about architecture should have succinct materrial. GAP: This material does not exist yet.
D1.2-12.21-ChgMgt	WP12, WP8, WP9, WP13	n/a	Architecture documents are revision controlled under cvs tas3repo:arch. Further, any externally released copy has a two digit release numbers that advances for every minor release.
D1.2-12.22-Plan	WP8, WP9, WP7, external	n/a	The planning exercise is not in scope of the architecture.
D1.2-12.23-BugTraq	WP12	n/a	Bug tracker is not in scope of the architecture.
D1.2-12.24-RelRepo	WP12	n/a	Release repository is not in scope of the architecture.
D1.2-12.25-IfCat	WP12, WP2, WP8, WP9	GAP	Architecture will contribute to the interface catalog in due time. There will be additional interfaces defined by WP8 and WP9 that are not in scope of the architecture. WP8 and WP9 will contribute these separately.
D1.2-12.26-RefImpl	WP2, WP4	GAP, D4.3	Architecture plans to provide a reference implementation for realistic online testing. This is not available yet. Deliverable D4.3 provides a simulation of the functionality.
D1.2-12.27-ComOnto	WP9, WP2	D2.2	Common reference data model, i.e. an ontology, will be delivered by the ontology activities of WP2. However, this model is limited to a very high level, with a drill down in the authorization area, until WP9 liaises with ontology.
D1.2-12.28-AppOnto	WP9, WP2	D2.2	Application ontologies, and their mapping, are an active research topic of TAS^3 . Architecture foresees this as an Attribute Broker.
D1.2-12.29-MockUp	WP8, WP9, WP7, WP12	n/a	A Mock Up compenent is typically able to provide standard response irrespective of input and will act as a stand-in until the real component can be developed (or is stable enough). Use of Mock-Ups is an integration and testing strategy that allows project to stay on schedule.
D1.2-12.30-root	WP12, WP13	n/a	Root access for key project authors/developers will certainly reduce friction and make the project more efficient.

8.1 Gaps

The following table lists gaps found between requirements and the M24 edition of the TAS^3 architecture. These requirements are addressed in the M36 edition of the architecture, as described.

Req.	Primary Responsibility	Architecture Component	How addressed
D1.2-3.10-JITPerm	WP2, WP7	A.1.1 SAML; D2.1 Sec 3.2.1.3 Back Channel, Simple; GAP	GAP: Credential revocation in general may need more architectural specification.
D1.2-3.11-UPAPD	WP2	GAP; D4.1	GAP: Architecture has to specify the Policy Authoring interface. See also Reqs. D1.2-7.7-UPA, D1.2-9.2-UPA.
D1.2-3.12-SPManifest	WP3, WP2	GAP? D2.1 Sec 5 Using Business Process Modelling to Configure the Components; D4.1	It is not clear what is meant by "user" in this requirement. It seems nonsensical that the end users would be able to edit the business process nilly willy.
D1.2-5.12-TrustRank	WP5, WP2	Trust PDP	D2.4 Sec 2.7 "Using Trust Scoring in Discovery" provides the plumbing for passing the trust scores around.
D1.2-7.11-PolMerge	WP7, WP4	GAP; D7.1 Sec 7 Dynamic Management of Policies Infrastructure	GAP: At data access time, the data aggregation function must also address policy aggregation.
D1.2-9.2-UPA	WP7	GAP	Policy editing is supposed to solve this, but currently (2010) we do not have satisfactory solution. The achievable granularity of control will greatly depend on the abilities of the underlying data model and Policy Enforcement Point (PEP). Especially in case of legacy systems it is unrealistic to expect fully granular control. It may also be unrealistic to expect users to comprehend the full detail of the fully granular data and policies. Finally, determining and visualizing the full consequences of a policy choice is a difficult problem. See also: D1.2-9.25-Consequences
D1.2-9.6-UPADetail	WP7	GAP; D2.4 sec 2.1.1 System Entity Authentication	Satisfying this requirement is a very tough policy editing job. Granularity down to organizational or server level is easily achieved by the architecture and its System Entity Authentication mechanims. If granularity needs to progress to level of individual users, we encounter the issue of properly identifying the user when pseudonymous identifiers are used. Generally same solution as in delegation needs to be adopted: use invitations to pseudonymously introduce the users to each other.
D1.2-9.25-Consequences	WP8, WP2	Dashboard, Identity Mirror	The identity mirror functionality is only partially addressed by dashboard. More work is needed.

D1.2-10.12-ModelIf	WP2, WP10		Typical Service Provider that joins Trust Network will describe its services in terms of (i) SAML Metadata, (ii) Registration of EPR, and (iii) WSDL. Currently (2010) no facility to register or distribute WSDL is provided. More work is needed in registering and distributing complete model.
D1.2-10.13-ModelAz	WP7, WP10, WP2		Current (2010) we do not adequately capture authorization model. It is expected that the WP10 test case generation activity can use the actual policies to derive the test cases. No facility to register authorization model is provided either.

9 Requirements fulfilled by existing solutions

The objective of this section is to give an overview and analysis of the existing solutions that can be used in the development of TAS^3 and those selected for use in the TAS^3 project. The complete list and details of existing solutions that were considered for use by the various work packages are in Appendix D.

We use tables to give an overview of the existing solutions, the requirements they fulfill and the selected solutions. For better readability, we preferred to show the results in multiple tables instead of a very large table that includes all the existing solutions and all the requirements that they fully or partially fulfill. Each table contains a subset of the existing solutions suggested by a subset of the TAS^3 work packages.

The tables are organized as follows. We first grouped shared solutions together and then listed in each table all the other solutions that were considered by those work packages. For example, Work Package 3 and Work Package 7 have PERMIS as a common solution. So, we have included in Table 9.5 all the solutions suggested by those two work packages. Further, Work Package 7 and Work Package 10 have common solutions. Hence, these and all the other solutions used by Work Package 10 are included in Table 9.5. The solutions selected for use in the TAS^3 project research and development activities are highlighted with grey columns. The columns of the compared solutions are delimited with extra white stripes.

Further, we noticed from the inputs of the partners that an important criteria in selecting software is the license conditions of the solutions. The TAS^3 partners prefer open source solutions or open standards when they are available. In order to make these choices visible, we also inicated whether the given solution is open source (O), proprietary (Pr), or subject to both, here called a dual licensing system (D).

Some solutions only partially fulfilled a given requirement. In case of partial fulfillment of a requirement we used (P). If the requirement is fulfilled by the solutions then we denoted that with an (F). No indication means that the solution does not fulfill the requirement in any way.

In each section we also included a summary of the justifications for the selected solutions. The detailed justifications with additional information on the solutions are included in Appendix D.

9.1 Existing solutions considered and selected by WP 3, 7 and 10 (CNR)

Existing solutions considered by work packages 3, 7 and 10 are as follows:

- s1: Intalio Designer, BPMS and Tempo
- s2: Oracle BPM-Suite
- s3: IBM Web Sphere Integration Developer
- s4: ActiveBPEL Community Edition Engine
- s5: jBPM
- s6: PERMIS
- s7: Trustbuilder2
- s8: Shibboleth software from Internet2
- s9: SAMP PHP
- s10: ZXID
- s11: Lasso
- s12: Authentic
- s13: WS Guard
- s14: TAXI

Solutions s1 through s5 can all be used for business process modeling. Intalio Designer BPMS is the solution of choice since it is open source software; it provides graphical modeling as well as a process execution engine and integrates both parts; and, the process modeling tool together is a very comprehensive and comfortably usable tool.

PERMIS (s6) are going to be used by both WP 3 and WP7. PERMIS is selected because: it is open source software, is modular; allows plug and play with an XACML PDP; and has more required functionality than any other package.

Trustbuilderv2 (s7) is selected because it is a configurable open source solution for trust negotiation. It is written in Java and allows plugin modules for policy evaluation and negotiation strategy. It allows credentials and policies to be written in any language providing the correct plugins are available. Whilst although WP7 activities will probably include writing some plugins in order to support the policies and credentials of TAS3, nevertheless they anticipate that the TrustBuilder2 infrastructure will support this.

Solutions s8 through s10 provide SSO functionality. The selection has not yet been finalized since it requires further investigation. ZXID has already been selected for the project and also facilitates SSO. The selection is nevertheless not exclusive. ZXID is selected because: it is written by a SAML, ID-WSF, and XACML insider; it is interoperable; it is SAML 2.0 and IDWSF 2.0 certified in its commercial (Symlabs) incarnation; it is developed by a TAS^3 contributor, so ensures good support. ZXID will be used by both WP7 and WP10 in their research and development activities. It is also included in the architecture.

WS Guard (s13) and TAXI (s14) are both developed by CNR as a result of research in related areas. There are no comparative tools performing the same functionalities.

Solutions	**s1**	**s2**	**s3**	**s4**	**s5**	**s6**	**s7**	**s8**	**s9**	**s10**	**s11**	**s12**	**s13**	**s14**
Access	O	Pr	Pr	Pr	O	O	O	O	O	O	O	O	O	O
D1.2-3.1	F	F	F	F	F									
D1.2-3.2	F	F	F	F	P									
D1.2-3.3	F	F	F	F										
D1.2-3.4	P	P	P	P	P									
D1.2-3.5						P								
D1.2-3.6						P								
D1.2-7.1						P								
D1.2-7.2						P								
D1.2-7.3								F	F					
D1.2-7.6						F								
D1.2-7.7												F		
D1.2-7.9						F								
D1.2-7.10												F		
D1.2-7.12						P								
D1.2-7.13						P								
D1.2-7.14						P								
D1.2-7.15						P								
D1.2-7.16					F	P								
D1.2-7.17							F							
D1.2-7.18								F	F					
D1.2-7.21						P								
D1.2-7.23						P								
D1.2-7.24						F								
D1.2-7.26												F		
D1.2-10.1													F	F
D1.2-10.2										F	F	F	F	F
D1.2-10.8										F	F	F		

Table 9.1: Existing solutions considered by WP3, WP7 and WP8 and the related TAS^3 requirements

9.2 Existing solutions considered and selected by WP 4 and 5

Existing solutions considered by work packages 4 and 5 are as follows:

- s15: K.U. Leuven's Demonstrator Framework
- s16: Belgian e-ID Card

- s17: Encryption Algorithm AES
- s18: Tulip Trust Management
- s19: Postgre SQL
- s20: ORACLE
- s21: SunXACML
- s22: Trust Policy Wizard

The K.U. Leuven Demonstrator Framework (s15) was selected because it is a proven technology that can easily be extended. During the first year of TAS3, the demonstrator framework has been extended with support for complex business processes, the break-the-glass function, and advanced policy enforcement. The Belgian e-ID Card (s16) is used as the authentication token that has the highest level of assurance that is currently available in the consortium. And AES (s17) is a standard encryption decryption algorithm with, currently, proven strength.

Feedback data required for Reputation Trust Management (RTM) is typically stored in a database management system such as Oracle Database (s20) or PostgreSQL (s19). The key advantage of the RTM system in TAS^3 is that reputation is computed directly inside the database. Existing database management systems do not support this computation. Compared to Oracle Database, PostgreSQL is open source and thus allows for the necessary modifications. The other existing solutions had no alternatives with respect to the necessary requirements of these work packages. Compared to other existing CTM systems TuLiP Trust Management (s18) excels in key aspects for TAS^3 especially with respect to flexibility of the syntax, user autonomy and automation. The Trust Policy Wizard (s22) is selected because providing a wizard is a powerful yet straightforward way of supporting user selected policies. The work package team does not exclude the possibility for more integrated solutions such as e.g. natural language policy editors as the project proceeds.

SunXACML was selected because it is a well known open source XACML implementation; uses an OASIS standard policy language; supports a wide range of access control policies, and can be combined with PERMIS which will be used and further developed by work packages 3 and 8.

Solutions	**s15**	**s16**	**s17**	**s18**	**s19**	**s20**	**s21**	**s22**
Access	O	D	O	O	O	Pr	O	O
D1.2-2.1	F							
D1.2-2.5	F							
D1.2-2.6	F							
D1.2-3.7	F							
D1.2-10.5	F							
D1.2-12.1	F							
D1.2-5.6				F				
D1.2-5.3					F	F		
D1.2-5.4					F	F		
D1.2-5.1							F	
D1.2-7.6							F	
D1.2-5.9								F
D1.2-4.2	P							
D1.2-4.3	P							
D1.2-4.4	P							
D1.2-4.5	P							
D1.2-4.6	F							
D1.2-4.8	P							
D1.2-4.9	P							

Table 9.2: Existing solutions relevant to WP4 and WP5 and the requirements the solutions fulfill

9.3 Existing solutions considered and selected by WP 8

Existing solutions considered by Work Package 8 are as follows:

- s23: FEDORA
- s24: DSpace
- s25: CDSWare
- s26: EPrints

Among existing open source repositories Fedora (s23) was selected because: it is a repository that can be completely integrated in a SOA.Hence, all functionalities of the repository are accessible through a SOAP or REST based web service interface; and it is an open source solution with a strong community behind it.

Solutions	**s23**	**s24**	**s25**	**s26**
Access	O	O	O	O
D1.2-8.6	F	P	P	P

9.4 Existing solutions considered and selected by WP 9

Existing solutions considered by Work Package 9 are as follows:

- s27: Saturn
- s28: ePars
- s29: OPUS
- s30: Mahara
- s31: PebblePad
- s32: Kenteq Competent Web Application
- s33: Personal Health Record (PHR)
- s34: Patient Information Location Service (PILS)

The demonstrators, by definition take over existing software from their domain partners. The UK employability pilot relies on Saturn (s27), ePars (s28), OPUS (s29), Mahara (s30) and PebblePad (s31). Saturn (s27) is the database which is the source of student data as held by the institution. ePars (s28) allows access to Saturn data without having to access Saturn directly, which WP9 in Nottingham would not be allowed to do for demonstration purposes. OPUS (s29) is an open source placement co-ordination package available to WP9 in Nottingham. Mahara (s30) was selected by the team because out of the over 80 ePortfolio systems in use in the UK at the moment, not all are free and not all are web-based. Many ePortfolio systems remain under institutional control. Mahara is open source and WP9 Nottingham are in contact with the developers. They are also part of a strong community of interest that is currently developing Mahara which can provide further support in its use for work placements. PebblePad (s31) is a Web-based, learner-controlled system. The system supports exports in a variety of standards, including UK-LEAP and IMS ePortfolio. Futhermore, by using PebblePad the Nottingham team will be able to access candidates who have established ePortfolios using this system and offer a rich source of demonstrator data. WP 9 Nottingham team also has a good relationship with the company through other project work.

The WP9 Netherlands team working on employability will build upon the Kenteq Competent Web Application (s32). Solutions comparable to Competent are often embedded in software for internal HR processes. Competent supports the APL and profile matching process as such, independent from the organisation or individual who applies for an employability service. There are no other off-the-shelve application available who supports employability processes. The application is in English and in Dutch which is also an advantage for the NL demonstrator.

The WP9 healthcare demonstrator will rely on the Custodix PILS (Patient Information Location Service s34). This service integrates a medical data viewer with a system for distributed search of medical information. It will be

used in both the personal health record use case track (cf. Deliverable D9.1) and the backup pilot track involving the summary record (cf. Deliverable D1.4) as a front-end for locating (medical) information on TAS^3 enabled data providers. The Personal Health Record (PHR - s33) implementation required for the WP9 scenarios would originally be provided by MediSoft, however this partner has left the consortium. No replacement has been officially appointed yet (candidates are available).

The solutions used by WP 9 will be used to create the demonstrators that will be used to validate some of the TAS^3 requirements in the application domain and will also generate further requirements to the TAS^3 project. Hence, in its current state, existing solutions do not fulfill any of the requirements of the TAS^3 project.

9.5 Existing solutions considered and selected by WP 10 (UNIZAR)

Existing solutions considered by Work Package 10 are as follows:

- s35: EyeTracker
- s36: Click Tracks/ Web Tracks
- s37: Structural Modelling Tools (EQS, PLS, SPSS)

These are the standard tools used by and accessible to the UNIZAR team.

Solutions	**s35**	**s36**	**s37**
Access	Pr	Pr	Pr
D1.2-10.4			F
D1.2-10.5	F	F	F
D1.2-10.6	P	P	F

9.6 Existing solutions considered and selected by WP 12

Solutions	**s38**	**s39**	**s40**	**s41**	**s42**	**s43**	**s44**	**s45**	**s46**	**s47**	**s48**	**s49**	**s50**	**s51**	**s52**
Access	Pr	O	O	O	O	Pr	O	O	O	Pr	O	D	O	O	O
D1.2-12.1				F	F	F					F	F			
D1.2-12.2	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.3	F						F	F					F		
D1.2-12.4	F						F	F					F		
D1.2-12.5	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.6	F	F	F	F	F	F	F	F	F	F	F	F	F		
D1.2-12.7														F	F
D1.2-12.11														F	F
D1.2-12.15														F	F
D1.2-12.17	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.18	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.19	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.20				F	F	F					F	F			
D1.2-12.21	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.3	F						F	F					F		
D1.2-12.24	F	F	F	F	F	F	F	F	F	F	F	F	F		
D1.2-12.25	F	F	F	F	F	F	F	F	F	F	F	F			
D1.2-12.27					F	F	F				F	F			
D1.2-12.30	F	F	F	F	F	F	F	F	F	F			F		

Table 9.5: Existing solutions considered by WP12 and the related TAS^3 requirements

Existing solutions considered by Work Package 12 are as follows:

Common documentation repository:

- s38: Jira (proprietary)
- s39: Concurrent Versions System CVS (open source)*
- s40: Subversion SVN (open source)
- s41: MediaWiki (open source)
- s42: DokuWiki (open source)
- s43: Confluence (proprietary)
- s44: Redmine: (open source)
- s45: Trac (open source)*
- s46: GIT (open source)
- s47: ActiveCollab (proprietary)*
- s48: Semantic Media Wiki (open source)
- s49: OntoPrise Onto Studio (dual licence)

Central issue and defect tracking:

- s38: Jira (proprietary)
- s44: Redmine: (open source)
- s45: Trac (open source)*
- s50: BugZilla (open source)

Continuous integration incl. testing:

- s51: Hudson (open source)*
- s52: Nagios (open source)*

Data type level and other conceptual documentation:

- s41: MediaWiki (open source)
- s42: DokuWiki (open source)
- s43: Confluence (proprietary)
- s48: Semantic Media Wiki (open source)
- s49: OntoPrise Onto Studio (dual licence)*

WP12 provides the coordination and services to integrate the software modules produced by the security and application work packages. Because the complete constellation of components (web services) must meet specic requirements that directly reect on the individual components, WP12 also has a stake in guiding and monitoring the WPs that produce the components.The solutions listed above are under consideration to support the guiding and monitoring activities. This requires extensive evaluation of the existing solutions, which is currently under way. The likely candidates are denoted with an asterisk.

9.7 Existing solutions considered and selected by WP 2 (VUB)

The only existing solution considered by Work Package 2 (VUB) is as follows:

- s53: DOGMA Studio Workbench

DOGMA Studio Workbench is the only tool that suppor ts DOGMA inspired ontology and it fulfills the Requirement D1.2-2.23.

10 Requirements that call for new solutions

In this section we list the future activities of all partners to fulfill the requirements which are not addressed by existing solutions but are imminent to the TAS^3 project. Here again a difference is to be noticed with WP6 and WP9. WP6 depends on the activities of other work packages to fulfill its data protection requirements. We have been working closely with WP6 to refine the requirements to include legal and policy requirements, or to generate new requirements for these. These refinements in their initial form now included in D1.4 Section 6 [22] and will have to be discussed with all partners in the depth before the next iterations of these deliverables.

Similarly, the demonstrators in WP9 are in the process of preparation in their application domains. Hence, upon our request, they have listed an outline of their general activities with respect to their application domains. Once the application domain activities are fixed, we will expect them to review their requirements according to the conditions of their application domains. Resulting from those, WP9 will also list activities for the fulfillment of those application domain specific requirements. Once the demonstrators are running, WP9 will also generate new requirements for the TAS^3, which will have an effect on all the work packages. If these requirements are generated before the second and final iteraction of D1.2, we will capture those new requirements and trace their effects on the existing requirements.

In this iteration of the deliverable we are missing a concretization of the validation activities. Although suggestions for activities for validating the fulfillment of requirements were suggested by almost all work packages, these suggestions are very general. This is partially due to the fact that the requirements are at such a high level that they still need to be refined into verifiable sub-requirements which can then be validated. But, the gap analysis and the interaction analyses would have been difficult to execute with requirements of very high granularity. This is a tension between the need for a high-level analysis and low-level analysis necessary when doing requirements analysis. We hence conclude that the validation activities have to be revisited once the requirements are refined and consolidated.

10.1 Activities of WP2

WP2 partner for architecture has not submitted these activities. Sampo will map the requirements to the architecture next week.

D1.2-2.23	will be fulfilled by applying the DOGMA-MESS methodology to the TAS3 domain. We first plan to develop an upper ontology to allow the different topics (i.e. Security, Privacy, and Trust) to be modules within the same ontology. We are then going to use IT standards to develop the Upper Common Ontology (UCO) (as per the DOGMA methodology). We are then going to elicitate domain specific knowledge to develop the Lower Upper Ontology and any knowledge that need to be committed to the UCO through ontology evolution

10.2 Activities of WP3

D1.2-3.4	requires an authentication component provided by WP7 and design and implementation work in the role management component of the used BPMS (for a client component). D1.2-3.4 will be validated in the test bed.

D1.2-3.5 D1.2-3.6 D1.2-3.7 D1.2-3.8 D1.2-3.10 D1.2-3.11	D1.2-3.5 through D1.2-3.8, D1.2-3.10 and D1.2-3.11 require additional research to define a security model, as existing literature approaches are not sufficient and/or coherent. They require design and implementation work for both modeling and runtime enforcement. Especially, D1.2-3.6 and D1.2-3.10 require research how the security infrastructure can allow a process to change permissions. D1.2-3.11 requires the design of application-specific ontologies and a policy framework applicable to PII (not WP3's task: to be handled in WP4?). The concepts for D1.2-3.5 through D1.2-3.8, D1.2-3.10 and D1.2-3.11 will be validated by applying them to the demonstrators. Implementation will be validated by executing these applications in the test-bed. On the one hand, this is done for the original applications (including user interaction). On the other hand, we will replace user interaction by mock services and devise test-cases that run automatically.
D1.2-3.6 D1.2-3.7	D1.2-3.6 and D1.2-3.7 require the specification and enforcement of policies. This is partly in the scope of WP7, and the PERMIS product already fulfils the decision part of runtime enforcement. In WP3 we will have to design and implement specialized process-specific security policy management. Delegation (D1.2-3.7) requires (basic) usability testing. Individual, distinct functions (like role assignment, D1.2-3.6, or delegation, D1.2-3.7) will receive unit tests.
D1.2-3.9	requires additional design, and implementation, in the BPEL execution engine.
D1.2-3.12	is best applicable to an extensive eco-system, which will not be realised during the duration of the TAS^3 projects. Lacking such an infrastructure, we will validate it using case studies.
D1.2-3.13 D1.2-3.14 D1.2-3.15 D1.2-3.16 D1.2-3.17	D1.2-3.13 through D1.2-3.17 requires extra research in TAS^3 on the topic secure adaptation of business processes and model driven development of policies. They require the specification of changes of the process model, the check if these changes are allowed in respect to several criteria (consistency as well as security related), and the migration of process instances. Further on, security specifications at the business level have to be transformed on to the technical level by generating elements of the process execution level, (parts of) security policies and configuring process-specific enforcement components. The results must be implemented and validated. D1.2-3.13 through D1.2-3.17 requires (basic) usability testing for distinct components and integration testing in the WP12 testbed. It will be validated by applying them to the demonstrators, as well.

10.3 Activities of WP4

[danny we are missing validation activities for each.]

D1.2-4.1	will be implemented based on the application independent policy enforcement point (cf. wp7). This requirement will be validated during the accreditation and each re-accreditation of a TAS3 service provider.
D1.2-4.2	will be implemented based on the identifier mapper that is developed within WP4, cf. D4.2. This requirement will be validated during the accreditation and each re-accreditation of a TAS3 service provider.
D1.2-4.3	will be implemented based on the demonstrator framework that is developed within WP4, cf. D4.3. This requirement will be validated by implementing the demonstrators.
D1.2-4.4	will be implemented based on the dashboard service (cf. WP2) and the audit guard (cf. WP4, D4.1 and D4.2). This requirement will be validated during the accreditation and each re-accreditation of a TAS3 service provider. It will also be validated whenever external audits, service users or a data subjects exercise the rights given by data protection legislation, namely those referring to the openness and transparency of data and information processing.

D1.2-4.5	will be implemented based on the consistent business processes, cf. WP6, WP3 and WP9. This requirement will be validated during the accreditation and each re-accreditation of a TAS3 service provider. It will also be validated whenever external audits, service users or a data subjects exercise the rights given by data protection legislation, namely those referring to the openness and transparency of data and information processing.
D1.2-4.6	will be implemented using the break-the-glass mechanism, cf. WP7 and D4.3. This requirement will be validated during the pilots. This requirement will be validated during the accreditation and re-accreditation of a TAS3 service provider. It will also be validated while exercising the data subject's or auditor's right to detail the steps used while processing the related information.
D1.2-4.7	will be implemented based on the trust and privacy policy negotiation mechanism that will be developed by WP4 in collaboration with WP2, WP5 and WP7 and in compliance with WP6. This TPPN mechanism requires new research. This research has already been bootstrapped within FP7/PrimeLife. This requirement will be validated during the accreditation and each re-accreditation of a TAS3 service provider. It will also be validated whenever external audits, service users or a data subjects exercise the rights given by data protection legislation, namely those referring to the openness and transparency of data and information processing.
D1.2-4.8	will be implemented in the demonstrator framework of D4.3 using the input of WP10 on usability aspects. This requirement will be validated by the users during the different pilots.
D1.2-4.9	will be implemented based on the trust and reputation scoring mechanisms developed in WP5. This requirement will be validated during the accreditation and re-accreditation of a TAS3 service provider.

10.4 Activities of WP5

D1.2-5.1	will be fulfilled by a Trust PDP component developed within WP5. The Trust PDP will answer trust policy evaluation queries by calling specialized trust services, facilitating their interaction and combining their answers. The Trust PDP shall support XACML request/response context for trust evaluation queries to offer a standardized interface. Note that the use of XACML contexts does not imply the used of the XAMCL policy language; the Trust PDP will use a trust specific policy language. The XACML request context is flexible enough to embed the trust specific information and policies. The Trust PDP will be implemented by extending a standard XACML PDP.
D1.2-5.2 D1.2-5.8	will require research on flexible integration of different forms of trust management. This should result in an integrated trust architecture. The Trust PDP forms the interface to this architecture.
D1.2-5.3	will require research on flexible behavioural policies and efficient evaluation methods for these policies. The results of this research will be incorporated in a Reputation Trust Management Engine built around a relational database.
D1.2-5.4	A Trust Information Collection Point will be created which stores authenticated feedback and makes it available to the reputation based trust service. Ensuring authenticity of the feedback will need to be supported by the feedback procedure in the application business process (see requirement RA-1).
D1.2-5.5	will be fulfilled by the TAS3 dashboard, which provides a trust feedback form. This feedback form gives the user an opportunity to rate his or her satisfaction with the current process execution.

D1.2-5.6	will be fulfilled by the CTM service which will be built around the TuLiP TM system and using the Credential Verification Service developed by WP7.
D1.2-5.7	will be fulfilled by the KPITM service. This component gathers and combines several KPI factors from KPI factor providers, e.g. [Google Analytics].
D1.2-5.9	will be fulfilled by an enhanced trust policy wizard which adds support for structural trust policies and novel trust metrics to the exitings trust policy wizard.
D1.2-5.11	will be fulfilled by the contractual framework. (WP6)
D1.2-5.10	will be fulfilled by the TAS^3 authentication framework (WP7)

The various activities will be validated by experiments on the demonstrator test-beds. Testing realistic use case scenarios will evaluate the effectiveness and flexibility of the Trust language and architecture components such as the Trust PDP and TM services. End user experiments will validate the policy wizard and the usability of the feedback mechanism and understanding of the trust policies; i.e. do they produce the expected results.

10.5 Activities of WP6

WP6 is both a horizontal and vertical project within TAS3. The vertical aspects are the definition of legal requirements and the creation of contractual elements. TAS^3 cooperation with other groups in these vertical aspects is to assure that we are bother reviewing legal requirements that address all needs and functions as well as drafting contract elements that support all roles and business needs.

The horizontal elements of TAS^3 are much more difficult to define in terms of deliverables at any point in time as they are part of an iterative process. This is the refinement of understanding how law, policy and technology interact; where law supplements policy and technology; where technology supports law in logs, or audit; and where policy and technology are bound by legal obligations on the parties.

In terms of process improvement to achieve these ends and further unify function of TAS^3 as a whole, WP6 is working with the requirements team in developing the questions that further refine the requirements and also working more closely with the demonstrator projects to assure that as questions arise in developing implementation and deployment strategies legal questions are addressed and various options of law and policy are presented.

With Technical teams WP6 operates more as an on-demand resource. While we provide requirements documents and templates as resources our ongoing functions are more geared to helping in arriving at consensus in technical development options where issues of how to achieve legal compliance or definitions of what is legally required to be compliant are at issue. As in many legal related issues these are often processes of interpretation and balancing.

10.6 Activities of WP7

D1.2-7.1	requires enhancements to the delegation service of PERMIS in order to support a) the delegate pulling his credentials from the delegation service b) the delegator pushing his credentials to PERMIS c) credentials in SAML format
D1.2-7.2	requires design and implementation from scratch
D1.2-7.4	requires enhancements to the authorization infrastructure to support the linking of credentials from multiple providers when the user is known by different IDs at the different providers (design and implementation)

D1.2-7.5	will be fulfilled by additional enhancements to the SAML protocol and subsequent implementation
D1.2-7.7	requires design of a GUI for setting a privacy policy and a means of sticking this privacy policy to the users PII.
D1.2-7.8	may be impossible to fully support in technology. May ultimately require legal policies and prosecutions to stop this ie. D1.2-7.27. Technology can only go so far, such as ensuring different identifiers are used for the same user at different SPs. We will investigate how much can be supported by various means
D1.2-7.9	requires full support for revocation adding to PERMIS. Note that SAML based protocols cannot support this requirement so it will need enhancements to SAML if this is to be used for credentials.
D1.2-7.10	requires enhancements to credential issuer to insert the target field, and to PERMIS to check the value of this field in the credentials that it validates.
D1.2-7.11	requires a new authorization component, the Master PDP, to be designed and built.
D1.2-7.12	whilst PERMIS already has the capability of pulling multiple credentials from multiple sources, the PEP needs to trigger it at appropriate times to do the pulling. The design and implementation of this triggering mechanism is needed.
D1.2-7.13	requires the PEP to tell PERMIS where to pull the credentials from
D1.2-7.14	requires the same enhancements as D1.2-7.1
D1.2-7.15	requires support at the application level for the pushing of credentials.
D1.2-7.16	will need designing to ensure that all credentials can be tied to the pseudonyms.
D1.2-7.17	may be supported by the TrustBuilder2 package. We will need to investigate this and may have to either edit this package or write our own.
D1.2-7.19	requires enhancements to the PERMIS package to support the dynamic changing of policies.
D1.2-7.20	requires enhancement to PERMIS to support multiple policy administrators.
D1.2-7.21	requires validation of and possible enhancement to PERMIS existing support for separation of duties policies.
D1.2-7.22	needs BTG policies to be defined and the authorization infrastructure to support them.
D1.2-7.23	needs the PDP to support state based decision making. This can be engineered through the introduction of an application independent PEP and obligations.
D1.2-7.25	will be fulfilled through additional development of the PERMIS package.
D1.2-7.27	will be fulfilled through additional developments of the SAML package and/or legal policies in WP6.

10.7 Activities of WP8

Requirements D1.2-8.1, D1.2-8.2, D1.2-8.3, D1.2-8.4, D1.2-8.5 will be fulfilled through the implementation of software components. These will be validated using various testing methods which are mentioned in the activi-

ties below.

D1.2-8.1	Implementation of two gateways. We call this gateway on requester side *Service Requester ADPEP*. On provider side it is called *Service Responder ADPEP*. The two gateways will be implemented using the SOA (Service Oriented Architecture) approach. For testing purposes the Intalio BPEL engine on one side and the Fedora repository on the provider side will be exemplarily integrated.
D1.2-8.2	This will be done by the so called *TAS*^{3} *Apache module*. Risaris is working on this. Beside the Fedora reference repository Risaris provides other legacy databases to function as a data provider. They will test this component by replacing an existing Fedora repository with their legacy database combined with the RISARIS SOA gateway.
D1.2-8.3	The component, which will allow this interaction is called Intalio BPEL service interface. The reference BPEL engine is from our partner Intalio. On requester side we have to adapt the Intalio BPEL engine, so that it can be easily call TAS^3 secured services. Well test this functionality by demonstrating 4 use cases: Creating (ingesting) a new ePortfolio, modifying the ingested ePortfolio, deleting the ePortfolio and reading it.
D1.2-8.4	The generic client is based on the XForms provided by the Intalio BPEL engine. In the generic client we will integrate those XForms, so that they can be used without the Intalio BPEL engine in a more generic way. In a later phase of the project well replace the Business Process Engine by the generic client to test its functionality.
D1.2-8.5	The special database to provide this policy management functionality is called ADPEP Database. University of Nottingham is working on this. They plan to test the functionality within the demonstration of the CRUD use case: crating, reading, updating and deleting an ePortfolio or eHealth data.

10.8 Activities of WP9

The validation of the fulfilment of the requirements will be achieved through executing the demonstrators. A testing program will be developed in collaboration with WP10.

The activities of Work Package 9 will support validation of the requirements fulfillment activities of the technical WPs. WP9 is not building the TAS^3 architecture, rather WP9 is providing a realistic environment in which it can be tested. Our requirements come from the user viewpoint and need to be taken into account by all other WPs.

To fulfil the overall requirements of WP09 the NL employability, UK employability and eHealth demonstrator activities need to take the following set of steps:

- Scope the domain and establish a baseline: NL Employability demonstrators will be carried out in the scope of the scenarios described in D1.4 1.3 APL and 1.4 Mass layoff. UK employability demonstrators have decided to focus on data transfer to support education in employment, to be detailed in the next iteration of D1.4. The eHealth pilot focuses on exchange of medical information and patient empowerment within the context of Continuity of Care as described in D1.1.

- Identify a specific area or subset of the domain where TAS^3 could be usefully implemented: The demonstrator cannot engage with the whole domain at once. For the NL employability demonstrator it is possible to identify a smaller area where the processes described in D1.4 1.3 APL and 1.4 Mass layoff can be supported by and offer a test for the TAS^3 system. The UK employability demonstrator will in the first instance concentrate on data exchange to support student work placement. TAS3 enabled data exchange within the eHealth domain will be demonstrated in the context of the summary record (in which health care professionals are the main actors) and the Personal Health Record (in which the patient takes a central role).

  For all three demonstrators WP9 will establish and engage contacts who will be willing to take part in the demonstrator activity. Once a subset of the domain has been identified, organisations and individuals

who are able and willing to take part in a demonstrator need to be identified and briefed about the project. Any necessary risk assessment for their taking part in a demonstrator needs to take place at this stage.

- Work with these contacts to detail scenarios for demonstrator activity: Existing as is and to be scenarios need to be agreed in collaboration with demonstrator partners.
- Investigate existing systems and interactions: An understanding of how existing systems function and interact is needed, also any modifications needed to support web services and interoperability (needed for D1.2-9.15).
- Research additional systems that might be needed to support the scenario: Alternative systems (e.g. ePortfolio systems) may need to be examined.
- Define data flows and formats (needed for D1.2-9.15)
- Set up any new interoperability and data exchange between systems (needed for D1.2-9.15)
- Create any necessary hooks or feeds for the TAS^3 architecture
- Refine use cases: This may be necessary following an assessment of the technical feasibility of joining systems and implementing the TAS^3 architecture
- Assist with integration of TAS^3 functionality into existing systems and test that the user experience will be acceptable
- Carry out any user training needed to conduct demonstrators: this may include training in non-TAS^3 systems being interfaced with
- Conduct demonstrators implementing current versions of the architecture and systems, including interim testing and evaluation and ensuring any minor fixes are carried out
- Evaluate overall demonstrator outcomes and feed back to development partners to inform further iterations of development, design and build. This will include information about user perceptions and expectations.

In order for demonstrator activity to support the use cases to run, interoperability needs to be established between the systems being used; if this proves not to be possible, it will be necessary to research further alternative systems. As data is stored using a variety of formats and standards, and can be held behind firewalls, there is work to be done on moving data around the ecosystem for the basic use cases which the demonstrators will test. While this is not strictly work for TAS3, it is a requirement for setting up a testbed on which TAS^3 can be demonstrated. WP9 does not yet have a final list of systems to be used as this will depend on the exact set of demonstrator partners involved.

To validate that requirements have been fulfilled, WP9 will run the demonstrators using as-live systems and test data based on that from real life users. This activity will be used to fulfill test requirements 9.13 and 9.14.

However most of the requirements of this WP will be met by activities carried out by the WPs building the architecture and systems for the project. The demonstrator activity will be validating that these have been fulfilled. Only requirement 9.11 will be addressed directly by WP09 activity; the remainder of the demonstrator activities will ensure that the other requirements have been met.

10.9 Activities of WP10

D1.2-10.1
D1.2-10.2
D1.2-10.9

extra research on model-based automated testing of service-oriented compositions in necessary for the fulfillment of these requirements. The results of the research will be prototyped within the TAS^3 architecture. In particular, our intent is to develop a prototype version of the framework implementing the on-line testing strategy based on the manifested policies of the services. The methodology behind such framework will be supported by automatic generation and instantiation of test suites.
In our vision a service asking registered to a directory service will undergo two different kinds of periodic check since the request for registration. The first concerns the ability of the service of behaving according to its manifested policy and the second of being able to correctly interact with required services. Nevertheless some issues have to be considered in particular to derive a real implementation of the service and to better understand the applicability of the framework itself.
Trustable services are the ultimate goal of our research: we wish to increase the interoperability and testability of SOA by fostering the application of rigorous model based testing methodologies. The availability of a service registry enhanced with testing capabilities, granting the registration only to good services, should reduce the risk of run-time failures and run-time interoperability mismatches.

D1.2-10.4
D1.2-10.5
D1.2-10.6
D1.2-10.7

will be fulfilled through the development of specific measures of end-user perceptions. To be precise, we have to develop measurement tools that contemplate the true character of the concepts; that is, measures that represent the psychological perception of the system user. To do that, we will conduct the following activities:

- Firstly, measure development will be based on:
  - User test
  - Focus groups with experts and potential end-users
  - In-depth personal interviews
- Secondly, in order to validate the measurement tools developed by Unizar to evaluate end-user perceptions, we are following the steps recommended in scientific literature:
  - Content and face validity
  - Exploratory analysis of reliability and dimensionality
  - Confirmatory Factor Analysis
  - Convergent and discriminant validity
- Finally, we will apply structural modeling (EQS, PLS, SPSS) in order to determine relationships among variables.
- As a consequent stage of the measurement of perceptions about trust, usability and service quality and the relationships among them, an effective implementation must be carry on:
  - Firstly, based on end-user perceptions several guidelines and recommendations will be proposed.
  - Secondly, if designers consider it possible, these guidelines will be implemented in TAS^3 architecture and demonstrators following user-centric criteria.

D1.2-10.7

will be fulfilled according to the main accessibility guidelines (Section 508 Standards and WAI criteria). A manual or semi-automatic evaluation (e.g. HTML interfaces) will be developed

10.10 Activities of WP12

WP12 will be setting up the central resources required to deploy test beds, using the software packages mentioned before. Actual testing will be performed on the test bed by the development partners (unit tests) and WP10 (general tests).

D1.2-12.1 D1.2-12.2 D1.2-12.19 D1.2-12.20	Make sure that all relevant system and architecture documentation is available and accessible to everybody. This is done by having fixed process steps checking for this.
D1.2-12.3 D1.2-12.4 D1.2-12.21 D1.2-12.22 D1.2-12.23 D1.2-12.24	Maintain close contact with WP13 project management, to integrate formal software delivery into the integration process.
D1.2-12.5 D1.2-12.6 D1.2-12.23 D1.2-12.24 D1.2-12.25	Create and maintain central project resources to support the integration process. This requires both system administrator resources and content moderator/editor resources.
D1.2-12.7 D1.2-12.8 D1.2-12.10 D1.2-12.11 D1.2-12.13 D1.2-12.14 D1.2-12.15 D1.2-12.16 D1.2-12.26	Work with WP10 to establish continuous testing and integration processes on central test beds.
D1.2-12.9 D1.2-12.12 D1.2-12.17 D1.2-12.18 D1.2-12.19	Establish guidelines and rules for software developers so the delivered components can be integrated into the process, not just into the system.

11 Conclusion:

The contributions specific to the final iteration of the Deliverable 1.2 is as follows:

- we provide an the list of WP technical requirements with including new, refined (edited) and deleted requirements in the TAS^3 project after all the requirements analysis activities.
- we provide documentation of the analysis of Inter-WP requirements to consolidate the technical and legal requirements with the architecture. This work includes the development and use of an automated analysis tool to identify inconsistency candidates.
- we provide a mapping of global, technical and legal requirements to the components of the architecture, aligning all of the main artifacts developed in TAS^3.

We have also learned many lessons during the execution of Deliverable 1.2. The completion of the various interaction analysis activities in a distributed manner caused a great communication overhead which we had to resolve by organizing face-to-face meetings and workshop. Further, the interaction analysis provided the chance for various WPs to align their work and to resolve ambiguities. We are very excited about the Trac Wiki tool, but we are now aware that it is easy for partners to edit the wrong documents at the wrong time. Such unexpected editing may cause communication problems among the partners. Nevertheless, we have made the final list of requirements available on the Trac Wiki to be updated by the WPs as the project progresses. Finally, on a positive note, we have seen that interaction analysis is powerful in determining inter-WP requirement inconsistencies, gaps and overlaps. We plan to write a second paper to follow our recently submitted paper on the requirements engineering process in TAS^3 [15].

The contribution of the deliverable in general is threefold. It provides a gap analysis which was used to map out future activities. In order to complete the gap analysis, in the deliverable the partners have elaborated on the technical, legal and application domain requirements of TAS^3. The deliverable also provides an extensive analysis of the interactions of the TAS^3 requirements and maps out responsibilities and necessary cooperations for fulfilling these requirements.

More specifically, in Section 3 we revisited the objectives of TAS^3 and each work package. For each WP we stated the solved and unsolved problems that they are addressing in TAS^3.

In Section 4, we captured those requirements that are central and therefore of higher priority for each of the work packages. We also mapped out interdependencies between work packages as stated by the partners. In Section 5 those interdependencies were further elaborated from the viewpoints of the different WPs. The results of the interaction of legal and technical requirements, a novel research element in the deliverable, is presented in Section 6. In Sections 7 and 7 we mapped the global and technical requirements to the architecture. Overlapping and conflicting requirements, as well as other inconsistencies were analyzed and refined until a consistent and complete set of requirements were reached.

In Section 9 we listed existing solutions and the requirements they fulfill, which showed both: that the partners are aware of existing solutions and their utility for their research and development activities; and, that there is a need for future research and development in the area of trust and security in service oriented environments. In Section 10 we listed the planned activities of each work package. We expect partners to review this list, especially with regard to their validation activities as the project proceeds.

As we advanced with the requirements of TAS^3, it became evident that any further partitioning of the requirements into functional, security, trust and/or privacy requirements is unreasonable. This is due to the fact that this project is about building a trusted and secure service architecture that implements the data protection principles. Hence, most higher level requirements are non-functional requirements that go hand in hand, e.g., most security requirements also fulfill the security principle of data protection legislation. Further, functional requirements are de-emphasized in most of the project: the objective of TAS^3 is to define the security, trust and privacy aspects of communication between services, regardless of their functionality. Hence, we only distinguish the technical and legal requirements and do not further partition the requirements with respect to privacy, security and trust requirements, as it was planned in the earlier iterations of D1.2.

As we complete the final iteration of Deliverable 1.2, we conclude that we have consolidated the viewpoints into a monolithic set of technical requirements, whose interaction with both the legal requirements and the architecture are analyzed and validated. We believe D1.2 will continue to provide a stable basis upon which to complete the activities of the TAS^3 project.

Bibliography

[1] A. Aurum and C. Wohlin. Requirements interdependencies: State of the art and future challenges. In *Engineering and Managing Software Requirements*, 2006.

[2] E. Barka and R. Sandhu. Framework for role-based delegation models. In *The 16th Annual Computer Security Applications Conference (ACSAC'00), Los Alamitos, CA, USA*, pages 168 –177, 2000.

[3] O. Canovas and A. F. Gomez. Delegation in distributed systems: Challenges and open issues. In *The 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Republic,*, pages 499–503, 2003.

[4] P. Carlshamre, K. Sandahl, M. Lindvall, B. Regnell, and J. N. Dag. An industrial survey of requirements interdependencies in software product release plannin. In *RE '01: Proceedings of the Fifth IEEE International Symposium on Requirements Engineering*, pages 84 – 91, Washington, DC, USA, 2001. IEEE Computer Society.

[5] L. Casaló, J. Cisneros, C. Flavián, and M. Guinalíu. Determinants of success in open source determinants of success in open source software networks. *Industrial Management and Data Systems*, 2009.

[6] L. Casaló, C. Flavián, and M. Guinalíu. The role of perceived usability, reputation, satisfaction and consumer familiarity on the website loyalty formation process. *Computers in Human Behavior*, 24(2):324–345, 2008.

[7] D. Chadwick. Delegation issuing service for x.509. In *The 4th Annual Research and Development PKI Workshop, Gaithersburg, MD, USA*, 2005.

[8] D. Chen and G. Doumeingts. European initiatives to develop interoperability of enterprise european initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap. *Annual Reviews in Control*, 27:153 – 162, 2003.

[9] S. Chou, E. J. Lu, and Y.-H. Chen. . x-rdr: a role-based delegation processor for web-based information systems. *ACM SIGOPS Operating Systems Review*, 39(1):4–21, 2005.

[10] A. Cockburn. Goals and use cases. *Journal of Object Oriented Programming*, 1997.

[11] B. Crispo and G. Ruffo. Reasoning about accountability with delegation. In *3rd International Conference on Information and Communication Security*, 2001.

[12] E. Cristobal, C. Flavián, and M. Guinalíu. Perceived e-service quality (pesq): measurement validation perceived e-service quality (pesq): measurement validation and effects on consumer satisfaction and website loyalty. *Managing Service Quality*, 17(3):317–340, 2007.

[13] M. R. Czenko and S. Etalle. Core tulip - logic programming for trust management. In V. Dahl and I. Niemelä, editors, *Proc. ICLP 2007, Porto, Portugal*, volume 4670 of *LNCS*, pages 380–394, Berlin, October 2007. Springer Verlag.

[14] C. Flavián, M. M. Guinalíu, and R. Gurrea. The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information and Management*, 43(1):1–14., 2006.

[15] S. Gürses, G. Montagnon, M. Seguran, and N. Zannone. Requirements engineering within a security-oriented project: lessons learned requirements engineering within a security-oriented project: lessons learned. In *Requirements Engineering*, 2010 (submitted).

[16] P. Herings, G. v. d. Laan, and D. Talman. Measuring the power of nodes in digraphs. Technical report, Tinbergen Institute, 2001.

[17] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. in proc. In *12th International Conference on World Wide Web*, pages 640 – 651, 2003.

[18] S. Kellomäki. Deliverable 2.1: Architecture. Technical report, TAS3, 2009.

[19] J. M. Kleinberg. Authoritative sources in a hyperlinked environment. *Journal of the ACM*, 46(5):604 – 632, 1999.

[20] N. Lin. *Foundations of Social Research.* New York: McGraw-Hill, 1976.

[21] S. Marczak, D. Damian, U. Stege, and A. Schröter. Information brokers in requirement-dependency social networks. In *16th IEEE International Requirements Engineering Conference*, 2008.

[22] G. Montagnon. Deliverable 1.4: Design requirements. Technical report, TAS3, 2009.

[23] J. Mülle. Deliverable 3.1: Design of a semantic underpinned, secure and adaptable process management platform. Technical report, TAS3, 2009.

[24] L. Page, S. Brin, R. Motwani, and T. Winograd. The pagerank citation ranking: Bringing order to the web. Technical report, Stanford University, 1998.

[25] J.-C. Pazzaglia. Deliverable 1.1: State of the art. Technical report, TAS3, 2008.

[26] J. Robertson and S. Robertson. Volere requirements specification template. Edition 14, Atlantic Systems Guild, 2009.

[27] A. D. Toro, B. B. Jiménez, A. R. Cortés, and M. T. Bonilla. A requirements elicitation approach based in templates and patterns. In *Workshop Engineering Requirements (WER'99)*, 1999.

[28] T. Valente and R. Foreman. Integration and radiality: Measuring the extent of an individualís connectedness and reachability in a network. *Social Networks*, 20(89):105, 1998.

[29] A. Yamamoto, D. Asahara, T. Itao, S. Tanaka, and T. Suda. Distributed pagerank: A distributed reputation model for open peer-to-peer networks. In *SAINT-W í04 (SAINT í04 Workshops), Washington, DC, USA*, 2004.

Part II

Deliverable 1.2: Supporting Documents

A Requirements Assessment Templates

A.1 Template 1 for Gap Analysis and Requirements Elaboration

Instruction 1: Describe the objectives of the workpackage (5-10 lines). Those objectives should be consistent with the ones in the Description of Work and the Workpackage Deliverables. Further, they should take the two scenarios above as a point of reference. If it applies, you may specify which part of the scenarios or which properties of the scenarios the activities in your workpackage support.

Instruction 2: Describe solved and unsolved problems in the field of trust and security in service-oriented open and distributed environments in the context of the Workpackage. Include literature about existing research and/or software addressing the objectives described in Instruction 1 and discuss why such research/implementations are sufficient/not sufficient to address those objectives (2 paragraphs). If you need to refer to details, please feel free to refer to other deliverables.

Instruction 3: Write down the technical, legal and application requirements that apply to the activities in your work package. You may use the requirements that you submitted to the prior Deliverable 1.2. All requirements should be formulated in full sentences using MUST/SHALL for requirements that are mandatory and SHOULD for those that are optional but nice to have. Requirements should define problems that need to be solved and not solutions that need to be adopted (e.g., "Workpackage shall implement separation of duties" is not a requirement) . For each requirement include:

- a short justification for the requirement. You are encouraged to include reference to the application scenarios above.
- how it interacts with other requirements in your work package. You can distinguish between the following:
  - A depends on B: requirement A requires requirement B. B is a condition for A.
  - A supports B: requirement A is needed to fulfill requirement B. A is a condition for B.
  - A implements B: requirement A is a specialization of requirement B.
  - A abstracts B: requirement A is a generalization of requirement B.
  - A is in conflict with B: requirement A and requirement B are logically inconsistent or the implementation of both requirements is not feasible.

You should include interactions among your workpackage requirements as well as the interaction of your requirements with the design requirements defined in Deliverable 1.4 [22].

The numbering of the requirements are as follows:
DeliverableNumber-WorkpackageNumber.RequirementNumber.

Instruction 4: List available solutions which you can use of to fulfill the requirements of your work package. You may use/refer to the list of software you submitted to the prior D1.2 or to the State of the Art in Deliverable 1.1. Provide information using the following template.

Name of Software Package:
Link:
Access: Open Source/Open Standard or proprietary, any limitations
Functionality:
Limitations with respect to TAS3:
Related Requirements: include which requirements can be fulfilled using this software.
For the software or application of your choice, add to the template
Justification for selection:
and please include why you have selected this one over the others.

Instruction 5 Provide a list of the requirements distinguishing between:

- requirements that cannot be fulfilled because necessary research or implementations are missing: Explain shortly how you will be attending to those requirements within the project. If possible, explain how you plan to validate that those requirements are fulfilled.
- requirements that will not be fulfilled because they are beyond the scope of TAS3: please give a convincing justification if this is the case.

A.2 Template 2 for Inter-WP interactions

Please fill in the following table for each of your requirements that have interactions with the requirements of other WPs. Use the list of requirements in Appendix C. We have provided you with a controlled vocabulary to name the interactions. These are defined as follows:

- A depends on B: requirement A requires requirement B. B is a condition for A.
- A supports B: requirement A is needed to fulfill requirement B.
- A implements B: requirement A is a specialization of requirement B.
- A abstracts B: requirement A is a generalization of requirement B.
- A is in conflict with B: requirement A and requirement B are logically inconsistent or the implementation of both requirements is not feasible.
- A is similar to B: A is similar to or overlapping with B.

We have also created a row for any notes you want to make. Please make use of this if you want to explain an interaction in more detail or if somehow you are not sure about the interaction, or you want us to include something about the interaction in the deliverable. And last, we have a field for who will fulfill the requirement. If it is not only your team/work package, but also requires activities by other work packages, please list those work packages here.

At the end of the interaction analysis process you may feel the need to document some new requirements, please feel encouraged to do so. If your interaction analysis generates new requirements, these should be formatted like all the other requirements with a requirement ID number, the requirement itself, justification and interaction.

We are aware that this is a repetitive/iterative work. We expect it to nevertheless be useful and to make visible the interactions between the work packages. Especially we expect it to be helpful in mapping out those interactions between the technical, demonstrator and legal work packages, which all have different emphases and strong interactions. We thank you for your collaboration and look forward to receiving your interaction tables. Please feel free to contact us if you think anything is unclear or if you have any questions or comments.

A.3 Template 3 for Requirements Updates

Step 1: New, edited or deleted requirements and consolidation of similar requirements

Step 1.A **Instructions:** The following are the requirements of your WP listed in D1.2. Please review this list. You may decide to edit, add or delete some of these requirements on this page, by clicking the ”Edit this page” button at the bottom of this page. Here are the instructions on how to do each of these actions:

- *add new requirements:* if you have elaborated any new requirements in the last months relevant to D1.2 (gap analysis and research requirements) please add these to the list below. For any new requirement, please keep the requirements template from D1.2 shown below. All requirements should be formulated in full sentences using MUST/SHALL for requirements that are mandatory and SHOULD for those that are optional but nice to have. Requirements should define problems that need to be solved and not solutions that need to be adopted. For the interactions, please pay attention to the definition of the controlled vocabulary below and only use these relationships to define interactions.

ReqID	**D1.2-1.7** (NEW)
Requirement	The different policies should be machine readable.
Justification	This requirement refined D1.2-1.6
Interaction	implements D1.2-1.6

Here is the controlled vocabulary for interactions:

- *A depends on B:* requirement A requires requirement B. B is a condition for A.
- *A supports B:* requirement A is needed to fulfill requirement B. A is a condition for B.
- *A implements B:* requirement A is a specialization of requirement B.
- *A abstracts B:* requirement A is a generalization of requirement B.

Last, please do not forget to add the (NEW) tag next to the ReqID to indicate that this is a new requirement.

- *edit an existing requirement:* if you need to change the formulation of any of your requirements, please, do so and indicate that you have done so next to the ReqID i.e., D1.2-6.1 (Edited)

ReqID	**D1.2-1.7** (EDITED)
Requirement	The different policies should be machine readable.
Justification	The requirement D1.2-1.7 contained two different requirements, these are now split in D1.2-1.7 and D1.2-1.8.

- *delete a requirement:* if you need to delete a requirement, please indicate that this needs to be so next to the ReqID i.e., D1.2-6.1 (Delete). Please also add a justification for the deletion. Example:

ReqID	**D1.2-1.7** (DELETED)
Requirement	The different policies should be machine readable.
Justification	The requirement D1.2-1.7 contained two different requirements, these are now split in D1.2-1.7 and D1.2-1.8.

Step1.B In the first iteration of D1.2 each partner indicated interactions with the requirements of other WPs. One of the interaction types was of similarity, suggesting that two requirements are similar or overlapping. Please find below the requirements that other WPs have indicated are similar to yours. You can either confirm the similarity and the two requirements will be merged. If you disagree with the similarity relationship then please consider contacting those WPs to better distinguish their difference. Otherwise, please either state why the two requirements must be included although they are similar, change the wording so that the distinction is clear, or suggest a new relationship between the two requirements (supports, depends, implements, or abstracts as defined above).

For example: “D1.2-3.12 is similar to D1.2-4.7 but this is justifiable because D1.2-3.12 articulates the specifics of this requirement which is crucial to business processes” or“the label between D1.2-3.12 and D1.2-4.7 should be changed to a “depends” relationship as this better reflects the relationship between the two requirements”.

For the updates please use the given notation language (.dot) which looks like this:

“Requirement 1” → “Requirement 2” [label = “Type of interaction”]

where Type of Interaction is an element of the controlled vocabulary, which is made up of the following set:

- S : Supports means requirement A is needed to fulfill requirement B. A is a condition for B
- D : Depends means requirement A requires requirement B. B is a condition for A
- A : Abstracts means requirement A is a generalization of requirement B
- I : Implements means requirement A is a specialization of requirement B
- Sim : Similar means A is similar to or overlapping with B.
- C : Conflicts means requirement A and requirement B are logically inconsistent or the implementation of both requirements is not feasible.

Requirements are written in the format of the deliverable D1.2-WP#.Req#.

You can access the graph in the .dot format when you edit this page and add changes to relationship labels directly.

DOCUMENTATION AND JUSTIFICATION OF CHANGES:

Please add your comments here. Indicate for each requirement with similarities, if you agree with the similiarity (in which case the two requirements will be merged), or if you decided to make changes to the wording or label of your requirement. You may also justify why the similarity relationship is not correct. Any changes will also be confirmed with the relevant WPs.

B Updates to Requirements of TAS^3

This section presents the updates to the requirements elaborated by the partners as part of the gap analysis. The requirements are grouped in three: new requirements, changed requirements and deleted requirements. Each requirement has a requirement ID, a justification for the introduction, editing or deletion of the requirement.

B.1 New Requirements of TAS^3

These are the new requirements captured in TAS^3.

ReqID	**D1.2-3.14**
Requirement	Business processes MUST be executable in the Trust Network. It is fundamental for all requirements in respect to enforcing security and privacy in business processes.
Justification	It is fundamental for all requirements in respect to enforcing security and privacy in business processes.The requirement had previously been forgotten.
ReqID	**D1.2-5.12**
Requirement	The trust management system SHALL support ranking entities according to trustworthiness score.
Justification	Ranking providers according to trustworthiness will be convenient for a user choosing between suitable providers (e.g. as part of the service discovery and selection procedure).
ReqID	**D1.2-7.28**
Requirement	The system must be able to send users summary audits of accesses and attempted accesses to their personal data.
Justification	Gives the user visibility that his/her privacy policy is being enforced correctly.
ReqID	**D1.2-7.29**
Requirement	Users externally assigned roles and attributes should be mapped into internal authorisation attributes.
Justification	Separates authorization attributes from externally assigned attributes and allows external attribute authorities to be replaced. It also separates workflow authorization attributes from organizational roles.
ReqID	**D1.2-8.7**
Requirement	An end user SHALL be able to be in control of her data using a web based dashboard application.
Justification	
ReqID	**D1.2-8.8**
Requirement	All TAS^3 core components SHALL be able to log errors and process informations in an audit service.
Justification	
ReqID	**D1.2-8.9**
Requirement	User SHOULD be able to negotiate the meaning of the vocabulary collaboratively.
Justification	
ReqID	**D1.2-9.17**
Requirement	The system MUST take care of policy combinations and have a mechanism to resolve different policies interacting on data at the same time.
Justification	There will be policy combinations, so the system must be able to handle those.
ReqID	**D1.2-9.18**

Requirement	There SHOULD be provision for journaling of data, showing what data has been changed and who has changed what.
Justification	Track back of data is necessary in case of doubt or indistinctness.
ReqID	**D1.2-9.19**
Requirement	The system SHOULD provide means to guarantee data integrity and authenticity.
Justification	Data should not be changed by the Service Provider and it should be possible to see who the original author is.
ReqID	**D1.2-9.20**
Requirement	There MUST be a provision for confidentiality in data transmission.
Justification	
ReqID	**D1.2-9.21**
Requirement	There MUST be provision for different levels of authentication, authorisation and trust, and to encompass existing mandatory security mechanisms.
Justification	
ReqID	**D1.2-9.22**
Requirement	There MUST be a mechanism to establish trust between service providers.
Justification	
ReqID	**D1.2-9.23**
Requirement	Processes MUST only be able to access specific data they need in order to execute successfully.
Justification	The requirement D1.2-9.1 contained two different requirements, these are now split in D1.2-9.1 and D1.2-9.23.
ReqID	**D1.2-9.24**
Requirement	Service providers MUST act on dynamically set privacy policies with immediate effect.
Justification	The requirement D1.2-9.9 contained two different requirements, these are now split in D1.2-9.9 and D1.2-9.24.
ReqID	**D1.2-9.25**
Requirement	Users MUST be informed about the consequences of their choosen or pre-set policies; they must clearly understand the implications of this policy choice.
Justification	The requirement D1.2-9.6 contained two different requirements, these are now split in D1.2-9.6 and D1.2-9.25.
ReqID	**D1.2-9.26**
Requirement	All users MUST be securely authorised before any access to data is allowed.
Justification	The requirement is split into D1.2-9.4 and D1.2-9.26.
ReqID	**D1.2-9.27**
Requirement	(Final)TAS^3 demonstrators MUST be subject to formal usability testing.
Justification	Usability requirements were moved from WP10 and applied to demonstrators.
ReqID	**D1.2-9.28**
Requirement	Demonstrator usability testing MUST evaluate end user perceptions of trust in the TAS^3 system.
Justification	Usability requirements were moved from WP10 and applied to demonstrators.
ReqID	**D1.2-9.29**
Requirement	Demonstrator usability testing MUST capture and record both user expectations and perceptions of usability of the TAS^3 system.
Justification	Usability requirements were moved from WP10 and applied to demonstrators.

ReqID	**D1.2-10.2.1**
Requirement	The Audit and Monitoring domain of the TAS^3 SHOULD notify authorization failures to the Authorization Infrastructure of TAS^3.
Justification	This requirement is a refinement of D1.2-10.2 Interaction: D1.2-10.2.1
ReqID	**D1.2-10.2.2**
Requirement	The Audit and Monitoring domain of the TAS^3 SHOULD notify authorization failures to the Trust Reputation Infrastructure of TAS^3.
Justification	Justification: This requirement is a refinement of D1.2-10.2
ReqID	**D1.2-10.8.1**
Requirement	Services that are to participate in a TAS^3 choreography MUST be accompanied with models describing their public interface.
Justification	This requirement is a refinement of D1.2-10.8
ReqID	**D1.2-10.8.2**
Requirement	Services that are to participate in a TAS^3 choreography MUST be accompanied with models describing their access policy.
Justification	This requirement is a refinement of D1.2-10.8
ReqID	**D1.2-6.85**
Requirement	Availability: the TAS3 technical authorization infrastructure MUST ensure that legitimate persons shall have ready to access personal data, particularly in emergency situations (e.g., when it is necessary to safeguard the vital interests of the data subject).
Justification	
ReqID	**D1.2-6.85.1**
Requirement	Where a user decides to override the ordinary authorization process under the pretext of an emergency, appropriate notifications and follow-up procedures to deter abuse must be executed.
Justification	
ReqID	**D1.2-6.86**
Requirement	Data minimization : appropriate measures MUST be in place to avoid unnecessary duplication of personal data in multiple repositories.
Justification	
ReqID	**D1.2-6.87**
Requirement	Use of feedback information: Users SHALL have the ability to specify how the feedback they provide with regards to service providers and service experiences may be used (e.g. only for the purpose of calculating reputations)
Justification	
ReqID	**D1.2-6.87.1**
Requirement	The operator of the Trust Reputation server MUST be bound to only process user feedback information in accordance with the users policies.
Justification	
ReqID	**D1.2-6.88**
Requirement	Outsourcing/delegation of responsibilities of TAS3 participants: TAS3 participants MUST be bound to outsource or delegate only those tasks for which outsourcing or delegation is permitted.
Justification	
ReqID	**D1.2-6.88.1**
Requirement	Where a TAS3 participant decides to outsource/delegate a task which involves the processing of personal data, this entity must choose a processor providing sufficient guarantees in terms of technical security measures and organizational measures.
Justification	
ReqID	**D1.2-6.88.2**

Requirement	Any TAS3 participant outsourcing/delegating a task which involves the processing of personal data must ensure that the processing is governed by a contract or legal act binding the processor to the controller which stipulates: (1) that the processor shall act only on instructions from the controller; (2) that the processor is subject to the confidentiality and security obligations set forth by Directive 95/46/EC.
Justification	

B.2 Edited Requirements of TAS^3

These are the requirements which have been edited to better articulate the needs of TAS^3 WPs.

ReqID	**D1.2-3.4**
Requirement	Users MUST have an identifier that stays the same throughout the execution of a business process instance.
Justification	This clarifies what specific properties an identity management must fulfill in order to be used with business processes.
ReqID	**D1.2-3.7**
Requirement	Participants in business processes MUST be able to delegate their responsibilities and permissions in a controlled manner, [added this part:] on a per process-instance level.
Justification	Distinguish it from the general D1.2-7.1 and point out the WP3 specific details.
ReqID	**D1.2-3.9**
Requirement	Business processes SHOULD be able to recover from error situations.
Justification	This is a feature which would be nice to have in particular cases.
ReqID	**D1.2-3.12**
Requirement	Users SHOULD be able to annotate business processes with concepts e.g. from the TAS^3 ontology to achieve semantic interoperability to comply to a common security and privacy vocabulary.
Justification	Clarify the distinction between D1.2-2.23 and this requirement, focus must be on security and privacy.
ReqID	**D1.2-5.10**
Requirement	A user SHALL be able to prove her identity when providing trust feedback.
Justification	The old formulation (The TAS^3 architecture SHALL support user identification.) too general.
ReqID	**D1.2-9.1**
Requirement	Processes MUST have secure access to data drawn from a variety of existing sources.
Justification	The requirement D1.2-9.1 contained two different requirements, these are now split in D1.2-9.1 and D1.2-9.23.
ReqID	**D1.2-9.2**
Requirement	Users MUST be able to set, view, control and change policies for their data (or data objects) at a variety of levels, down to the lowest (field) level, from accepting and assembling clearly-formulated pre-set policies to adding fine-grained policies to specific sets of data (or data objects); they must clearly understand the implications of this policy choice. Any inherent contradictions or inconsistencies SHOULD be pointed out to users before the policy is accepted.
Justification	Extension.
ReqID	**D1.2-9.3**

Requirement	Users MUST have easy, and easily-understood, access to the system, without the need for overly-complex authentication and authorization processes; preferably via SSO and using a familiair interface.
Justification	Refinement.
ReqID	**D1.2-9.4**
Requirement	All users MUST be securely authenticated before any access to data is allowed.
Justification	The requirement is split into D1.2-9.4 and D1.2-9-26.
ReqID	**D1.2-9.5**
Requirement	There MUST be a secure and reliable audit trail showing who accessed user PII, when and for what purpose, and whether any changes were made, and this audit trail must in turn be secure and only accessible by the user, authorised individuals or service providers.
Justification	Refinement.
ReqID	**D1.2-9.6**
Requirement	Users MUST be able to set specific policies for all possible data-requesters from highest level (country/international organisations) down to the lowest level (named actor), including accepting clearly-formulated pre-set policies for common data-requesters.
Justification	The requirement is split into D1.2-9.6 and D1.2-9-25.
ReqID	**D1.2-9.8**
Requirement	Users MUST be able to see who (named actor) has requested access to which of their PII data and whether or not access was granted.
Justification	Refinement.
ReqID	**D1.2-9.9**
Requirement	Users MUST be able to change the policies attached to their PII data at any time.
Justification	The requirement is split into D1.2-9.9 and D1.2-9-24. Interaction: Similar to D1.2-7.7.
ReqID	**D1.2-6.6**
Requirement	Binding Effect of technical processes and policies. All TAS3 participants and users MUST agree to be bound by the technical processes within the TAS3 network, including the obligations resulting from the transactions they engage in or choices they exercise through the TAS3 architecture.
Justification	integration Req 6.5 and 6.6
ReqID	**D1.2-6.6.1**
Requirement	All TAS3 participants and users MUST agree to accept the contents of TAS3 logs as evidence of their actions within the TAS3 network (to the extent the relevant logging mechanisms are working properly and their properties have been appropriately disclosed and consented to).
Justification	
ReqID	**D1.2-6.6.5**
Requirement	Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience , so as to enable all relevant parties to understand their scope of application and which resources (data, services etc.) are governed by which policies
Justification	Req 6.6.5 and 6.6.6
ReqID	**D1.2-6.7**

Requirement	Implementation of Required Policies. Organizational participants in the TAS3 network MUST implement TAS3 defined or compatible policies specified in the contractual framework (e.g. internal privacy and security policies) or as approved during the intake process. See also Req 6.69.
Justification	: reference to Req 6.69 added
ReqID	**D1.2-6.10**
Requirement	Collection, use, and subsequent use, of personal data MUST be with the informed consent of the data subject EXCEPT where mandated by law or through an exception recognized in law.
Justification	: removed finality component from 6.10 already dealt with in 6.15 et seq
ReqID	**D1.2-6.16**
Requirement	Consent Capture for New or Changed Use: If an entity wishes to process personal data in a manner which cannot objectively be considered as compatible with the originally specified purpose(s), a new informed consent MUST obtained from the data subject prior to this new or changed use, unless this processing is explicitly required or permitted by law.
Justification	integration 6.12 and 6.16
ReqID	**D1.2-6.18.2**
Requirement	The data recipient MUST be legally bound to restrict itself to authorized usage and to execute the obligations specified in these data handling policies (see also Reqs 6.5-6.6).
Justification	typo: specified was mentioned twice
ReqID	**D1.2-6.23**
Requirement	Response to attribute requests and granular access control: Technical policy enforcement mechanisms MUST have the ability to respond to data requests with only that information that the requesting entity needs to receive in order to achieve the purposes of the processing. See also Req 6.37.
Justification	modified is authorized -¿ needs + added to receive in order to achieve the purposes of the processing
ReqID	**D1.2-6.24.1**
Requirement	Mechanisms SHALL be in place to enable the user to choose which identity providers and/or attribute authorities shall be used for a particular service, subject to applicable policy (e.g. minimum level of assurance, prerequisite attributes for authorization decision etc.).
Justification	
ReqID	**D1.2-6.28.2**
Requirement	In the event of indirect collection, the accuracy of the data SHOULD be verified with the data subject where this is both possible and appropriate.
Justification	removed prior
ReqID	**D1.2-6.37.1**
Requirement	A list and directory of resources (e.g. applications, data) and categories of potential users/data recipients MUST be made.
Justification	inserted categories of
ReqID	**D1.2-6.39**
Requirement	Avoid unnecessary linkability. TAS3 SHALL support advanced pseudonym management to limit the level of linkability or correlation among personal data to that which is necessary.
Justification	appropriate -¿ to that which is necessary
ReqID	**D1.2-6.57**

Requirement	A (back-office) procedure SHOULD be in place to adequately deal with the situation whereby a TAS3 actor receives a data subject request which is not competent to decide itself.
Justification	

B.3 Deleted Requirements of TAS^3

This is the list of requirements that have been removed from TAS^3 due to overlaps, re-focusing of scope, or change of responsible workpackages.

ReqID	**D1.2-9.7**
Requirement	Users MUST be able to check (read) their personal data stored in all possible data stores connected to the TAS^3 infrastructure and contest any that they feel is inaccurate.
Justification	This is not part of TAS^3, its more about the contractual arrangement between the user and the service provider, or part of the national legal framework. The data stores are not part of the TAS^3 architecture.
ReqID	**D1.2-9.11**
Requirement	Interoperability between different systems MUST be established to exchange and share data. This includes interoperability between credential providers.
Justification	D1.2-2.23 says that the TAS^3 architecture must facilitate interoperability.
ReqID	**D1.2-9.13**
Requirement	Actors (data-requesters, service providers) MUST be able to connect to the TAS^3 infrastructure in a secure way, using varying levels of authentication and trust.
Justification	Replaced by D1.2-9.21
ReqID	**D1.2-9.15**
Requirement	TAS^3 specific processes SHOULD not adversely affect performance or add complications to existing processes from the users viewpoint.
Justification	This is a requirement for an operational system.
ReqID	**D1.2-10.4**
Requirement	Demonstrators SHALL provide good levels of end-user perceived trust.
Justification	This requirement was introduced by UNIZAR. After the revision of the DOW, UNIZAR already completed their effort in WP10. Probably someother WPs is currently dealing with this aspect.
ReqID	**D1.2-10.5**
Requirement	Demonstrators SHALL provide good levels of end-user perceived usability.
Justification	This requirement was introduced by UNIZAR. After the revision of the DOW, UNIZAR already completed their effort in WP10. Probably someother WPs is currently dealing with this aspect.
ReqID	**D1.2-10.6**
Requirement	Demonstrators SHALL provide good levels of end-user perceived usability.
Justification	This requirement was introduced by UNIZAR. After the revision of the DOW, UNIZAR already completed their effort in WP10. Probably someother WPs is currently dealing with this aspect.
ReqID	**D1.2-10.7**
Requirement	Demonstrators SHALL provide good levels of accessibility.

Justification	This requirement was introduced by UNIZAR. After the revision of the DOW, UNIZAR already completed their effort in WP10. Probably someother WPs is currently dealing with this aspect.
ReqID	**D1.2-6.5**
Requirement	Agreement to be bound. All parties MUST agree to be bound to the obligations they take on both by becoming and being part of the TAS3 network, as well as those which are the result of transactions or choices they exercise through the TAS3 Architecture.
Justification	integration Req 6.5 and 6.6
ReqID	**D1.2-6.6.6**
Requirement	The policies SHALL be drafted in a way which enables all parties to understand their scope of application and which resources (data, services etc.) are governed by which policies.
Justification	integration Req 6.6.5 and 6.6.6
ReqID	**D1.2-6.12**
Requirement	Consent Capture for New or Changed Use: If the use of information changes or if there is a new use of information there MUST be a new informed consent obtained prior to the new or changed use of information. (see also Req 6.16)
Justification	integration 6.12 and 6.16
ReqID	**D1.2-6.37.8**
Requirement	Adequate measures and procedures MUST be in place to support enforcement of authorization policies at both central and local levels.
Justification	depends on model of implementation

C Requirements of TAS^3

This section presents the requirements elaborated by the partners as part of the gap analysis. The requirements are grouped with respect to the work packages that elaborated them. Meaning, the requirement is important for the partners in that given work package, but they may depend on other work packages for the fulfillment of the requirements. Each requirement has a requirement ID, a justification for the introduction of the requirement and an analysis of the interactions of the requirements with other requirements in that given WP.

C.1 General Requirements of TAS^3

These are requirements that follow from the objectives of TAS^3 and have been provided by WP2.

ReqID	**D1.2-2.1**
Requirement	TAS^3 Architecture MUST be feasible to implement
ReqID	**D1.2-2.2**
Requirement	TAS^3 Architecture MUST be feasible to deploy
ReqID	**D1.2-2.3**
Requirement	TAS^3 Architecture MUST support plurality of service business models
ReqID	**D1.2-2.4**
Requirement	TAS^3 Architecture MUST support multiple software suppliers
ReqID	**D1.2-2.5**
Requirement	TAS^3 Architecture MUST be platform independent
ReqID	**D1.2-2.6**
Requirement	TAS^3 Architecture MUST be programming language agnostic
ReqID	**D1.2-2.7**
Requirement	TAS^3 Architecture MUST be fail safe, i.e. failure should not lead to security breach
ReqID	**D1.2-2.8**
Requirement	TAS^3 Architecture MUST be available
ReqID	**D1.2-2.9**
Requirement	Implementation MUST correctly implement TAS^3 Architecture
ReqID	**D1.2-2.10**
Requirement	TAS^3 MUST appear to the users to work correctly
ReqID	**D1.2-2.11**
Requirement	The functionality of TAS^3 must be transparent to the users (user can see what is going on)
ReqID	**D1.2-2.12**
Requirement	TAS^3 MUST be comprehensible to the user. The user MUST be able to understand what has happened, what should have happened, and what will happen.
ReqID	**D1.2-2.13**
Requirement	TAS^3 MUST be easy to use
ReqID	**D1.2-2.14**
Requirement	TAS^3 MUST appear to the user to be privacy protective
ReqID	**D1.2-2.15**
Requirement	TAS^3 MUST make it possible to hold people and companies accountable for the activities with respect to personal data

C.2 Requirements of WP2

ReqID	D1.2-2.16
Requirement	TAS^3 MUST mitigate risks or prevent risks to the trust and security of the architecture.
Justification	
Interaction	
ReqID	D1.2-2.17
Requirement	TAS^3 MUST provide an untamperable audit trail
Justification	
Interaction	
ReqID	D1.2-2.18
Requirement	Authentication in TAS^3 MUST be credible
Justification	
Interaction	
ReqID	D1.2-2.19
Requirement	Authorization in TAS^3 MUST be credible
Justification	
Interaction	
ReqID	D1.2-2.20
Requirement	TAS^3 MUST guarantee only authorized disclosures and actions
Justification	
Interaction	
ReqID	D1.2-2.21
Requirement	TAS^3 MUST implement data protection legislation in technology.
Justification	
Interaction	
ReqID	D1.2-2.22
Requirement	TAS^3 MUST permit access to the audits for legitimate authorities if this is legally necessary.
Justification	
Interaction	
ReqID	D1.2-2.23
Requirement	Semantic interoperability should be achieved across web services and business processes.
Justification	Web services and business processes need to comply to specific security and privacy protocol and provide a measure of trustworthiness to allow communication across the TAS^3 architecture.
Interaction	D1.2-R3.12, D1.2-R3.14

C.3 Requirements of WP3

ReqID	D1.2-3.1
Requirement	Process designers SHOULD be given tools to define (graphical) models of their business processes including the interactions of the process with external components, i.e. web services and human activities (web interfaces), and other business processes.
Justification	It is not feasible to define a business process model without tool support, as processes can get quite complex. This especially holds as several aspects have to be included into the model, such as interfaces, services, trust and security.
Interaction	*Abstracts* D1.2-3.6
ReqID	D1.2-3.2

Requirement	Service providers MUST be able to automatically translate their security-aware process models into an executable form and into security parameters configuring some parts of the trust and security infrastructure.
Justification	Having (graphical) process models just as documentation that then must be implemented (again) manually is insufficient, as there is no guarantee that the model, and especially the security settings, is implemented faithfully.
Interaction	*Depends on* D1.2-3.1
ReqID	**D1.2-3.3**
Requirement	Users MUST have an interface where they can see their present tasks in business processes and the present status of the processes they are currently involved.
Justification	Business processes involve humans like a job seeker who must have a user interface to interact with the process, e.g., to provide his/her portfolio.
Interaction	
ReqID	**D1.2-3.4**
Requirement	Users MUST have an identity in the business process that is compliant with their identity at other service providers.
Justification	Business processes process, inter alia, PII. Such PII (like a diploma) is retrieved from other service providers (like an authentic data source) and possibly sent for processing to other providers (e.g. to check and amend it).
Interaction	*Support* D1.2-3.3. *Abstracts* D1.4-3.1
ReqID	**D1.2-3.5**
Requirement	Process designers MUST be able to specify the assignment of tasks to actors in a business process in a sufficiently abstract, flexible and secure way, using roles for grouping tasks and responsibilities.
Justification	Employees and their responsibilities can change often and quickly, thus a process model cannot determine the exact individuals responsible in advance. Thus, specifications must allow for flexibility but without loss of security. In a business process, several people cooperate to achieve a common business goal. For example, the Kenteq APL process (see D3.1) detailing the assessor Kenteq in the first scenario above involves, i.e., coach, assessor and quality controller. Their responsibilities and the activities they have to perform for each person category are the same regardless of who actually performs the function. Thus, they can best be described using roles.
Interaction	*Abstracts* D1.2-3.6. *Supports* D1.2-3.9. *Abstracts* D1.4-3.2.
ReqID	**D1.2-3.6**
Requirement	Business process providers (in general: coordinators of a complex service) MUST be able to control who performs a task, by binding authorization to perform a task and access necessary resources to roles.
Justification	Control of who performs a task is critical for achieving the objective of a business process and to keep PII secure. An example for a task (taken from the Kenteq APL process) is to view the competency profile of the candidate (PII) and make an approval decision based on that. Specifying authorisation for each task and each access permission is a tedious and error-prone task. It is often clear in advance what kind of data is involved in the business process (e.g., the personal competency profile of the candidate) and who must be able to access it (e.g., the coach and the assessor), so authorizations can often be bound to a role by a manual decision or a defined policy.

Interaction	*Implements* D1.2-3.1, D1.2-3.5. *Supports* D1.2-3.9. *Abstracts* D1.4-3.3.
ReqID	**D1.2-3.7**
Requirement	Participants in business processes MUST be able to delegate their responsibilities and permissions in a controlled manner.
Justification	When participants are unavailable or overloaded with work, it must be possible for the business process to proceed towards its objective but with appropriate control because responsibilities and permissions are transferred.
Interaction	*Supports* D1.2-3.6. *Similar to* D1.4-3.4.
ReqID	**D1.2-3.8**
Requirement	Process designers MUST be able to specify mutual exclusion between roles in the scope of a process.
Justification	Some responsibilities within a business process are incompatible in the sense that they may not be performed by the same person, otherwise security would be compromised. This especially concerns situations where the holder of one role supervises the decisions of that of the other one. E.g., the assessor approves a profile the candidate has created with assistance from the coach
Interaction	*Implements* D1.2-3.6. *Supports* D1.2-3.9. *Similar to* D1.4-3.5.
ReqID	**D1.2-3.9**
Requirement	Business processes MUST be able to recover from error situations.
Justification	It is not always completely foreseeable if resources are accessible at runtime. However, a fault might be recoverable, e.g. by repeating the request after initiating a break-the-glass procedure, requesting necessary permissions to be granted or choosing another source. A recoverable fault should not cause termination of the business process.
Interaction	*Similar to* D1.4-3.10.
ReqID	**D1.2-3.10**
Requirement	Permissions SHOULD only be valid when needed.
Justification	Roles imply access permissions to resources connected with the business process. However, they are not necessarily needed for the whole duration of the process. To prevent abuse, they should not be usable when not needed.
Interaction	*Implements* D1.2-3.6, D1.4-3.3.
ReqID	**D1.2-3.11**
Requirement	Users MUST be able to specify on which of their PII the process should have access, and service providers MUST be able to discover for a particular piece of PII which user settings apply and whether the PII is particularly sensitive
Justification	Each business process has distinct needs about the data to process. The user must be able to see these requirements in advance, together with a privacy policy. Further, in the employability domain, portfolios can contain sensitive data, for example medical data or criminal records. For instance, the personal competency profile of an APL candidate might contain a medical report about health-related restrictions of the candidate. Kenteq must be able to detect this in order to act appropriately, e.g., by assing specially qualified employees to deal with the case.
Interaction	*Supports* D1.2-3.9. *Abstracts* D1.4-3.6. *Depends on* D1.4-3.9.
ReqID	**D1.2-3.12**
Requirement	Business processes MUST be able to receive sufficient (semantically interoperable) information about services, also business processes, available from other service providers. Especially, they MUST be able to inspect the privacy policy.

Justification	Service providers will outsource parts of their business process to other service providers. To be able to do so, they must have sufficient information about the available processes (interfaces, assumptions, i.e. pre- and postconditions and effects, interaction behaviour, non-functional properties).
Interaction	*Implements Depends on* D1.2-3.11
ReqID	**D1.2-3.13**
Requirement	Business processes SHALL adapt the specified flow to the specific context of the running process (instance) by replacing a subprocess, a used service, data or even change the defined flow.
Justification	Process flows are not always modelled in a fixed manner, sometimes it is not possible to foresee all possible alternative flows, that may occur. E.g., depending on the candidate the process to perform the assessment or to choose an adequate coach may differ from the predefined way in the modelled business process. Another example is that the change of data that will result from calling a subprocess or web service must be handled by adapting the process in that part, that processes that data. In these cases an adaptation of the process during it is running is needed.
Interaction	*Depends on* D1.2-3.12
ReqID	**D1.2-3.14**
Requirement	Choosing an adequate service provider, privacy policies for processes MUST be available, and they must be semantically interoperable, otherwise automatic comparison is not possible at all, and manual comparison is more difficult than necessary, as well.
Justification	Users expect to know as early as possible what PII they need to provide so that a particular business process can complete successfully, or, the other way round, if the process can complete successfully with the PII they are willing to contribute.
Interaction	*Supports* D1.2-3.11
ReqID	**D1.2-3.15**
Requirement	Adaption of a process must result in a process with guaranteeing the same quality level of security.
Justification	The running process follows an agreement of the process participants, e.g. the candidate and the assessor, which security policy has to be observed. The change of the process must result in a process which at least allows following the same security policy.
Interaction	*Implements* D1.2-3.13 *Depends on* D1.2-3.12

C.4 Requirements of WP4

ReqID	**D1.2-4.1**
Requirement	TAS^3 MUST be able to enforce user-centric policies on information gathered from data subjects and on aggregated information sets.

Justification	Information on users and data subjects consists of multiple sets of electronic personal identifying information that are stored at authoritative repositories to avoid multiple, possibly conflicting, copies of at least some information. Each set is of varying size and complexity, and is held in different digital formats. Different subsets of this information have different sensitivity levels. Some of these subsets may be considered publicly accessible information (e.g., postal address, telephone number), some of it the user may be willing to share with a wide range of people (e.g., degree classification or other awards), other of it will be highly confidential with the users only wishing to share it with close associates (e.g., career plans), whilst yet other of it may have strict legal restrictions on who may view the information and under what conditions (e.g., sexual preference). One set of such information may refer to another set of information, and users (human and other) need to be able to determine whether their data/information has been processed by actors in a manner that is compatible with the policies they agreed on while the data/information was collected. This requirement guarantees compliance with data protection legislation such that personal information is handled appropriately by the recipients, subjects and holders of the personal information.
Interaction	*Depends on* D1.2-4.4, D1.2-4.8, D1.2-4.9
ReqID	**D1.2-4.2**
Requirement	Distinct transactions or executions of a business process that takes place in the TAS^3 environment MUST be indistinguishable from one another.
Justification	An outside observer should not be able to determine whether two distinct runs of a transaction or business process relate to the same entity. Note that subsets of personally identifying information are likely to be identified in different repositories with different unique but unrelated identifiers. If such information includes, e.g., national identification numbers, the transactions dealing with this information may be indistinguishable, but the information itself not.
Interaction	*Supports* D1.2-4.4
hline **ReqID**	**D1.2-4.3**
Requirement	It MUST be possible to demonstrate the complex security and trust features of the TAS^3 functionality and concepts in a comprehensible way for lay users.
Justification	Because the concepts the project is about are rather complex, and a visual tool is the best/simplest way to convey the message to the lay user.
Interaction	*Depends on* D1.2-4.1, D1.2-4.2, D1.2-4.4, D1.2-4.7, D1.2-4.8, D1.2-4.9, *Supports* D1.2-4.5
hline **ReqID**	**D1.2-4.4**
Requirement	TAS^3 service providers MUST be able to prove that they processed the information and services in accordance to the required policies. The proof MUST be usable in court.
Justification	This is necessary to comply with basic data protection requirements with respect to oversight and with the End-to-End trustworthiness of the TAS^3 system. Any service provider or consumer must be able to prove who processed data, for what purpose, etc. This is especially necessary for gateways between TAS^3 service providers and legacy repositories when dealing with information held in legacy databases.
Interaction	*Depends on* D1.2-4.2, D1.2-4.5, D1.2-4.6, D1.2-4.7, D1.2-4.8, D1.2-4.9,
hline **ReqID**	**D1.2-4.5**

Requirement	Each TAS^3 actor (i.e., service provider or service consumer) MUST process the information in compliance with the appropriate policies.
Justification	This is necessary to implement the proportionality and finality principles of data protection regulation. The data subject, service providers and service consumers may extend and narrow down information and policies while exchanging information during the execution of a business process.
Interaction	*Depends on* D1.2-4.1, D1.2-4.2, D1.2-4.6, D1.2-4.7, D1.2-4.8, D1.2-4.9
hline **ReqID**	**D1.2-4.6**
Requirement	In exceptional situations, an identified TAS^3 actor needs to be granted access to information to which access would be denied under normal circumstances. Such functionality MUST be offered by TAS^3.
Justification	This is due to liability issues when dealing with life-and-death matters: one would not like to be held liable if some important information was not available or accessible because of technical matters. If data is needed to deal with life threatening issues, it should be made available to (properly identifiable) actors.
Interaction	*Depends on* D1.2-4.1
ReqID	**D1.2-4.7**
Requirement	TAS^3 service consumers MUST be able to discover service providers that commit to meeting their requirements and policies.
Justification	Service consumers are not able to know beforehand which service providers exist, and whether the existing ones can meet the consumers expectations with respect to the policies and functionality they can provide.
Interaction	*Depends on* D1.2-4.8, D1.2-4.9, *Supports* D1.2-4.1
ReqID	**D1.2-4.8**
Requirement	TAS^3 discovery service and policy management system MUST be user friendly and easy to configure and use.
Justification	The TAS^3 system needs to be usable by non-expert users.
Interaction	*Depends on* D1.2-4.9 *Supports* D1.2-4.3
ReqID	**D1.2-4.9**
Requirement	TAS^3 discovery service MUST take into account the trust and reputation score of both service consumers and providers.
Justification	Because the TAS^3 system needs to select service providers that comply with the relevant policies. These policies may specify certain trust and reputation requirements.
Interaction	*Supports* D1.2-4.1

C.5 Requirements of WP5

ReqID	**D1.2-5.1**
Requirement	The trust management system SHALL answer trust policy evaluation requests which can use different sources of trust.
Justification	Users' trust (see e.g. step 5 of the APL scenario) depends on different sources, such as credentials, reputations or economical information. The trust management system must support combinations of such sources of trust to capture the users trust requirements.
Interaction	*Depends* on D1.2-5.2 which provides the policy language to be used. *Abstracts* D1.4-5.2, D1.4-5.4(b), D1.4-5.7, D1.4-5.8, D1.4-5.9 *Implements* D1.4-5.1
ReqID	**D1.2-5.2**

Requirement	The trust management system SHALL define a combined trust policy language that allows user to formulate trust policies based on credentials, reputations and economical information.
Justification	The reason why an entity trusts another entity can be the role an entity plays, e.g. a certified doctor and/or the past performance of the entity in a given task or with respect to some economical parameters. The trust management system needs to support these different sources of trust in its policies.
Interaction	*Supports* D1.2-5.1, D1.4-5.1(a,b)
ReqID	**D1.2-5.3**
Requirement	The trust management system SHALL provide a reputation based trust management service.
Justification	To evaluate the trustworthiness of entities of services based on reputations which are built from (user) feedback.
Interaction	*Supports* D1.2-5.1, D1.4-5.4, D1.4-5.1(a,b) *Depends* on D1.2-5.2
ReqID	**D1.2-5.4**
Requirement	The trust management system SHALL support the gathering of reputation feedback information.
Justification	Feedback on performance (see e.g. step 8 in the APL scenario) provides the data on which reputations are built. It needs to be collected, stored and made available to the reputation based trust service.
Interaction	*Implements* D1.4-5.4(c) *Supports* D1.2-5.3, D1.4-5.4(d,e) *Depends* on D1.2-5.5
ReqID	**D1.2-5.5**
Requirement	The application business process SHOULD provide a trust feedback opportunity.
Justification	Reputations of entities and services are based on the feedback provided by users. The application business process should ensure the user is provided with an opportunity to give this feedback at relevant points in the process.
Interaction	*Implements* D1.4-5.4(d,e) *Depends* on D1.2-5.4, D1.2-5.10 *Supports* D1.2-5.3
ReqID	**D1.2-5.6**
Requirement	The trust management system SHALL provide a credential based trust management service.
Justification	To evaluate the trustworthiness of entities of services based on their credentials. The credentials determine the role an entity placed and thus in which setting they are trusted.
Interaction	*Supports* D1.2-5.1, D1.4-5.1(a,b) *Implements* D1.4-5.1(c-e)
ReqID	**D1.2-5.7**
Requirement	The trust management system SHALL provide a key performance indicator based trust management service.
Justification	Key performance factors capture (business) performance on specific aspects such as delivery times, etc. Indicators which combine several factors provide valuable economical information about an entity which can be used as a source of trust.
Interaction	*Supports* D1.2-5.1 *Implements* D1.4-5.3
ReqID	**D1.2-5.8**
Requirement	The trust management system SHOULD be extendable with novel trust metrics.

Justification	As users trust requirements may evolve or be different in new settings the trust management system should be flexible enough to support new sources of trust. This includes new metrics for existing services but also support for new trust services.
Interaction	*Depends* on D1.2-5.1 *Supports* D1.4-5.1
ReqID	**D1.2-5.9**
Requirement	The trust management system SHALL provide trust policy formulation support.
Justification	The flexibility of the trust policies can make it difficult for the user to write policies. To aid the user in formulating policies we plan to provide a policy wizard.
Interaction	*Supports* D1.4-5.1(a-e)
ReqID	**D1.2-5.10**
Requirement	The TAS^3 architecture SHALL support user identification.
Justification	Links requesters, recommendations and feedback etc. to names (e.g., in policies). Needed to ensure authenticity of feedback and recommendations.
Interaction	*Supports* all trust policy related requirements
ReqID	**D1.2-5.11**
Requirement	The legal/contractual framework SHALL support feedback data use policies.
Justification	Data on which trust is based may itself be sensitive. Technical protection is provided for some data such as credentials through trust negotiation. Protection of other data, such as feedback on performance, needs to be supported by contract/policy which specifies the allowed usage of the (feedback) data. Such contracts should conform to new legislation in Europe that is being composed on scoring algorithms.
Interaction	*Supports* D1.2-5.4

C.6 Requirements of WP6

ReqID	**D1.2-6.1**
Requirement	Intake Process (Person). The intake process MUST include: documentation, validation of identity and a technical user interface.
Justification	We need to enroll people into the system.
Interaction	The Intake process reviews the execution of contracts, compliance ability and infratructure requirements. To that end the intake process both supports and is informed by all the other requirements (it provides the evolution of the policies, practices contract and ability to comply of a prospective service provider.)
ReqID	**D1.2-6.2**
Requirement	Intake Process (organization). The intake process MUST include: documentation; validation of identity; verification of policies, contracts and the capacity to comply as well as a technical user interface.
Justification	We need to enroll organizations into the system and review their infrastructure and compliance capacity
Interaction	The Intake process reviews the execution of contracts, compliance ability and infratructure requirements. To that end the intake process both supports and is informed by all the other requirements (it provides the evolution of the policies, practices contract and ability to comply of a prospective service provider.)

ReqID	D1.2-6.3
Requirement	Notice: When information is collected, it MUST be specified: what information is collected, how it is collected, who it might be shared with, how it will be used and how it will be managed.
Justification	Required by the Directive.
Interaction	Notice encompasses all foreseeable uses and sharing. In many ways it is dependent on all the following topics and they are dependent on it. All requirements *depend on* and *support* D1.2-6.3
ReqID	D1.2-6.4
Requirement	Collection Limitation/Data Minimization: The TAS^3 system and related processes MUST have appropriate limits on personal data collection to what is needed for legitimate, identified and noticed business function. The system must be supplemented by policies that are articulated that limit employee access to information based on business need.
Justification	Required by the Directive
Interaction	This section is informed by notice and use (below) but is also related to security in terms of data minimization. *depends on* and *supports* 6.3 *Depends on* 6.5 *Supports* 6.12
ReqID	D1.2-6.5
Requirement	Purpose specification. The purpose(s) for collection MUST be clearly specified. The collection related to those purposes must be relevant and non-excessive.
Justification	Required by the directive.
Interaction	This is related/codependent on notice and collection limitation/data minimization. Which means this is relevant to not only those groups that collect information, but also those that use the information, as they must appropriately minimize the data as well as secure it and control access. *Depends on* and *supports* 6.3. *Supports* 6.4
ReqID	D1.2-6.6
Requirement	Consent: Use, and subsequent use, of personal data MUST be compatible with the purposes specified and MUST be with the consent[1] of the data subject.
Justification	Required by the Directive
Interaction	Dependent on notice and purpose specification applies to/requires subsequent consent capture. 6.6 *abstracts* 6.7. *Depends on* and *supports* 6.3 and 6.5.
ReqID	D1.2-6.7
Requirement	Subsequent consent capture: If the use of information changes or if there is a new use of information there MUST be a subsequent capture of information.
Justification	Required by the Directive.
Interaction	Contingent on business model and cross dependent on notice and use. 6.7 *implements* 6.6 *Depends on* and *supports* 6.3 and 6.5.
ReqID	D1.2-6.8
Requirement	Access request process: there MUST be a process to enable users to request access (and possibly amend or correct) to types of information that have been collected and sharing of information. Implicit in this requirement is the need to know where data came from or was sourced.
Justification	Required by the Directive
Interaction	Related to Collection Limitation and Notice. *Depends on* and *support* 6.4 and 6.3

[1] It should be noted that consent often bears important adjectives of clear, unambiguous or explicit. From a technical point of view, this requires that the user opt in to the collection of personal information.

ReqID	D1.2-6.9
Requirement	Compliant capture system: Potential abuses to the system or concerns of either users or organizations MUST be captured.
Justification	Emanates from requirements of the Directive. The directive specifies that a person must be able to complain which is not the same as a specification of a complaint handling system.
Interaction	Should reflect the major elements of these requirements, may also be joined to access mechanism. Has to support all requirements which could be basis of compliant, is also a proof element of 6.1
ReqID	D1.2-6.10
Requirement	Redress/oversight Processes: Once a compliant is captured, redress MUST be possible. Oversight process is a proactive version of this concept.
Justification	Emanates from requirements of the Directive.
Interaction	Interdependent with all of the major elements of these requirements in terms of oversight, specific to breach or harm in terms of redress. This will be defined in legal, but may require a BPM process to be made effective. Audit information in redress is required as a proof element and is essential to oversight. *depends on* all proof element required by 6.1
ReqID	D1.2-6.11
Requirement	Confidentiality. Controllers and processors MUST have duties to maintain confidentiality of information. In some cases this will mean encryption, especially in the UK.
Justification	Required by the Directive.
Interaction	Horizontal requirement that attaches to use, management and storage of data. Everything across the project that touches PII has this requirement including all aspects of legal. It also *supports* D1.2-6.12
ReqID	D1.2-6.12
Requirement	Security. Appropriate security (technical and organizational) measures against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data MUST be in place.
Justification	Required by the Directive.
Interaction	Horizontal across requirements as well as all entities involved in development and operations
ReqID	D1.2-6.13
Requirement	Contract execution. All participants to the TAS^3 system MUST execute the appropriate TAS^3 contract documents.
Justification	Required to enable a contract framework that binds all parties to the use of appropriate technologies and the rights and obligations appertaining to the transactions and uses of information.
Interaction	*Depends on* D1.2-6.14, D1.2-6.15, D1.2-6.16, D1.2-6.17
ReqID	D1.2-6.14
Requirement	Use of TAS^3 Technology and Processes. According to the contract all parties MUST agree to use the appropriate TAS^3 or TAS^3 compatible, technology and processes.
Justification	This is required to assure that all parties can exchange information and engage in transactions in a compatible and secure manner.
Interaction	*Supports* D1.2-6.13
ReqID	D1.2-6.15
Requirement	Implementation of Required Policies. According to the contract organizational participants in the TAS^3 infrastructure MUST implement TAS^3 defined or compatible policies specified in the contract.

Justification	The contract framework is dependent on the need for appropriate polices to support both the technology and the legal obligations set forth in the EU Directive and other applicable laws.
Interaction	*Supports* D1.2-6.13
ReqID	**D1.2-6.16**
Requirement	Agreement to be bound. According to the contract all parties MUST agree to be bound to the obligations they take on both as part of the TAS 3 infrastructure and as a result of transaction or choices exercised through the TAS^3 Architecture.
Justification	In order to give effect to the legal requirements of the Data Protection Directive and other applicable laws, all parties must agree to be bound by both the infrastructure obligations as well as those that arise through use of or transactions over the TAS^3 architecture.
Interaction	*Supports* D1.2-6.13
ReqID	**D1.2-6.17**
Requirement	Binding Effect of technical processes. All parties MUST agree to be bound by the technical processes in the architecture to the extent that they are working properly and have been appropriately disclosed and consented to.
Justification	The TAS^3 architecture provides technical components that enhance trust and facilitate transactions such as sticky polices. The content of the instructions contained in these policies or other technical components and the obligations associated with those instructions must be respected across the TAS^3 architecture.
Interaction	*Supports* D1.2-6.13

C.7 Requirements of WP7

ReqID	**D1.2-7.1**
Requirement	A user sometimes needs to be able to authorise another user or service to act on his behalf.
Justification	A user needs to delegate to a portal to act on his behalf (step 7 of the use case 2 in [22]: Delegation from the user to the portal). A user needs to delegate to his employer to access his eportfolio (step 9 of use case 1 in [22]: The employee authorizes his employer (HR manager) to access the showcase of his ePortfolio)
Interaction	*Depends on* D1.2-7.9 and *implements* D1.2-7.6
ReqID	**D1.2-7.2**
Requirement	Users sometimes need to be able to sign documents using their roles.
Justification	It is a necessary functionality in step 8 of the use case 2 and step 6 of use case 1: Role based signing is required
Interaction	
ReqID	**D1.2-7.3**
Requirement	The user must be able to prove who he is to any service, and also be sure that he is talking to the correct service.
Justification	It is a necessary security need in step 1 of both use cases: Mutual authentication and authorisation.
Interaction	*Supports* D1.2-7.16
ReqID	**D1.2-7.4**
Requirement	A user may need to present several authorisation credentials in order to obtain a service e.g. a credit card and a club membership card
Justification	It is a necessary functionality in step 2 of the use case 2: Attribute aggregation of credentials.

Interaction	This is related to Requirement D1.2-7.5 but orthogonal to it. Whilst D1.2-7.4 is stating that multiple credentials from multiple issuers may be needed, D1.2-7.5 is saying that each credentials should be released incrementally even if they come from the same issuer. Hence, D1.2-7.4 *depends on* D1.2-7.5 and *implements* D1.2-7.6.
ReqID	**D1.2-7.5**
Requirement	Users should only need to provide the minimum of credentials that are needed to obtain a service, and no more.
Justification	It is a necessary condition in step 2 of the use case 2 and step 3 of use case 1: Minimum of credentials in order to Register.
Interaction	This is the user pushing his minimum credentials to a service provider. It is related to requirement D1.2-7.17 as the system may use similar mechanisms to accomplish both requirements. D1.2-7.5 hence *depends on* D1.2-7.17, *supports* D1.2-7.4 and *implements* D1.2-7.6.
ReqID	**D1.2-7.6**
Requirement	Users must have the authorisation to perform any action.
Justification	It is explicit in step 1 of the use case 1 and implicit in most steps.
Interaction	This is a very generic high level requirement and *abstracts* requirements D1.2-7.1, D1.2-7.4, D1.2-7.5, D1.2-7.9, D1.2-7.10, D1.2-7.12, D1.2-7.13, D1.2-7.15, D1.2-7.17, D1.2-7.24.
ReqID	**D1.2-7.7**
Requirement	Users should be able to dynamically set their privacy policies.
Justification	Its in step 2 of the use case 1 Set the user's privacy policy for Personal Identifying Information (PII) and consent to use this PII and step 3 of use case 2.
Interaction	*Depends on* D1.2-7.19 and *supports* D1.2-7.26
ReqID	**D1.2-7.8**
Requirement	Different service providers should not be able to collude together to determine who a pseudonymous user is without the users consent.
Justification	Service providers could jointly profile the user. Related to step 4 of use case 1.
Interaction	May conflict with Requirement D1.2-7.18.
ReqID	**D1.2-7.9**
Requirement	Credentials should be revocable.
Justification	If a user delegates his credential to another person or process he must be able to revoke this delegation if either the delegate abuses its privileges or the user changes his mind.
Interaction	*Supports* D1.2-7.1 and D1.2-7.14 and *implements* D1.2-7.6
ReqID	**D1.2-7.10**
Requirement	Credentials should be targetable to a specific relying party.
Justification	A credential owner does not wish a credential receiver to use the credential on his behalf. It is related to step 4 in use case 1.
Interaction	*implements* D1.2-7.6
ReqID	**D1.2-7.11**
Requirement	The system must support the merging and enforcement of multiple policies.
Justification	It is in step 5 of use case 1.
Interaction	
ReqID	**D1.2-7.12**
Requirement	The system must be able to pull additional user credentials on demand/as required.
Justification	It is in step 6 and 7 of use case 1.
Interaction	Depends upon D1.2-7.13. *Supports* D1.2-7.15
ReqID	**D1.2-7.13**

Requirement	The system must be able to determine where to pull additional credentials from.
Justification	It is in step 6 of use case 1.
Interaction	*Supports* D1.2-7.12. and *implements* D1.2-7.6
ReqID	**D1.2-7.14**
Requirement	One service provider should be able to subcontract (delegate) to another service provider to get work done on behalf of the original user.
Justification	Another instance of delegation of authority, this time service to service.
Interaction	This is similar to D1.2-7.1 only it is system to system rather than person to person. It may depend on D1.2-7.9
ReqID	**D1.2-7.15**
Requirement	Users should be able to push their credentials to the system dynamically when more are needed.
Justification	Step 3 of use case 2: Consent to collect additional PII or ask user to provide it.
Interaction	*Supports* D1.2-7.12. The authorisation system should be able to pull user credentials and accept pushed user credentials and these may need to be supplemented at any time with additional user credentials.emphimplements D1.2-7.6.
ReqID	**D1.2-7.16**
Requirement	User should be able to use different pseudonyms in order to protect their privacy.
Justification	Step 3 of use case 2: User must be able to act with different personas with different vacancy profiles.
Interaction	May depend on D1.2-7.3
ReqID	**D1.2-7.17**
Requirement	Credentials should be incrementally released as trust is established.
Justification	Step 4 of use case 2: Find possible Service Providers that provide the right sort of jobs via the portal. Find out which are trustworthy. Neither party must reveal too much information about themselves.
Interaction	May use similar mechanisms to D1.2-7.5 as this requirement requires both the user and the remote service provider to push the minimum of their credentials to the other party. It *implements* D1.2-7.6.
ReqID	**D1.2-7.18**
Requirement	A service provider should not be able to link together the sequential requests of a user without the users consent.
Justification	Services should not be able to profile users without their consent.
Interaction	may conflict with D1.2-7.8
ReqID	**D1.2-7.19**
Requirement	Service providers should be able to update their policies dynamically without having to bring down the system.
Justification	Service providers often need to be able to provide 24/24 provision of service and bringing the system down to change the policy is not fast enough or pro-active enough.
Interaction	*Supports* D1.2-7.7 in that a user policy may be one of the SPs policies so D1.2-7.19 must be met before D1.2-7.7 can be fulfilled.
ReqID	**D1.2-7.20**
Requirement	Service providers should be able to distribute policy administration between multiple administrators.
Justification	Different administrators have different skills and knowledge and therefore are more competent to set particular polices. Furthermore, it can be too big a job for anyone person to do.

Interaction	Could support Requirement D1.2-7.2 by having role based signing of policies.
ReqID	**D1.2-7.21**
Requirement	The system needs to be resilient to fraud or mistakes by users and administrators.
Justification	Organisations have a legal duty of care to prevent fraud.
Interaction	
ReqID	**D1.2-7.22**
Requirement	The authorisation system needs to have an escape mechanism in emergencies (so called break the glass policies).
Justification	For example, when a patient is taken unconscious to an emergency department and has not authorised the doctor on duty to access his personal health records, the doctor may need to get access to this, regardless of the patients policy.
Interaction	*Depends on* D1.2-7.23
ReqID	**D1.2-7.23**
Requirement	The authorisation system needs to be able to make decisions based on the current state of the application and/or system.
Justification	Systems are naturally dynamic and authorisation systems need to be able to cater for this.
Interaction	*Supports* D1.2-7.22
ReqID	**D1.2-7.24**
Requirement	The authorisation system should securely record/audit the decisions that have been made in a tamperproof and confidential manner.
Justification	Auditors and criminal investigators may need access to these events post-facto, and they need to be assured that the logs have not been tampered with.
Interaction	*Supports* D1.2-7.25, *implements* D1.2-7.6
ReqID	**D1.2-7.25**
Requirement	Auditing needs to be dynamic and adaptive to changes in the system and/or environment.
Justification	If the system detects an attack then the level of auditing should automatically increase.
Interaction	*Depends on* D1.2-7.24
ReqID	**D1.2-7.26**
Requirement	A user must provide consent for the use of his private data and credentials.
Justification	It is part of data protection legislation and in step 2 of the use case.
Interaction	*Depends on* D1.2-7.7
ReqID	**D1.2-7.27**
Requirement	Sensitive tasks must be split between multiple users
Justification	Separation of duties is a well known procedure for ensuring the security and safety of sensitive tasks. It is also required by the business process managers in WP3
Interaction	

C.8 Requirements of WP8

ReqID	**D1.2-8.1**
Requirement	The pilots MUST have a gateway to access the TAS^3 infrastructure.
Justification	Either the requesting applications or the providing or responding applications shall be able to access TAS^3 over a unified interface. By this it is also possible that other applications in the future can be easily integrated into TAS^3.

Interaction	
ReqID	**D1.2-8.2**
Requirement	Legacy databases SHALL be able to provide their data and service to TAS^3.
Justification	TAS^3 shall be open for legacy systems like legacy databases. To provide such an easy way of integration, there must be an interface especially for legacy databases.
Interaction	*Depends* on D1.2-8.1 which specifies the ADPEP.
ReqID	**D1.2-8.3**
Requirement	An end-user SHALL be able to access TAS^3 functionality through a business process.
Justification	Many workflows in organisations use a business process engine to keep track of the workflow or business process. Since TAS^3 legitimized service providers are part of these workflows, they shall be easily integrated into the business process.
Interaction	*Depends* on D1.2-8.1 which specifies the ADPEP.
ReqID	**D1.2-8.4**
Requirement	An end user SHALL be able to access TAS^3 services through a special TAS^3 generic client without having to use a complete Business Process Engine.
Justification	Not in every case the user accesses TAS^3 through a business process engine. Other possible clients are smart phones, web front-end or fat clients. To also support these types of clients, we need a more generic client.
Interaction	*Depends* on D1.2-8.1 which specifies the ADPEP.
ReqID	**D1.2-8.5**
Requirement	An end user SHALL be able to access and manage her/his policies.
Justification	TAS^3 user will get into contact with different layers of policies. Policies may be user centric, organisational or even TAS^3 wide. For user centric policies the user needs a special front-end and back-end to manage her/his policies.
Interaction	*Depends* on D1.2-8.1 which specifies the ADPEP.
ReqID	**D1.2-8.6**
Requirement	An end user SHALL be able to store and modify its data in a repository for person related data. This repository has to be reachable in a TAS^3 secured and trusted way.
Justification	Among other things, TAS^3 is about storing and exchanging person related data in a secure and trusted way. To store such data, we need special TAS^3 adapted repositories.
Interaction	

C.9 Requirements of WP9

ReqID	**D1.2-9.1**
Requirement	Processes MUST have secure access to data drawn from a variety of distributed sources, but only be able to access the data they need.
Justification	This is needed to ensure the efficiency and security of the process, accuracy, and support for data protection requirements
Interaction	
ReqID	**D1.2-9.2**

Requirement	Users MUST be able to set, view, control and change policies for their data at a variety of levels, down to the lowest (field) level, from accepting clearly-formulated pre-set policies to adding fine-grained policies to specific sets of data; they must clearly understand the implications of this policy choice.
Justification	This is needed for the user to exercise control, and to comply with privacy legislation. Users will want the same data to be used in a variety of processes, so may want to add context-specific policies to how it will be used.
Interaction	*Supports* D1.2-9.1, D1.2- 9.4, D1.2-9.6 *Depends on* D1.2-9.3
ReqID	**D1.2-9.3**
Requirement	Users MUST have easy, and easily-understood, access to the system, without the need for overly-complex authentication and authorization processes; preferably via SSO.
Justification	This is necessary to support users support for the system: if it is too complex to access they will not use it unless they have to or will take measures to simplify access that may compromise security (e.g. writing down passwords); however they also have to feel trust in the systems security
Interaction	*Supports* D1.2-9.2, D1.2-9.4, D1.2-9.13
ReqID	**D1.2-9.4**
Requirement	Users MUST be securely authenticated and authorised before any access to data is allowed.
Justification	The system needs to know that only appropriate access is being requested, and users must be matched against the correct sets of data. This complies with legal and ethical requirements and is protection against fraud. There needs to be a provision for different levels of authentication and trust.
Interaction	*Supports* D1.2-9.1, D1.2-9.5 *Depends on*emphAbstracts D1.2-9.3
ReqID	**D1.2-9.5**
Requirement	There MUST be a secure and reliable audit trail showing who accessed user PII, when and for what purpose, and whether any changes were made, and this audit trail must in turn be secure and only accessible by authorised individuals or service providers.
Justification	Necessary for investigation of breaches of security or any official enquiry, especially into breaches of data protection legislation or suspected fraud. This is an administrative tool, rather than the user interface.
Interaction	Depends on D1.2-9.2, D1.2-9.4, *Supports* D1.2-9.8
ReqID	**D1.2-9.6**
Requirement	Users MUST be able to set specific policies for all possible data-requesters from highest level (country) down to the lowest level (named actor), including accepting clearly-formulated pre-set policies for common data-requesters; they must clearly understand the implications of this policy choice.
Justification	This is one of the main objectives and USPs (unique selling points) of TAS^3 for users. This should also allow for combinations of policies and include a mechanism for when different policies are interacting at the same time.
Interaction	*Supports* D1.2-9.2 *Depends on* D1.2-9.3, D1.2-9.4
ReqID	**D1.2-9.7**
Requirement	Users MUST be able to check (read) their personal data stored in all possible data stores connected to the TAS^3 infrastructure and contest any that they feel is inaccurate.
Justification	Users have the legal right to know from the system what data is stored about them and to challenge it if it is incorrect.

Interaction	*Depends on* D1.2-9.1, D1.2-9.3, D1.2-9.5
ReqID	**D1.2-9.8**
Requirement	Users MUST be able to see who has requested access to which of their PII data and whether or not access was granted.
Justification	Users trust in the system depends on this; it is the main reason for them to engage with TAS^3. They also have the legal right to know who has had access to personal data.
Interaction	*Depends on* D1.2-9.5, D1.2-9.4 *Supports* D1.2-9.2
ReqID	**D1.2-9.9**
Requirement	Users MUST be able to change the policies attached to their PII data at any time.
Justification	User requirements and situations may change and the policies for their data may change with them. Evolving legal requirements also make this a necessity. Includes interactive changes such as responses to consent questions.
Interaction	Depends on D1.2-9.2 D1.2-9.6
ReqID	**D1.2-9.10**
Requirement	The policy management user interface MUST meet the highest known current standards (complying with current best practice on interface design, w3c guidelines).
Justification	Policy setting is a complex task and the implications of decisions made should be very clear to the user. The policy interface is the main interface for users and thus the showpiece of TAS^3; most of the rest of the exchanges is performed by back office systems. Users from a variety of different social backgrounds and educational levels should be able to work easily with this interface. To comply with UK SENDA legislation, any user interface must adhere to strict accessibility guidelines.
Interaction	*Supports* D1.2-9.2, D1.2-9.3, D1.2-9.6, D1.2-9.8, D1.2-9.9
ReqID	**D1.2-9.11**
Requirement	Interoperability between different systems MUST be established to exchange and share data. This includes interoperability between credential providers.
Justification	Not all systems used in the pilots use the same standards, formats, tables or fields. As the system will be web-based, we need to ensure that all legacy systems are web-service compliant and build in any necessary interfaces to support interoperability which is not currently in place. Any existing mandatory security mechanisms must be encompassed. Service Providers need to be able to provide data in a form that can be accepted by a Service Requester.
Interaction	*Supports* D1.2-9.1, D1.2-9.3
ReqID	**D1.2-9.12**
Requirement	Persistent and unique electronic means of identification MUST be provided for users/actors of the TAS^3 infrastructure.
Justification	The system must be able to consistently, uniquely and positively identify all users/actors within the TAS? infrastructure to ensure data integrity and correct levels of access permission
Interaction	*Supports* D1.2-9.3, D1.2-9.4, D1.2-9.5
ReqID	**D1.2-9.13**
Requirement	Actors (data-requesters, service providers) MUST be able to connect to the TAS^3 infrastructure in a secure way, using varying levels of authentication and trust.
Justification	This is necessary to provide services access to the TAS^3 infrastructure and preserve confidentiality of data.
Interaction	*Depends on* D1.2-9.1, *Supports* D1.2-9.3

ReqID	D1.2-9.14
Requirement	Back office services must be invisible to the user.
Justification	While users must be able to know and verify how their data has been used, this needs to be done seamlessly; users do not need to see the internal workings of the system
Interaction	*Supports* D1.2-9.3, *Depends on* D1.2-9.11
ReqID	D1.2-9.15
Requirement	TAS^3 specific processes must not adversely affect performance or add complications to existing processes from the users viewpoint
Justification	For users the overall process must remain smooth; speed and performance must not be impaired by the trust and security processes. If additional complications and extra steps are added, users are likely to bypass or ignore them.
Interaction	*Supports* D1.2-9.3, D1.2-9.14
ReqID	D1.2-9.16
Requirement	Data within the ecosystem SHOULD not be copied or duplicated: it should be stored once, used many times.
Justification	Copying data leads to version control issues, issues with deletion and issues with auditing and journaling.
Interaction	*Depends on* D1.2-9.1

C.10 Requirements of WP10

ReqID	D1.2-10.1
Requirement	The TAS^3 architecture MUST support perpetual (i.e. event-driven, periodical) and automated compliance testing of services.
Justification	Service-oriented applications are characterized by great dynamism, e.g., service implementations and service bindings may change at runtime. In the reference scenarios, the services (instances) that participate in the interaction may change independently and without interrupting the service provision (e.g. a new implementation of a functionality can be deployed; the quality of the new implementation needs to be assessed dynamically). Testing strategies that are based only on offline techniques are therefore inadequate and in fact implementing run-time checking mechanism is generally recognized a best practice in service-oriented settings.
Interaction	*Depends* on D1.2-10.8, in that continuous automatic testing requires precise models to be available for each service involved in a choreography.
ReqID	D1.2-10.2
Requirement	The TAS^3 infrastructure SHALL detect service failures in granting or denying access to resources with respect to their manifested policies.
Justification	This kind of failures is especially critical as the trustworthiness of TAS^3 heavily depends on proper handling (management and enforcement) of policies.
Interaction	*Depends* on D1.2-10.8; this requirement can only be fulfilled if policies are manifested by services as part of their specification.
ReqID	D1.2-10.3
Requirement	In a TAS^3 choreography, error messages returned after a request of a resource (e.g. “access denied” message) MUST be identifiable as such, e.g. through a special flag in the message header.

Justification	Applications might masquerade error messages for user-friendliness (e.g. they could produce a "pretty formatted" page); nonetheless, the TAS^3 architecture needs to be able to unambiguously recognize error messages without the need to delve into the semantics of the payload of the message. If we consider, for instance, the APL scenario, certain operations (such as accessing data or using functions) must be allowed only upon exhibiting corresponding credentials (e.g., to fill-out portfolio information, or to read certain portions of a portfolio).
Interaction	*Supports* R10.1, as test automation needs an oracle to determine the success/failure outcome of a test execution.
ReqID	**D1.2-10.4**
Requirement	Demonstrators SHALL provide good levels of end-user perceived trust.
Justification	The success of any information system architecture must be based not only on technology schemes, standards and protocols, but also on users' perceptions. We need to assure that TAS^3 services are improved in terms of perceived trust.
Interaction	*Depends on* D1.2-10.5, D1.2-10.6
ReqID	**D1.2-10.5**
Requirement	Demonstrators SHALL provide good levels of end-user perceived service quality.
Justification	The success of any information system architecture must be based not only on technology schemes, standards and protocols, but also on users' perceptions. Thus, we need to assure that TAS^3 services are improved in terms of perceived service quality from a non-technical perspective.
Interaction	*Supports* , D1.2-10.4, D1.2-10.6, D1.2-10.7.
ReqID	**D1.2-10.6**
Requirement	Demonstrators SHALL provide good levels of end-user perceived usability.
Justification	Usability is one of the most important validation issues for TAS^3 architecture. It is necessary to assure that TAS^3's services achieve good usability levels.
Interaction	*Supports* D1.2-10.5, D1.2-10.4 *Depends on* D1.2-10.7
ReqID	**D1.2-10.7**
Requirement	Demonstrators SHALL provide good levels of accessibility.
Justification	According to several EU's agreements, accessibility must be considered, especially in the case of public services (e.g., health). Thus, accessibility must be analyzed and taken into account in TAS^3's services.
Interaction	Supports D1.2-10.6
ReqID	**D1.2-10.8**
Requirement	Services that are to participate in a TAS^3 choreography MUST be accompanied with models describing their characteristics.
Justification	These models are part of a TAS^3 "governance contract" and constitute the basis on which the services are verified.
Interaction	*Supports* D1.2-10.1, D1.2-10.2, and D1.2-10.9.
ReqID	**D1.2-10.9**
Requirement	All services willing to participate in a TAS^3 choreography SHOULD be validated against the accompanying models.

Justification	Mandating that service characteristics (e.g., their behaviour, their extra-functional characteristics) be documented enables a number of (automated, rigorous) validation activities that are key to enhance the trustworthiness of services. In both the reference scenarios, all parties that interact should have gone through a preliminary validation phase. Furthermore, the outcome of this validation can also be used when selecting providers based on their trustworthiness (e.g., at step 3 of the APL scenario as well as at step 4 of the ML scenario). The type of validation and the extent to which such validation can be carried out depends on what information is included in the models attached to the services.
Interaction	*Depends* on D1.2-10.8, which mandates that services that are to participate in a TAS^3 choreography must be accompanied by specifications.

C.11 Requirements of WP12

ReqID	**D1.2-12.1**
Requirement	All developers, testers, and users MUST understand significant parts of the complete system at least at the conceptual level.
Justification	TAS^3 fundamentally secures business processes end to end. Isolated components may provide a tiny part of the end-to-end security, but are still part of a chain or mesh that can break. Knowledge outside the component focus is required ahead of time, so that expensive basic design mistakes can be avoided.
Interaction	*Depends* on D1.2-12.2
ReqID	**D1.2-12.2**
Requirement	All developers, testers, and users MUST have access to all project documentation regardless of origin, target audience, or assumed relevance.
Justification	The scope of the project is too wide to predetermine which people need what document, so the distribution is going to be pull instead of push.
Interaction	*Supports* D1.2-12.1
ReqID	**D1.2-12.3**
Requirement	Project participants MUST be left free to choose when and how to perform their contractual duties, within reason.
Justification	TAS^3 for nearly no participant is a 100% workload. Care needs to be taken that no process is pushed onto the participants that would dictate their daily work process which takes place in another organisation.
Interaction	
ReqID	**D1.2-12.4**
Requirement	A hierarchical escalation structure MUST be in place to raise important and/or urgent events to organisational levels above non-responsive ones.
Justification	When reasonable limits on time/resource allocation flexibility are exceeded and project progress is threatened, other partners daily operation may need to be altered.
Interaction	*Supports* D1.2-12.3
ReqID	**D1.2-12.5**
Requirement	All developers and testers MUST maintain their component documentation in a central repository that at the very least MUST be current for software that has been released outside the developers lab.

Justification	When any developer, tester, or user wants insight in what a component does, (s)he needs to be able to directly get the answer.
Interaction	*Supports* D1.2-12.1, D1.2-12.2
ReqID	**D1.2-12.6**
Requirement	E-mail as message system and/or dissemination system MUST be reduced as much as practical, and replaced by on-demand (pull) systems.
Justification	Twofold: it is often not possible to determine for exactly which people a message is important or will become important, yet broadcast to all is no option; and most people already receive too many messages so that the message would be likely lost anyway.
Interaction	*Supports* D1.2-12.2, D1.2-12.3, D1.2-12.4
ReqID	**D1.2-12.7**
Requirement	Released components MUST be checked and re-checked for correct operation in the network environment and developers MUST be kept up to date as of the performance of their released component.
Justification	Even when a component adheres exactly to the specifications, it may happen that situations arise where the specifications turn out to be wrong or incomplete. Unit tests are only run in isolation. Continuous integration has the power to reveal integration problems at an early stage.
Interaction	*Depends* on D1.2-12.4
ReqID	**D1.2-12.8**
Requirement	A controlled environment MUST be available to perform complex use cases and abuse cases of components in an orchestration.
Justification	Situations will arise where unexpected events, such as component failures or unspecified environmental conditions, interfere with a set of components. Due to complex relationships and cause-and-event patterns, problems may appear which are hard to create or foresee in isolated unit testing. It needs to be demonstrated that the orchestration is resilient to intentional abuse.
Interaction	*Supports* D1.2-12.7
ReqID	**D1.2-12.9**
Requirement	Components MUST be configurable in such a way that they intentionally perform in abnormal ways.
Justification	To fully test a constellation for resilience against malfunctions, components must be exposed to failing peers. We do not want to specifically develop mock components just for abuse testing when the real thing is available, and “knows” exactly what nasty failure modes it would have.
Interaction	*Supports* D1.2-12.7
ReqID	**D1.2-12.10**
Requirement	Multiple controlled environments SHOULD be available to rig parallel use and abuse setups with different components and/or configurations.
Justification	It is cumbersome to schedule tests on one central rig and tell developers to postpone testing until the rig has the right configuration in a specific time window.
Interaction	*Supports* D1.2-12.7
ReqID	**D1.2-12.11**
Requirement	An automated process SHOULD be available that allows hands-off setup of a complete controlled environment in a pre-defined configuration, running a set of use and abuse cases, and report the results.
Justification	
Interaction	*Supports* D1.2-12.7

ReqID	**D1.2-12.12**
Requirement	Components MUST come with a sub-component (“installation script”) which allows partial automation of the installation and configuration of the component.
Justification	With the central use/abuse rig central to the project, there is no excuse to rely on written textual material for very regular, routine installation and configuration procedures. Given the controlled environment, assumptions may be made about available resources and locations that in a more generic case would need to be left to the installing person.
Interaction	*Supports* D1.2-12.11
ReqID	**D1.2-12.13**
Requirement	Users MUST be able to verify that a constellation of components behaves according to their specifications.
Justification	TAS^3 aims to demonstrate usability in user scenarios.
Interaction	*Depends* on D1.2-12.8 *Supports* D1.2-12.15
ReqID	**D1.2-12.14**
Requirement	Specific test scenarios MUST be made available to automatically test constellations of components.
Justification	Without automation, testing remains a one-off event that cannot be used to continuously validate the quality of a constellation in production.
Interaction	*Implements* D1.2-12.13
ReqID	**D1.2-12.15**
Requirement	Users MUST be able to validate that a constellation of components behaves according to their scenario.
Justification	TAS^3 aims to solve user problems expressed in scenarios, but we need to make sure that the scenarios are correctly specified.
Interaction	*Depends* on D1.2-12.13
ReqID	**D1.2-12.16**
Requirement	Most procedures and automated functions required for the test bed MUST allow to be carried over to a production situation for permanent constellation monitoring.
Justification	TAS^3 Quality of Service requirements assume continuous monitoring of the working system, to provide KPI for quality assessment and trust perception.
Interaction	
ReqID	**D1.2-12.17**
Requirement	All components MUST come with documentation according to established standards and MUST follow an established delivery procedure.
Justification	To facilitate integration and production setup, modules need to be routinely handled by people not necessarily knowing the particular details of each module. This holds both for externally provided and in-house manufactured components.
Interaction	*Supports* D1.2-12.5 *Abstracts* D1.2-12.12
ReqID	**D1.2-12.18**
Requirement	All external components used in TAS^3 MUST have proper documentation and installation procedures available and one responsible partner per component MUST keep them current.

Justification	It cannot be left to the integrator or production maintainer to take on the burden of finding out exactly how one of the project partners wants to set up an external component. And more than one partner may need a conflicting setup. Component ownership.
Interaction	
ReqID	**D1.2-12.19**
Requirement	All components MUST come with documentation broken down in sections or reading guides for: 1. component developers, 2. peer component developers, 3. system administrators, 4. users, and 5. user managers.
Justification	People at all levels may need to refer to the module. Providing this index is little work for people familiar with the component, and impossible for newcomers. Having a clear management summary means overall trust in the system may improve.
Interaction	*Implements* D1.2-12.2
ReqID	**D1.2-12.20**
Requirement	Training sessions for developers and system managers MUST be provided.
Justification	It cannot be expected from all people that they can without training pick up and learn the important (security and business) aspects of all components. Expert help is required.
Interaction	*Implements* D1.2-12.1
ReqID	**D1.2-12.21**
Requirement	Change management MUST be enforced on core integration resources.
Justification	Where changes have the potential to cause far-reaching consequences not necessarily apparent to the changer, we need to manage the change proposal.
Interaction	*Supports* D1.2-12.2, D1.2-12.4, D1.2-12.6 *Conflicts* with D1.2-12.3 *Abstracts* D1.2-12.5
ReqID	**D1.2-12.22**
Requirement	Short, medium, and long term planning MUST be provided for the component developers to set their priorities.
Justification	The project-wide deliverable plan is too coarse to suggest daily, weekly, and monthly development activities, especially with respect to the interactions between components from different developers, and the advancing insight gained during the project.
Interaction	*Supports* D1.2-12.1, D1.2-12.3 *Implements* D1.2-12.4
ReqID	**D1.2-12.23**
Requirement	A single, central place MUST be available where all known issues and defects of all components are administrated.
Justification	With the projects focus on integration, even individual component developers need to be very aware of problems with their component outside the laboratory. And users of the component (peer developers) must be aware of problems with their peer component even if they have not encountered them yet.
Interaction	*Supports* D1.2-12.2, D1.2-12.6, D1.2-12.21 *Conflicts* with D1.2-12.3
ReqID	**D1.2-12.24**
Requirement	One resource MUST be available which authoritatively lists all available and required components, external and internal, uniquely identifiable throughout their life cycle.

Justification	For project planning and progress monitoring, a current overview of the purpose, status, and use of all components needs to be maintained.
Interaction	*Supports* D1.2-12.1, D1.2-12.23
ReqID	**D1.2-12.25**
Requirement	As part of a component catalog, an interface catalog MUST be centrally available.
Justification	Not all components are designed to talk to all other components. Designed or planned peer components share one interface, which must be documented, where possible ahead of implementation.
Interaction	*Supports* D1.2-12.22
ReqID	**D1.2-12.26**
Requirement	At least one reference constellation SHOULD be available which allows application-independent components to be integration-tested without a specific demonstrator scenario.
Justification	It can be expected that application-dependent modules put less demand and stress on an infrastructural component than what the infrastructural component was architecturally designed to cope with.
Interaction	*Supports* D1.2-12.7
ReqID	**D1.2-12.27**
Requirement	A common reference system MUST be available to uniquely identify data object types cross-application.
Justification	Policies are used to specify what is allowed to happen with data. Unknown data types mean the data is not allowed to be stored or processed and must be rejected. It is unlikely that any top-down standard will develop soon which unifies data types. Applications can bi-laterally agree on data types by using unique identifiers, allowing succesfull forwarding of data and policies even if the data format itself is as yet unprocessable.
Interaction	
ReqID	**D1.2-12.28**
Requirement	A transformation service SHOULD be available to help applications use data which is not natively known to them.
Justification	If parties have bi-laterally agreed on a unique data type, they can forward each others data while maintaining trust and privacy rules. By adding transformations, they can also process and manipulate the data according to trust and privacy rules.
Interaction	*Depends* on D1.2-12.27
ReqID	**D1.2-12.29**
Requirement	On request, developers MUST release a component which conforms to the standard framework (documentation, installation procedure, interface specification) even if this means releasing a mockup component without real functionality.
Justification	Peer developers often need to use a stub component to test their own component. Instead of developing the same stub over and over again, it is much more effective and efficient to have an early non-functional release of the actual component.
Interaction	*Supports* D1.2-12.22, D1.2-12.23
ReqID	**D1.2-12.30**
Requirement	Central resources MUST be updatable by all relevant people.
Justification	TAS^3 is too small a project to allow dedicated full-time support staff. When a central resource is found being inadequate or in error, everybody relevant to the resource should be able to change it. The resource editor then can, after the fact, inspect the change and possibly undo it or re-change. This avoids resource update bottlenecks.

Interaction	*Supports* D1.2-12.3, D1.2-12.4, D1.2-12.5

D Existing Solutions

The following is the list of software that provide existing solutions to some of the solved problems in TAS^3 . Solutions that solve the same problem, that provide alternative solutions are listed in a single table one after the other. Every separate table is another solution that will be adopted by the partners in TAS^3 .

The following includes the complete list of existing solutions that will be used by WP 3,4,5,7,8,9,10 and 12. The VUB team in WP2 has also provided us with existing solutions. The solutions that will be utilized by the Architecture team is included in Deliverable 2.1 [18].

Name of Solution	Intalio Designer, BPMS and Tempo
Link	http://www.intalio.org
Access	open source/open standard
Functionality	Graphical Process Modelling Tool based on BPMN (Business Process Modelling Notation), allows to deploy BPEL processes, which can be executed by Intalio/BPMS. Intalio Tempo is a enhancement of the Intalio Suite which supports human activities.
Limitations with respect to TAS^3	Open source part does not include XForms editor, data mapper, transformation into BPEL, and automatic deployment. Intalio/BPMS does not support security issues, like authorization, access rules, and their enforcement. Adaptation is only supported in a simple form, i.e. change a web service before its call without newly deploying the process. Tempo does not yet support federated identity/SSO.
Related Requirements	Fulfills D1.2-3.1 through D1.2-3.3, partially fulfills D1.2-3.4
Justification of Selection	In main parts it is open source software. Intalio provides graphical modeling as well as process execution engine and integrates both parts. The process modeling tool together with human activities is a very comprehensive and comfortably usable tool.
Name of Solution	Oracle BPM-Suite
Link	http://www.oracle.com/technologies/bpm/bpm-suite.html
Access	proprietary
Functionality	Business Process Modelling and Management in a SOA
Limitations with respect to TAS^3	Not open source software, not sufficient support of process adaptations and process security.
Related Requirements	Fulfills D1.2-3.1 through D1.2-3.3, partially fulfills D1.2-3.4
Name of Solution	IBM Web Sphere Integration Developer
Link	http://www-306.ibm.com/software/integration/wid/
Access	proprietary
Functionality	Business Process Modelling and Management in a SOA
Limitations with respect to TAS^3	Not open source software, not sufficient support of process adaptations and process security.
Related Requirements	Fulfills D1.2-3.1 through D1.2-3.3, partially fulfills D1.2-3.4
Name of Solution	ActiveBPEL Community Edition Engine
Link	http://www.activevos.com/community-open-source.php

Access	Proprietary
Functionality	Business Process Modelling and Management supporting BPEL (Business Process Execution Language)
Limitations with respect to TAS^3	Not open source software, not sufficient support of process adatations and process security.
Related Requirements	R3.1 through R3.3
Name of Solution	jBPM
Link	http://www.jboss.com/products/jbpm/
Access	Open source
Functionality	Business Process Modelling and Management
Limitations with respect to TAS^3	Lack of inherent web service support, not sufficient support of process adaptations and process security, no enhanced support for human activities.
Related Requirements	fulfills D1.2-3.1, fulfills D1.2-3.2 and D1.2-3.4 with limitations.

Name of Solution	PERMIS
Link	http://sec.cs.kent.ac.uk/permis
Access	open source/open standard
Functionality	- Allows one user to dynamically delegate access rights/permissions to another user and allows a process to be split into two or more tasks that have to be undertaken by different entities (e.g. manager and clerk) - Has a PDP and a CVS, Allows credentials to be pulled or pushed. Supports separation of duties and state based decision making. Supports delegation of authority. Has an XACML interface to the PDP. Supports XACML formatted obligations.
Limitations with respect to TAS^3	- Based on using X.509 ACs stored in LDAP directories. Start up can be time consuming if large audit trails are present. - Originally build to support authorisation credentials encoded as X.509 attribute certificates. Currently only has limited support for SAML formatted attribute assertions (e.g. Delegation only works with ACs and not with SAML assertions). - The policy language is not standardized - Is purely RBAC/ABAC based though could be extended to support DAC
Related Requirements	Fully fulfilled D1.2-7.6, D1.2-7.9, D1.2-7.24 Partially fulfilled: D1.2-3.5, D1.2-3.6, D1.2-7.1, D1.2-7.2, D1.2-7.12-15, D1.2-7.21, D1.2-7.23
Justification of Selection	- Open source software, based on XACML. -Has more required functionality than any other package, Is modular and allows plug and play with an XACML PDP

Name of Solution	K.U.Leuvens demonstrator framework
Link	To be provided
Access	open source

Functionality	Demonstrator framework that is able to illustrate the TAS^3 concepts. It currently provides a proof-of-concept implementation of the following TAS^3 concepts: break-the-glass, policy enforcement, user friendly policy management, transparency of executed business processes, secure communications
Limitations with respect to TAS^3	The service provider discovery mechanism of the demonstrator framework does not yet support trust and privacy policy negotiation.
Related Requirements	D1.2-2.1, D1.2-2.5, D1.2-2.6, D1.2-3.7, D1.2-10.5, D1.2-12.1
Justification of Selection	The demonstrator framework is proven technology that can easily be extended. During the first year of TAS^3 , the demonstrator framework has been extended with support for complex business processes, the break-the-glass function, and advanced policy enforcement.

Name of Solution	Belgian e-ID card
Link	http://eid.belgium.be
Access	open source and proprietary for Belgian citizens
Functionality	authentication mechanism used as a token that supports client authentication
Limitations with respect to TAS^3	no limitations specific to TAS^3
Related Requirements	
Justification of Selection	It is the authentication token that has the highest level of assurance that is currently available in the consortium.

Name of Solution	Encryption Algorithm AES
Link	http:csrc.nist.gov/publications/fips/fips197/fips-197.pdf
Access	open source
Functionality	encryption and decryption of data
Limitations with respect to TAS^3	no limitations specific to TAS^3
Related Requirements	
Justification of Selection	It is a standard encryption algorithm.

Name of Solution	Tulip Trust Management system
Link	http://dies.cs.utwente.nl/~czenkom/tulip/doc/
Access	open source
Functionality	Credential based trust management system.
Limitations with respect to TAS^3	Credential based trust management only, no support for other trust metrics. Does not use the TAS^3 trust service methodology.
Related Requirements	D1.2-5.6
Justification of Selection	Compared to other existing CTM systems TuLiP excels in key aspects for TAS^3 ; flexibility of the syntax, user authonomy and automation.

Name of Solution	PostgreSQL

Link	http://www.postgresql.org/
Access	Open source
Functionality	Relational database. Can be used to gather reputation feedback information and make it available to the reputation based trust management engine.
Limitations with respect to TAS^3	Does not provide complex operations required for behaviour-based trust policies. Not yet a web service. No support for integrity of information. Possibly requires strict access controls to prevent rigging of data. Does not support users privacy policies.
Related Requirements	D1.2-5.3, D1.2-5.4
Name of Solution	ORACLE
Link	http://www.oracle.com/database/index.html
Access	Proprietary
Functionality	Relational database. Can be used to gather reputation feedback information and make it available to the reputation based trust management engine.
Limitations with respect to TAS^3	Does not provide complex operations required for behaviour-based trust policies. Not yet a web service. No support for integrity of information. Possibly requires strict access controls to prevent rigging of data. Does not support users privacy policies.
Related Requirements	D1.2-5.3, D1.2- 5.4

Name of Solution	SunXACML
Link	http://sunxacml.sourceforge.net/
Access	Open source
Functionality	- XACMLv2 policy language reference implementation. Can be used as a basis for the Trust PDP.
Limitations with respect to TAS^3	- Supports the XACMLv2 standard but does not deal with trust or other TAS^3 extensions. - Does not support separation of duties, state based decision making. - Requires a separate CVS to validate user credentials. - Requires separate components to pull and push credentials. - Not good at supporting pure RBAC policies. - No good user interfaces for writing policies
Related Requirements	D1.2-5.1, D1.2-7.6
Justification of Selection	- Well known open source XACML implementation. - Uses an OASIS standard policy language. - Supports a wide range of access control policies. - Can be combined with PERMIS.

Name of Solution	Trust Policy Wizard
Link	http://i40virt02.ipd.uka.de/CoSim/
Access	Open source
Functionality	Allows guided interactive formulation of trust policies.
Limitations with respect to TAS^3	Only supports behaviour-based trust policies.
Related Requirements	D1.2-5.9
Justification of Selection	Providing a wizard is a powerful yet straightforward way of supporting user selected policies. We do not exclude the possibility for more integrate solutions such as e.g. natural language policy editors.

Name of Solution	Shibboleth IDP and SP software for SSO
Link	
Access	Open Source
Functionality	Provides user authentication and SSO using SAMLv2.
Limitations with respect to TAS^3	Not easy to install or configure
Related Requirements	D1.2-7.3, D1.2-7.18
Name of Solution	SAMP PHP
Link	
Access	Open Source
Functionality	Provides user authentication and SSO using SAMLv2. Reputedly easy to use
Limitations with respect to TAS^3	Not sure, will need to investigate
Related Requirements	D1.2-7.3.D1.2-7.18.
Name of Solution	Lasso
Link	http://lasso.entrouvert.org/
Access	Open Source
Functionality	Liberty Alliance Library, support : SAML2, ID-WSF, ID-SIS Personal Profile and HR (based on Europass CV profile).
Limitations with respect to TAS^3	
Related Requirements	D1.2-10.8, D1.2-10.2

Justification of Selection	OpenSource, certified by Liberty Alliance / OASIS regarding SAML2 support. Supports the HR ID-SIS draft profile which is a profile of the European Europass CV initiative (promoted by CEDEFOP EU Agency). Note that this HR profile is also supported by ZXID.
Name of Solution	Authentic
Link	http://authentic.labs.libre-entreprise.org/
Access	Open Source
Functionality	Liberty Alliance compliant ID Provider, support : SAML2, ID-WSF, ID-SIS Personal Profile and HR (based on Europass CV profile).
Limitations with respect to TAS^3	
Related Requirements	D1.2-7.7, D1.2-7.10, D1.2-7.26, D1.2-7.27, D1.2-9.1, D1.2-9.16, D1.2-9.1, D1.2-9.16, D1.2-10.8, D1.2-10.2
Name of Solution	LARPE
Link	http://larpe.labs.libre-entreprise.org/
Access	Open Source
Functionality	Liberty Alliance Reverse Proxy. It allows any website to use Liberty Alliance features (Identity federation, Single Sign On and Single Logout) without changing the code of the service provider itself. Its Liberty Alliance compliance relies on Lasso. It also supports the draft HR ID-SIS which allow mapping of an existing applicant/recruiting form with user Europass CV data stored by another service in the Circle of Trust with privacy secured by ID-WSF.
Limitations with respect to TAS^3	
Related Requirements	D1.2-8.2, D1.2-9.11, D1.2-9.14, D1.2-9.16, D1.2-12.28

Name of Solution	CVT (CV Transcoding Web Service)
Link	http://cvt.eife-l.org/
Access	Open Source
Functionality	Interoperability gateway/backoffice service which allow transformation of CV/ePortfolio related data from one format to another one. Support: Europass CV, IMS ePortfolio Netherlands, LinkedIn hResume, HR ID-SIS.
Limitations with respect to TAS^3	
Related Requirements	D1.2-8.2, D1.2-9.11, D1.2-9.14, D1.2-10.8, D1.2-12.28

Name of Solution	TrustBuilder2
Link	
Access	Open Source
Functionality	Provides trust negotiation and gradual release of credentials. It is written in Java and allows plugin modules for policy evaluation and negotiation strategy. It allows credentials and policies to be written in any language providing the correct plugins are available.
Limitations with respect to TAS^3	Not sure, will need to investigate
Related Requirements	D1.2-7.17
Justification for Selection:	Whilst we will probably need to write some of our own plugins in order to support the policies and credentials of TAS^3 , nevertheless we anticipate that the TrustBuilder2 infrastructure will support this.

Name of Solution	Fedora Repository
Link	http://www.fedora-commons.org/
Access	open source
Functionality	Repository for all kind of data. Accessible through a web service interface. Can be integrated in a SOA.
Limitations with respect to TAS^3	Is not aware of TAS^3 secure or trusted communication.
Related Requirements	D1.2-8.6
Justification of Selection	- The Fedora repository can be completely integrated in a SOA. - In Fedora all functionalities of the repository are accessible through a SOAP or REST based web service interface. - Moreover, Fedora is Open Source and has a strong community behind it.
Name of Solution	DSpace
Link	http://www.dspace.org/
Access	Open source
Functionality	Storage of documents.
Limitations with respect to TAS^3	Not all functions available over web service interface.
Related Requirements	Partially D1.2-8.6
Name of Solution	CDSware
Link	http://cdsware.cern.ch/
Access	Open source
Functionality	Storage of documents.
Limitations with respect to TAS^3	Not all functions available over web service interface.
Related Requirements	Partially D1.2-8.6
Name of Solution	EPrints
Link	http://www.eprints.org/
Access	Open source
Functionality	Storage of documents.
Limitations with respect to TAS^3	Not all functions available over web service interface.
Related Requirements	Partially D1.2-8.6

Name of Solution	Saturn
Link	http://saturnportal.nottingham.ac.uk/
Access	University of Nottingham authorised access only as the system contains live student data. Proprietary system designed, built and maintained in house.
Functionality	University of Nottingham student records system
Limitations with respect to TAS^3	- Not yet web-service enabled. - Closed internal system. - As this is live student data we cannot create test accounts for the project
Related Requirements	Used for authentication of student ID within our demonstrator; also used to establish eligibility for scheme. Allows access to module information to show which modules the student is studying
Justification of Selection	Source of student data as held by the institution

Name of Solution	ePARS (electronic Personal and Academic Record System)
Link	https://epars.nottingham.ac.uk/shared/htm/about.asp
Access	University of Nottingham system

Functionality	Designed to support tutorials and student personal development.
Limitations with respect to TAS^3	Used as a proxy for Saturn
Related Requirements	Takes regular data dumps of data from the live Saturn system, and has a facility to create test accounts with dummy data, so can act as a proxy for Saturn in the demonstrator.
Justification of Selection	Allows access to Saturn data without having to access Saturn direct, which we would not be allowed to do for demonstration purposes.

Name of Solution	OPUS
Link	http://foss.ulster.ac.uk/projects/opus/
Access	Open source, we have an instance installed on our development server.
Functionality	Placement co-ordination package
Limitations with respect to TAS^3	Local implementations only, can have multiple instances in a system.
Related Requirements	The software is specially designed for placement management and will be linked into the ePortfolio to aid students in the vacancy discovery process and skills matching scenarios.
Justification of Selection	Open source, customisable

Name of Solution	Mahara
Link	http://mahara.org/
Access	Open source
Functionality	ePortfolio system
Limitations with respect to TAS^3	Designed primarily as a learning ePortfolio, but a lot of work is being done by the community to support use for work placements.
Related Requirements	Learner-owned system, needs to be hosted but is outside the university or placement provider control. The learner can control which information others can see. Web access.
Justification of Selection	Many ePortfolio systems are available, there are over 80 in use in the UK at the moment, but not all are free and not all are web-based. Many remain under institutional control. This system is open source, we are in contact with the developers through other project work, and there is ongoing development to support use for work placements so there is a strong community of interest

Name of Solution	PebblePad
Link	http://www.pebblepad.co.uk
Access	Proprietary
Functionality	Personal ePortfolio system
Limitations with respect to TAS^3	Designed primarily to support learning
Related Requirements	Learner-owned system which interfaces to the ePortfolio and let's learners control which information others can see.

Justification of Selection	Web-based, learner-controlled system. We have a good relationship with the company through other project work. The system supports exports in a variety of standards, including UK-LEAP and IMS ePortfolio. Furthermore, we are likely to be able to access demonstrator candidates who have established ePortfolios using the system and offer a rich source of demonstrator data.

Name of Solution	Kenteq Competent WEB application
Link	http://testcompetent.kenteq.nl
Access	The application is property of Kenteq
Functionality	Competent provides functionality to complete administration services, test employment candidates, and generate reports.
Limitations with respect to TAS^3	Competent does not support the full (complete) employability process.
Related Requirements	See prior D1.2, chapter WP09 APL demo 8 - 14.
Justification of Selection	Most applications that support (parts of) employability processes are embedded in software for internal HR processes. Competent supports the APL and profile matching process as such, independently from the organisation or individual who applies for an employability service. There is no other off-the-shelve application available who supports employability processes. The application of the employability provider is outside the TAS^3 infrastructure, but within the scope of the TAS^3 demonstrator, where it is necessary as application to support and exchange data for the demonstrator scenarios D1.4 1.3 APL and 1.4 Mass layoff. . The application is in English and Dutch language, what is an advantage for the NL demonstrator.

Name of Solution	PILS Patient Information Location Service
Link	http://www.custodix.com/
Access	Proprietary Custodix Software. Available for the demonstrators, can be customized for the demonstrators.
Functionality	Front-end for looking up (distributed search) and displaying medical information from different medical repositories.
Limitations with respect to TAS^3	No known limitations at this point in time.
Related Requirements	Providing a front-end for data retrieval in the eHealth scenarios of D1.4 and D9.1.
Justification of Selection	Fully working solution, completely under the control of one of the partners (Custodix), which means that the solution can easily be customized to fit into the pilots. Next to PILS, an XACML driven medical record repository is available. Together they form a complete system for access to distributed medical information with dynamic policy based access control. The complete system is a good benchmark for evaluating the added value of TAS^3 .

Name of Solution	Personal Health Record
Link	No link available.
Access	Depending on official choice (presumed to be proprietary)
Functionality	Personal data store for managing personal medical information (i.e. patient controlled repository).
Limitations with respect to TAS^3	Originally Medisoft was providing the Orca system. However they left the project early as they felt they could no longer provide the required software. The administrative complexity of this event has delayed official appointment of a new PHR subcontractor (a candidate is available though).
Related Requirements	User centric (i.e. with user supplied data) medical repository. A place where a patient can manage his own data. The PHR concentrates data from a variety of sources (from accredited professionals to carers and the patient himself) and is an important element for testing trust based components.
Justification of Selection	The current candidate is selected by the pilot end-users themselves for their pathology (patient organization).

Name of Solution	WS-Guard
Link	http://plastic.isti.cnr.it/wiki/tools
Access	Open source (GPLv3)
Functionality	WS-Guard provides a prototype implementation of a framework augmenting the registration phase of a service within a registry with a testing phase. Registration is then guaranteed only if the service passes the testing phase.
Limitations with respect to TAS^3	The conformance validation is based on behavioural models in the form of Service State Machines (SSM). Within TAS^3 , we intend to verify service compliance based on the manifested policy. Furthermore, there is no support to the notions of identity and roles.
Related Requirements	D1.2-10.9, D1.2-10.1, D1.2-10.2
Justification of Selection	WS-Guard is developed by CNR as a result of research in related areas. There is no comparative tool performing the same functionalities.

Name of Solution	ZXID
Link	http://www.zxid.org/
Access	Open source (Apache License 2.0)

Functionality	ZXID aims at full stack implementation of all federated identity management and identity web services protocols. Initial goal is supporting SP role, followed by ID-WSF WSC and IdP roles. Provides user authentication and SSO using SAMLv2. Specifically: 1. SAML 2.0 SSO SP role and XACML PEP for Apache as mod_auth_saml 2. SAML 2.0 SSO SP role as programming toolkit for C, C++, Java, C#, PHP, and Perl 3. SAML 2.0 SSO IdP role 4. XACML PEP as programming toolkit for C, C++, Java, C#, PHP, and Perl 5. ID-WSF WSC role as programming toolkit for C, C++, Java, C#, PHP, and Perl 6. ID-WSF WSP role as programming toolkit for C, C++, Java, C# PHP, and Perl 7. Discovery client as programming toolkit for C, C++, Java, C#, PHP, and Perl 8. Discovery registration as programming toolkit for C, C++, Java, C#, PHP, and Perl 9. Discovery service. 10. People Service Client as programming toolkit for C, C++, Java, C#, PHP, and Perl 11. People Service.
Limitations with respect to TAS^3	
Related Requirements	D1.2-10.8, D1.2-10.2
Justification of Selection	Nonexclusive choice. Written by SAML, ID-WSF, and XACML insider. Well interopped. SAML 2.0 and ID-WSF 2.0 certified in its commercial (Symlabs) incarnation. Developed by a TAS^3 contributor, so ensures good support. Also, selected by the architecture team.

Name of Solution	TAXI
Link	http://www1.isti.cnr.it/ERI/TAXI/taxi_index.html
Access	Open source (GPLv2)
Functionality	TAXI is a tool for the systematic generation of XML instances. The TAXI methodology is largely inspired to the well-known Category Partition, which provides a stepwise intuitive approach to functional testing, as follows: identify the relevant input parameters; define the environment conditions; combine their significant values into an effective test suite.
Limitations with respect to TAS^3	Cannot deal with negative tests and fuzz tests. Moreover it does not currently address handling of access policies, e.g. XACML
Related Requirements	D1.2-10.1, D1.2-10.2
Justification of Selection	TAXI is developed by CNR as a result of research in related areas. There is no comparative tool performing the same functionalities.

Name of Solution	Eye-Tracker Tobii
Link	http://www.tobii.com

Access	Proprietary. Accessible by University of Zaragoza at Walqa (a technological park of reference in Spain)
Functionality	Tools for identifying what participants look at during the course of a usability-accessibility test. Other offerings exist in the market but Tobbi solutions can be considered as the leader in this field.
Limitations with respect to TAS^3	Any usability and accessibility analysis is limited if it is not completed with indicators that allow accurate measurement of how easy it is to manage the application; that is, perceived usability by end-users
Related Requirements	D1.2-10.6, D1.2-10.7 (but this tool does not fully comply with the non-technical perspective of this requirement)
Justification of Selection	

Name of Solution	ClickTracks, WebTrends
Link	http://www.clicktracks.com, http://www.webtrends.com/
Access	Proprietary
Functionality	Specific software packages for tracking the software user's behaviour, especially when the software is implemented over web protocols. Others free or low-cost solutions, such Google Analytics dont offer the same level of functionalities.
Limitations with respect to TAS^3	This tools do not allow us to assess the levels of usability or accessibility, so that it is not possible to determine whether the software user is satisfied or not
Related Requirements	D1.2-10.6, D1.2-10.7, (but these tools are insufficient to fully comply with the non-technical perspective of this requirement)
Justification of Selection	

Name of Solution	Structural Modeling (EQS, PLS, SPSS)
Link	http://www.mvsoft.com/ http://www.spss.com
Access	Proprietary
Functionality	Analyze causal relationships among multiple latent variables. Others packages, such as LISREL or AMOS offer similar functionalities, but the research group has been working with EQS, PLS and SPSS for several years. In addition, other techniques such as linear regression or cluster analysis do not allow to analyze relationships among latent variables or to include a variable that plays a double role (independent as well dependent), which is possible to conduct in structural modeling.
Limitations with respect to TAS^3	N.A.
Related Requirements	D1.2-10.4, D1.2-10.5, D1.2-10.6 (these tools will help to analyze relationships among variables that will serve to determine the main precursors of trust and service quality on end-users mind)
Justification of Selection	University of Zaragoza has the access to these specific statistical packages.

Name of Solution	Jira
Link	http://www.atlassian.com/software/jira/
Access	Proprietary
Functionality	Flexible web based bug tracking, issue tracking, task tracking, and project management software solution used for open source and enterprise projects.
Limitations with respect to TAS^3	Cost, complexity.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	Concurrent Versions System CVS
Link	http://en.wikipedia.org/wiki/Concurrent_Versions_System
Access	Open source
Functionality	Basic file repository with good revision control.
Limitations with respect to TAS^3	File-based, optimised for text.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	Subversion SVN
Link	http://subversion.tigris.org/
Access	OpenSource
Functionality	Basic file repository with good revision control.
Limitations with respect to TAS^3	File-based.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	MediaWiki
Link	http://www.mediawiki.org/
Access	OpenSource
Functionality	Wiki package for document and file management.
Limitations with respect to TAS^3	Complexity, needs a database.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	DokuWiki
Link	http://www.dokuwiki.org/
Access	OpenSource
Functionality	Wiki package for document and file management.
Limitations with respect to TAS^3	
Related Requirements	D1.2-12.1, D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.20, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.27, D1.2-12.30).

Name of Solution	Confluence
Link	http://www.atlassian.com/software/confluence/
Access	Proprietary
Functionality	Confluence is a simple, powerful wiki that lets you create and share pages, documents and rich content with your team.
Limitations with respect to TAS^3	Cost, complexity, needs Java and a database.
Related Requirements	D1.2-12.1, D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.20, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.27, D1.2-12.30).

Name of Solution	Redmine
Link	http://www.redmine.org/
Access	OpenSource
Functionality	Redmine is a flexible project management web application. Written using Ruby on Rails framework, it is cross-platform and cross-database.
Limitations with respect to TAS^3	Assumes a particular work flow model and dedicated resources for response and dispatch.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	Trac
Link	http://trac.edgewall.org/
Access	OpenSource
Functionality	Trac is an enhanced wiki and issue tracking system for software development projects. Trac uses a minimalistic approach to web-based software project management. Our mission is to help developers write great software while staying out of the way. Trac should impose as little as possible on a team's established development process and policies.
Limitations with respect to TAS^3	Complex and heavyweight.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	BugZilla
Link	http://www.bugzilla.org/
Access	OpenSource
Functionality	Bugzilla is server software designed to help you manage software development.
Limitations with respect to TAS^3	Complex and heavyweight.
Related Requirements	D1.2-12.3, (D1.2-12.4, D1.2-12.6, D1.2-12.23, D1.2-12.24, D1.2-12.30)

Name of Solution	GIT
Link	http://git-scm.com/
Access	OpenSource
Functionality	Git is a free and open source, distributed version control system designed to handle everything from small to very large projects with speed and efficiency.
Limitations with respect to TAS^3	Possibly immature.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	Hudson
Link	https://hudson.dev.java.net/
Access	OpenSource

Functionality	Hudson monitors executions of repeated jobs, such as building a software project or jobs run by cron.
Limitations with respect to TAS^3	Possibly heavyweight, biased to Java.
Related Requirements	D1.2-12.7 (D1.2-12.11, D1.2-12.15).

Name of Solution	ActiveCollab
Link	http://www.activecollab.com/
Access	Proprietary
Functionality	ActiveCollab is a project management and collaboration tool that you can set up on your own website. Have an area where you can collaborate with your team, clients and contractors and keep projects on track while retaining full control over access permissions and your data.
Limitations with respect to TAS^3	Implies a work process that relies on dedicated resources.
Related Requirements	D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.30).

Name of Solution	Nagios
Link	http://www.nagios.org/
Access	OpenSource
Functionality	Scalable resource/network monitor framework.
Limitations with respect to TAS^3	
Related Requirements	D1.2-12.7 (D1.2-12.11, D1.2-12.15).
Justification of Selection	

Name of Solution	Semantic MediaWiki SMW
Link	http://en.wikipedia.org/wiki/Semantic_MediaWiki
Access	OpenSource
Functionality	SMW allows for annotating semantic data within wiki pages, thus turning a wiki that incorporates the extension into a semantic wiki.
Limitations with respect to TAS^3	Possibly over the top complex for what developers do.
Related Requirements	D1.2-12.1, D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.20, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.27, D1.2-12.30).

Name of Solution	OntoPrise OntoStudio
Link	http://www.ontoprise.de/en/home/products/ontostudio/
Access	Proprietary/OpenSource dual licensed
Functionality	Extensions of SMW for production purposes, supporting ontology development and integration.
Limitations with respect to TAS^3	Possibly cost, lack of dedicated resources to use it.

Related Requirements	D1.2-12.1, D1.2-12.2, D1.2-12.3 (D1.2-12.4, D1.2-12.5, D1.2-12.6, D1.2-12.6, D1.2-12.17, D1.2-12.18, D1.2-12.19, D1.2-12.20, D1.2-12.21, D1.2-12.24, D1.2-12.25, D1.2-12.27, D1.2-12.30).

Name of Solution	DOGMA Studio Workbench
Link	
Access	Although the solution is open-source, the software is located on a web server with restricted access.
Functionality	It allows the elicitation and visualisation of DOGMA inspired ontologies.
Limitations with respect to TAS^3	
Related Requirements	D1.2-2.23
Justification of Selection	This is the only tool that supports DOGMA inspired ontology.

E Inter-WP Requirements Interactions (First Iteration)

E.1 Interactions of WP2

Source Requirement	Interaction Type	Target Requirements
D1.2-2.23	supports	D1.2-3.12, D1.2-3.14
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP2

E.2 Interactions of WP3

Source Requirement	Interaction Type	Target Requirements
D1.2-3.1	supports	D1.2-2.23, D1.2-5.5
	depends on	D1.2-6.3
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3
D1.2-3.2	supports	D1.2-5.5, D1.2-6.12, D1.2-9.1
	depends on	D1.2-6.2
	abstracts	
	implements	D1.2-8.3
	similar to	
	Note	Partially implements D1.2-6.12
This requirement will be fulfilled by WPs		WP3
D1.2-3.3	supports	D1.2-6.10
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3
D1.2-3.4	supports	D1.2-9.12
	depends on	
	abstracts	
	implements	
	similar to	
	Note	I would have expected some requirement(s) that specifically target(s) the ID management infrastructure that D2.1 describes in so much detail, but I cant find one (would be a depends on).
This requirement will be fulfilled by WPs		WP7
	supports	

	depends on	D1.2-7.13
	abstracts	
	implements	D1.2-7.23, D1.2- 9.4
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3, WP7
D1.2-3.6	supports	
	depends on	D.1-7.13
	abstracts	
	implements	D1.2-7.23, D1.2-9.4
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP2, WP3
D1.2-3.7	supports	
	depends on	D1.2-7.13
	abstracts	
	implements	D1.2-7.1
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3
D1.2-3.9	supports	
	depends on	D1.2-10.3
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3
D1.2-3.11	supports	D1.2-2.14
	depends on	
	abstracts	D1.2-7.7
	implements	D1.2-7.26
	similar to	D1.2-8.5, D1.2-9.6
	Note	
This requirement will be fulfilled by WPs		WP3, WP4
D1.2-3.12	supports	D1.2-10.8
	depends on	
	abstracts	
	implements	
	similar to	D1.2-2.14, D1.2-4.7, D1.2-2.23
	Note	
This requirement will be fulfilled by WPs		WP3, WP6
D1.2-3.13	supports	D1.2-5.5
	depends on	D1.2-6.6
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3
D1.2-3.14	supports	
	depends on	
	abstracts	
	implements	D1.2-2.23, D1.2-10.8
	similar to	
	Note	
This requirement will be fulfilled by WPs		
D1.2-15	supports	
	depends on	D1.2-4.9, D1.2-5.1

	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP3

E.3 Interactions of WP4

Source Requirement	Interaction Type	Target Requirements
D1.2-4.1	supports	D1.2-2.9, D1.2-2.20, D1.2-7.7, D1.2-7.26, D1.2-8.5, D1.2-8.6, D1.2-9.2, D1.2-9.6, D1.2-9.7, D1.2-9.12, D1.2-9.13, D1.2-9.8, D1.2-9.9
	depends on	D1.2-2.18, D1.2-2.19
	abstracts	D1.2-3.11
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.2	supports	D1.2-7.8, D1.2-7.16, D1.2-7.18, D1.2-7.27, D1.2-9.16, D1.2-12.27
	depends on	
	abstracts	D1.2-3.4
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.3	supports	D1.2-2.1, D1.2-2.5, D1.2-2.6, D1.2-3.7, D1.2-12.1, D1.2-10.5
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.4	supports	D1.2-2.11, D1.2-2.12, D1.2-2.14, D1.2-7.1, D1.2-7.6, D1.2-2.10, D1.2-2.15, D1.2-2.22, D1.2-3.3, D1.2-3.7, D1.2-7.14, D1.2-7.21, D1.2-7.24, D1.2-7.25, D1.2-9.4, D1.2-9.5, D1.2-9.11, D1.2-9.16, D1.2-9.17
	depends on	D1.2-2.18, D1.2-2.19
	abstracts	D1.2-2.17, D1.2-3.12, D1.2-7.3, D1.2-9.10
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.5	supports	D1.2-2.11, D1.2-2.12, D1.2-2.14, D1.2-2.9, D1.2-2.10, D1.2-2.20, D1.2-3.7, D1.2-3.12, D1.2-3.15, D1.2-9.10, D1.2-9.16, D1.2-9.22
	depends on	D1.2-2.18, D1.2-2.19
	abstracts	D1.2-2.21, D1.2-7.24
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
	supports	D1.2-3.10, D1.2-7.22

	depends on	D1.2-2.18, D1.2-2.19
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.7	supports	D1.2-2.5,D1.2-2.10, D1.2-2.11, D1.2-2.12
	depends on	
	abstracts	D1.2-3.14
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.8	supports	D1.2-2.11, D1.2-2.12, D1.2-2.10, D1.2-2.13, D1.2-3.3, D1.2-9.3, D1.2-9.7, D1.2-9.14, D1.2-10.6
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4
D1.2-4.9	supports	D1.2-5.1, D1.2-2.10, D1.2-5.3, D1.2-5.4
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP4

E.4 Interactions of WP 5

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-5.1	supports	D1.2-10.4
	depends on	
	abstracts	
	implements	
	similar to	
	Note	As part of the overall authorization framework, this requirement also support requirements on authorization (D1.2-2.20, D1.2-3.11, D1.2-4.5, D1.2-6.6, D1.2-6.12, D1.2-7.6, D1.2-9.1, D1.2-9.4)
This requirement will be fulfilled by WPs		WP5
D1.2-5.5	supports	
	depends on	D1.2-3.1 and D1.2-3.13
	abstracts	
	implements	
	similar to	
	Note	Business process management (WP3) should provide support for and check inclusion of a feedback form which enables the user to give feedback on the current process. For the demonstrator use cases it will be addressed by WP9 in the trust dashboard.
This requirement will be fulfilled by WPs		WP3, WP9
D1.2-5.6	supports	

	depends on	D1.2-7.12, D1.2-7.15
	abstracts	
	implements	D1.2-7.13
	similar to	
	Note	The credential based trust management (CTM) service will require credential handling. For credentials expressing trust relationships finding credentials is part of the CTM service design.
This requirement will be fulfilled by WPs		WP5, WP7
D1.2-5.9	supports	D1.2-2.12, D1.2-2.13, D1.2-4.3, D1.2-8.4, D1.2-8.5, D1.2-9.6
	depends on	
	abstracts	
	implements	D1.2-7.13
	similar to	
	Note	The credential based trust management (CTM) service will require credential handling. For credentials expressing trust relationships finding credentials is part of the CTM service design
This requirement will be fulfilled by WPs		WP5, WP7
D1.2-5.10	supports	
	depends on	
	abstracts	
	implements	
	similar to	D1.2-7.3, D1.2-3.4, D1.2-9.12
	Note	Implementing D1.2-7.3 in such a way that D1.2-3.4 is achieved will also satisfy this requirement. D1.2-9.12 is a reformulation of the same requirement (with different justification).
This requirement will be fulfilled by WPs		WP7

E.5 Interactions of WP 6

WP 6 consists of the legal requirements and contractual framework. Both of these topics are horizontal and crosscutting; impacting or being impacted by every aspect of the project. To that end, WP6 Interactions will be set forth in a more text-based fashion at the level of the interaction with the WP rather than at the specific requirement level, though attempts will be made to call out those requirements that have special relationships with legal requirements or the contractual framework.

We mentioned in Section 4.4 that WP6 entails three kind of requirements: intake and qualification; basic legal requirements that emanate from the EU Data Protection Directive; and, requirements related to the contract and policy frameworks. In the course of mapping interactions, they will be described as the: Intake, Legal Requirement and Contract Framework sections, respectively.

WP2 – Architecture	As a central element of TAS^3, the architecture is perhaps most closely intertwined with both the legal requirements and contract framework. One of the innovative approaches of TAS^3 was the development of technology, policy and contract/legal in collaboration and there has been significant interaction between the architecture team in addressing legal requirements (D1.2-2.21, -2.22) and in functions such as authentication (D1.2-2.17) logging, access control and audit (D1.2-2.18. The Important relationships also exist as related to the contract framework where contract and required policies support security (D1.2-2.7, -2.16) oversight/accountability (D1.2-2.15), implementation of TAS^3 (D1.2-2.9) and functions such as limits on disclosure (D1.2-2.20).

WP3 – Business Process Modeling	Business processes are related to legal requirements because in their modeling they must operate within the confines of the legal requirements. Issues like treating PII/Identity management ((D1.2-3.4), Access control and role management (D1.2-3.6-3.6, -3.10) and user controls (D1.2-3.11). They are likewise supported and constrained by contractual requirements that impose obligations. The most important one is the requirement to have access to a privacy policy (D1.2-3.14). Contract framework can also help support functions like special circumstances and error recovery (D1.2-3.9) and delegation (D1.2-3.7).
WP4 – Secure and Trustworthy Processing	By its very subject matter WP4 is tasked to give effect to many of the legal requirements. Concepts of user control (D1.2-4.1), confidentiality/pseudonymity (D12.-4.2 contributes), and proof/compliance functions (D1.2-4.5-4.6) are all essential to privacy. The latter two are also essential elements that both support and are supported by the contract framework. One of the reasons why the collaborative approach is so needed is because of these interactions where a requirements is both supported by and supporting an aspect of the contract framework.
WP5 – Flexible Trust Management Framework	Legal and contract framework interaction with WP5 may be more in terms of how some elements of WP5 give effect to requirements through mechanisms as well as how those mechanisms may be enabled. For instance, legal requirements of user control will be given effect through (D1.2-5.1-5.3) the need for trust policies and management is essential to users making informed choices and setting appropriate controls. The ability to use reputation and other feedback information (D1.2-5.4-5.5) will need to be enabled by contracts binding the reputation services ((D1.2-5.11).
WP7 – Privacy Authorization Infrastructure	In many ways WP7 provides the technical mediation of privacy, which is informed by privacy requirements and supported by the contract framework to bind service providers to the processes/technical elements. Among the more important legal requirements support by WP7 are collection limitation ((D1.2-7.5), user control (D1.2-7.7), pseudonymity (D1.2-71.6), data minimization (D1.2-7.18), and consent (D1.2-7.26). WP7 also provides functions in support of the contract framework, which are likewise supported by provisions of the contract framework, most notably oversight by tracking delegations (D1.2-7.1, -7.14), authorizations (D1.2-7.6, -7.23) and preventing collusion (D1.2-7.8, -7.18).
WP8 – Uniform Interface	WP8 is mostly providing technical functionality/specification, which may be related to legal requirements and contract framework in elements such as end user interface ((D1.2-8.4) user control ((D1.2-8.5) and access to both legacy (D1.2-8.2) and repository data (D1.2-8.6).
WP9 – Demonstrators	The demonstrators are the place where we test the contract framework and assess mechanisms of compliance with legal requirements, as such they are part of the iterative development process of the operation of the contract framework and the completeness and usability of the legal requirements. Essential elements of both legal requirements and contract framework such as user control (D1.2-9.2, -9.6) audit (D1.2-9.5), Access (D1.2-9.7-9.8), data minimization (D1.2-9.16) and security (D1.2-9.4,-9.13) are all specified and brought to life in the demonstrators.

WP10 – Quality	WP10 is an important element in testing/demonstrating compliance and oversight. This role is important to help assure that legal requirements are followed and to enable better visibility of possible contract framework violations or issues. Some aspects of the testing process may also be useful in judging the capacity for compliance as part of the intake process. The WP requirements specify important compliance elements including: ongoing testing (D1.2-10.1), Detection of service failures and errors (D1.2-10.2-10.3) and propagation of service provider characteristics (D1.2-10.8).
WP12 – Integration	WP12 plays an important project role to help assure that the elements of TAS^3 work in unison. From both the legal requirements and contract framework perspective, these are import functions as both require that TAS^3 be able to provide a cohesive trust and security architecture with appropriate end-to end controls and functionality. Integration of program components is an obvious necessity.

E.6 Interactions of WP 7

Source Requirement	Interaction Type	Target Requirements
D1.2-7.1	supports	D1.2-3.7
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.3	supports	D1.2-5.10, D1.2-9.4, D1.2-9.16, D1.2-9.17, D1.2-9.18, D1.2-9.19, D1.2-9.20, D1.2-9.21
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.6	supports	D1.2-2.20, D1.2-4.5, D1.2-9.1, D1.2-9.4, D1.2-9.10, D1.2-9.22
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.7	supports	D1.2-3.11, D1.2-4.1, D1.2-8.5, D1.2-9.2, D1.2-9.6, D1.2-9.8, D1.2-9.12
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.9	supports	D1.2-3.10
	depends on	
	abstracts	

	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.12	supports	D1.2-5.6, D1.2-9.3
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.13	supports	D1.2-5.6, D1.2-9.3
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.15	supports	D1.2-5.6
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.17	supports	D1.2-5.6
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.19	supports	D1.2-3.6, D1.2-3.7, D1.2-3.13
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.20	supports	D1.2-3.6, D1.2-3.7
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.22	supports	D1.2-4.6
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.24	supports	D1.2-9.5
	depends on	
	abstracts	

	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-7.27	supports	D1.2-3.8
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP7

E.7 Interactions of WP 8

Source Requirement	Interaction Type	Target Requirements
D1.2-8.1	supports	D1.2-2.3, D1.2-2.4, D1.2-2.5 D1.2-2.6, D1.2-2.9, D1.2-2.13, D1.2-9.2, D1.2-9.11, D1.2-9.14, D1.2-3.12, D1.2-3.14, D1.2-7.18
	depends on	D1.2-2.21, D1.2-2.23, D1.2-7.2, D1.2-7.1, D1.2-7.3, D1.2-7.6, D1.2-7.14
	abstracts	
	implements	
	similar to	
	Note	ADPEP - gateway
This requirement will be fulfilled by WPs		WP8, WP2, WP7, WP4
D1.2-8.2	supports	D1.2-9.7, D1.2-7.18
	depends on	
	abstracts	
	implements	
	similar to	
	Note	Legacy databases
This requirement will be fulfilled by WPs		WP8, WP7
D1.2-8.3	supports	D1.2-3.12, D1.2-3.14
	depends on	D1.2-3.1, D1.2-3.2, D1.2-3.3, D1.2-3.6, D1.2-3.5, D1.2-3.7, D1.2-3.8, D1.2-3.9, D1.2-3.11
	abstracts	
	implements	
	similar to	
	Note	Business process
This requirement will be fulfilled by WPs		WP8, WP3
D1.2-8.4	supports	D1.2-9.7, D1.2-9.11, D1.2-9.14, D1.2-9.15, D1.2-9.16
	depends on	D1.2-3.1, D1.2-3.2, D1.2-3.3
	abstracts	
	implements	
	similar to	
	Note	Generic client
This requirement will be fulfilled by WPs		WP8, WP3
D1.2-8.5	supports	D1.2-9.6, D1.2-9.9, D1.2-7.11
	depends on	D1.2-7.19, D1.2-7.20
	abstracts	
	implements	
	similar to	
	Note	policymanagement
This requirement will be fulfilled by WPs		WP8, WP7, WP5

D1.2-8.6	supports	D1.2-9.7, D1.2-9.16
	depends on	
	abstracts	
	implements	
	similar to	
	Note	repository
This requirement will be fulfilled by WPs		WP8

E.8 Interactions of WP 9

Source Requirement	Interaction Type	Target Requirements
D1.2-9.1	supports	D1.2-2.20, D1.2-2.23, D1.2-12.14, D1.2-12.15
	depends on	D1.2-2.1, D1.2-2.2, , D1.2-2.5, D1.2-3.6, D1.2-3.7, D1.2-3.8, D1.2-3.10, D1.2-6.12, D1.2-7.11, D1.2-8.1, D1.2-8.2
	abstracts	D1.2-2.4, D1.2-8.6
	implements	D1.2-6.6, D1.2-10.8, D1.2-10.9
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP9
D1.2-9.2	supports	D1.2-2.15, D1.2-2.20, D1.2-3.6, D1.2-4.4, D1.2-4.5, D1.2-6.3, D1.2-6.6, D1.2-7.6, D1.2-7.26
	depends on	D1.2-2.11, D1.2-2.12, D1.2-3.14, D1.2-4.1, D1.2-4.8, D1.2-5.9, D1.2-12.13
	abstracts	D1.2-2.14, D1.2-3.11, D1.2-7.7, D1.2-7.11
	implements	
	similar to	D1.2-8.5
	Note	
This requirement will be fulfilled by WPs		WP6, WP7
D1.2-9.3	supports	D1.2-2.12,D1.2-4.3, D1.2-6.12
	depends on	D1.2-5.10, D1.2-7.6, D1.2-7.12, D.12-7.14, D1.27-15
	abstracts	D1.2-2.8, D1.2-2.10, D1.2-2.13, D1.2-4.8, D1.2-7.3
	implements	D1.2-7.3, D1.2-10.6, D1.2-10.7
	similar to	D1.2-7.5
	Note	
This requirement will be fulfilled by WPs		WP7, WP2, WP4
D1.2-9.4	supports	D1.2-2.10, D1.2-2.14, D1.2-2.15, D1.2-2.20, D1.2-3.4, D1.2-4.3, D1.2-6.8,D1.2-6.12, D1.2-7.26, D1.2-10.4, D1.2-10.5, D1.2-12.13
	depends on	D1.2-2.18, D1.2-2.19, D1.2-6.1, D1.2-7.23
	abstracts	D1.2-3.6, D1.2-7.4
	implements	D1.2-2.7, D1.2-12.15
	similar to	D1.2-5.10, D1.2-7.3, D1.2-7.6
	Note	
This requirement will be fulfilled by WPs		WP7, WP2, WP4
D1.2-9.5	supports	D1.2-2.15, D1.2-2.22, D1.2-4.1, D1.2-4.4, D1.2-6.9, D1.2-6.10, D1.2-7.21, D1.2-7.25, D1.2-10.2, D1.2-12.4, D1.2-12.10, D1.2-12.13, D1.2-12.15
	depends on	D1.2-3.4
	abstracts	
	implements	D1.2-2.17
	similar to	D1.2-7.24
	Note	

This requirement will be fulfilled by WPs		WP4, WP7
D1.2-9.6	supports	D1.2-2.11, D1.2-2.14, D1.2-2.20, D1.2-4.1, D1.2-4.4, D1.2-4.5, D1.2-6.4, D1.2-6.6, D1.2-7.1, D1.2-7.23, D1.2-10.4, D1.2-12.15
	depends on	D1.2-4.8, D1.2-7.7, D1.2-12.13
	abstracts	D1.2-2.10, D1.2-3.14, D1.2-7.11
	implements	D1.2-8.5
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP6, WP7
D1.2-9.7	supports	D1.2-2.11, D1.2-2.15, D1.2-4.3, D1.2-6.10, d1.2-7.21
	depends on	D1.2-2.8, D1.2-2.19, D1.2-6.2, D1.2-6.3, D1.2-6.12, D1.2-7.3, D1.2-7.6, D1.2-8.2
	abstracts	
	implements	
	similar to	D1.2-6.8, D1.2-8.6
	Note	
This requirement will be fulfilled by WPs		WP8
D1.2-9.8	supports	D1.2-2.10, D1.2-2.11, D1.2-2.20, D1.2-4.3, D1.2-5.5, D1.2-6.6, D1.2-6.9, D1.2-6.10, D1.2-7.22
	depends on	D1.2-2.13, D1.2-2.17, D1.2-3.11, D1.2-3.15, D1.2-4.1, D1.2-5.10, D1.2-7.6, D1.2-7.16, D1.2-7.24
	abstracts	
	implements	
	similar to	D1.2-2.22, D1.2-6.8
	Note	
This requirement will be fulfilled by WPs		WP7, WP8
D1.2-9.9	supports	D1.2-3.11, D1.2-4.1, D1.2-6.6
	depends on	D1.2-2.9, D1.2-2.10, D1.2-2.11, D1.2-2.14, D1.2-4.8
	abstracts	D1.2-3.15, D1.2-6.7, D1.2-8.5
	implements	D1.2-7.26
	similar to	D1.2-7.7, D1.2-7.11
	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-9.10	supports	D1.2-2.10, D1.2-2.12, D1.2-3.11, D1.2-3.14,
	depends on	
	abstracts	
	implements	D1.2-2.13, D1.2-2.14, D1.2-10.6, D1.2-10.7
	similar to	D1.2-3.3, D1.2-4.8, D1.2-8.4
	Note	
This requirement will be fulfilled by WPs		WP04,WP8, WP10
D1.2-9.11	supports	D1.2-2.2, D1.2-2.4, D1.2-2.10, D1.2-2.13, D1.2-3.12, D1.2-4.1, D1.2-4.2, D1.2-12.13
	depends on	D1.2-3.4, D1.2-6.12, D1.2-7.16, D1.2-8.2, D1.2-8.6,
	abstracts	D1.2-12.27, D1.2-12.28
	implements	D1.2-2.9
	similar to	D1.2-2.23
	Note	
This requirement will be fulfilled by WPs		WP08, WP09, WP12
D1.2-9.12	supports	D1.2-2.10, D1.2-2.11, D1.2-2.13 D1.2-2.17, D1.2-2.20, D1.2-3.6, D1.2-4.1, D1.2-6.6, D1.2-6.8, D1.2-7.2, D1.2-7.3, D1.2-7.6, D1.2-7.22, D1.2-7.26
	depends on	D1.2-2.18, D1.2-2.19
	abstracts	D1.2-7.4, D1.2-7.5, D1.2-7.16
	implements	D1.2-5.10
	similar to	

	Note	
This requirement will be fulfilled by WPs		WP7
D1.2-9.13	supports	D1.2-2.14, D1.2-2.20, D1.2-4.6, D1.2-6.12, D1.2-7.3, D1.2-7.26
	depends on	D1.2-4.3, D1.2-7.4, D1.2-7.5, D1.2-7.15, D1.2-7.16
	abstracts	D1.2-2.7, D1.2-2.16, D1.2-3.10
	implements	
	similar to	D1.2-2.18, D1.2-2.19, D1.2-7.6
	Note	
This requirement will be fulfilled by WPs		WP7, WP8
D1.2-9.14	supports	D1.2-2.4, D1.2-2.10
	depends on	
	abstracts	
	implements	
	similar to	
	Note	May contradict D1.2-2.11
This requirement will be fulfilled by WPs		WP8
D1.2-9.15	supports	D1.2-2.2, D1.2-2.10, D1210.5, D1.2-10.6
	depends on	
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		W2, WP4, WP8, WP10
D1.2-9.16	supports	D1.2-2.15, D1.2-2.16, D1.2-6.3, D1.2-6.12
	depends on	D1.2-8.2, D1.2-8.6
	abstracts	D1.2-6.4
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP8, WP9

E.9 Interactions of WP 10

Source Requirement	**Interaction Type**	**Target Requirements**
D1.2-10.1	supports	D1.2-2.16
	depends on	D1.2-2.1, D1.2-2.2, D1.2-2.5, D1.2-2.6, D1.2-12.1, D1.2-12.11
	abstracts	D1.2-12.9, D1.2-12.14
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		
D1.2-10.2	supports	D1.2-2.16
	depends on	D1.2-2.23, D1.2-5.6, D1.2-7.4 , D1.2-7.6, D1.2-12.11
	abstracts	D1.2-12.14
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10
D1.2-10.3	supports	D1.2-12.14, D1.2-12.15
	depends on	D1.2-2.23
	abstracts	
	implements	

	similar to	
	Note	
This requirement will be fulfilled by WPs		WP2
D1.2-10.8	supports	D1.2-4.7, D1.2-12.14, D1.2-12.15
	depends on	D1.2-2.23
	abstracts	
	implements	D1.2-12.13, D1.2-12.17
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP9, WP8
D1.2-10.9	supports	D1.2-2.16
	depends on	D1.2-2.1, D1.2-2.2
	abstracts	
	implements	D1.2-12.13, D1.2-12.14, D1.2-12.15
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10, WP2
D1.2-10.4	supports	D1.2-5.8
	depends on	D1.2-2.14, D1.2-2.16, D1.2-5.1, D1.2-4.3, D1.2-8.6, D1.2-9.4, D1.2-9.6
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10, WP9
D1.2-10.5	supports	
	depends on	D1.2-2.9, D1.2-4.3, D1.2-9.4, D1.2-9.15
	abstracts	
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10, WP9
D1.2-10.6	supports	D1.2-2.10, D1.2-2.11, D1.2-2.12, D1.2-2.13, D1.2-4.8, D1.2-9.15
	depends on	
	abstracts	D1.2-9.3, D1.2-9.10
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10, WP9
D1.2-10.7	supports	
	depends on	D1.2-2.8, D1.2-8.3, D1.2-8.4, D1.2-8.5
	abstracts	D1.2-9.3, D1.2-9.10
	implements	
	similar to	
	Note	
This requirement will be fulfilled by WPs		WP10, WP9

F Inter-WP Requirements Interaction (Second Iteration)

The following is a depiction of the interaction between the technical requirements after the second iteration of this analysis with all the updated requirements. The inconsistencies are combed out of this list which is presented in the DOT notation, which is interpreted as follows:

"Requirement 1" → "Requirement 2" [label = "Type of interaction"]

The number of "Requirement 1" also indicates the WP that authored the interaction.

F.1 Interactions of WP3

"D1.2-3.1" → "D1.2-5.5" [label = "I"];
"D1.2-3.1" → "D1.2-6.3" [label = "D"];

"D1.2-3.2" → "D1.2-5.5" [label = "I"];
"D1.2-3.2" → "D1.2-6.12" [label = "S"];
"D1.2-3.2" → "D1.2-9.1" [label = "S"];
"D1.2-3.2" → "D1.2-6.2" [label = "D"];
"D1.2-3.2" → "D1.2-8.3" [label = "I"];
"D1.2-3.2" → "D1.2-6.12" [label = "Part. I"];

"D1.2-3.3" → "D1.2-6.10" [label = "S"];

"D1.2-3.5" → "D1.2-7.13" [label = "D"]
"D1.2-3.5" → "D1.2-7.23" [label = "I"];
"D1.2-3.5" → "D1.2-7.29" [label = "D"]
"D1.2-3.6" → "D1.2-7.13" [label = "D"];
"D1.2-3.6" → "D1.2-7.23" [label = "I"];

"D1.2-3.7" → "D1.2-7.13" [label = "D"];
"D1.2-3.7" → "D1.2-7.1" [label = "I"];

"D1.2-3.9" → "D1.2-10.3" [label = "D"];

"D1.2-3.11"→ "D1.2-2.14" [label = "S"];
"D1.2-3.11"→ "D1.2-7.7" [label = "A"];
"D1.2-3.11"→ "D1.2-7.26" [label = "I"];

"D1.2-3.12"→ "D1.2-10.8" [label = "S"];

"D1.2-3.13"→ "D1.2-5.5" [label = "S"];
"D1.2-3.13"→ "D1.2-6.6" [label = "D"];

"D1.2-3.14" → "D1.2-2.23" [label = "I"];
"D1.2-3.14" → "D1.2-10.8" [label = "I"];

"D1.2-3.15" → "D1.2-4.9" [label = "D"];
"D1.2-3.15" → "D1.2-5.1" [label = "D"];

F.2 Interactions of WP4

“D1.2-4.1” → “D1.2-2.9” [label = “S”] ;
“D1.2-4.1” → “D1.2-2.20” [label = “S”];
“D1.2-4.1” → “D1.2-7.7” [label = “I”];
“D1.2-4.1” → “D1.2-7.26” [label = “S”];
“D1.2-4.1” → “D1.2-8.6” [label = “S”];
“D1.2-4.1” → “D1.2-9.2” [label = “S”];
“D1.2-4.1” → “D1.2-9.6” [label = “A”];
“D1.2-4.1” → “D1.2-9.8” [label = “S”];
“D1.2-4.1” → “D1.2-9.9” [label = “S”];
“D1.2-4.1” → “D1.2-2.18” [label = “D”];
“D1.2-4.1” → “D1.2-2.19” [label = “D”];
“D1.2-4.1” → “D1.2-3.1” [label = “A”];

“D1.2-4.2” → “D1.2-7.8” [label = “S”];
“D1.2-4.2” → “D1.2-7.16” [label = “S”];
“D1.2-4.2” → “D1.2-7.18” [label = “S”];
“D1.2-4.2” → “D1.2-7.27” [label = “S”];
“D1.2-4.2” → “D1.2-9.16” [label = “S”];
“D1.2-4.2” → “D1.2-12.27” [label = “S”];
“D1.2-4.2” → “D1.2-3.4” [label = “A”];

“D1.2-4.3” → “D1.2-2.1” [label = “S”];
“D1.2-4.3” → “D1.2-2.5” [label = “S”];
“D1.2-4.3” → “D1.2-2.6” [label = “S”];
“D1.2-4.3” → “D1.2-3.7” [label = “S”];
“D1.2-4.3” → “D1.2-12.1” [label = “S”];

“D1.2-4.4” → “D1.2-2.11” [label = “S”];
“D1.2-4.4” → “D1.2-2.12” [label = “S”];
“D1.2-4.4” → “D1.2-2.14” [label = “S”];
“D1.2-4.4” → “D1.2-7.1” [label = “S”];
“D1.2-4.4” → “D1.2-7.6” [label = “S”];
“D1.2-4.4” → “D1.2-2.10” [label = “S”];
“D1.2-4.4” → “D1.2-2.15” [label = “S”];
“D1.2-4.4” → “D1.2-2.22” [label = “S”];
“D1.2-4.4” → “D1.2-3.3” [label = “S”];
“D1.2-4.4” → “D1.2-3.7” [label = “S”];
“D1.2-4.4” → “D1.2-7.14” [label = “S”];
“D1.2-4.4” → “D1.2-7.21” [label = “S”];
“D1.2-4.4” → “D1.2-7.24” [label = “S”];
“D1.2-4.4” → “D1.2-7.25” [label = “S”];
“D1.2-4.4” → “D1.2-9.5” [label = “A”];
“D1.2-4.4” → “D1.2-9.16” [label = “S”];
“D1.2-4.4” → “D1.2-9.17” [label = “S”];
“D1.2-4.4” → “D1.2-2.18” [label = “D”];
“D1.2-4.4” → “D1.2-2.19” [label = “D”];
“D1.2-4.4” → “D1.2-2.17” [label = “A”];
“D1.2-4.4” → “D1.2-3.12” [label = “A”];
“D1.2-4.4” → “D1.2-7.3” [label = “A”];

“D1.2-4.5” → “D1.2-2.11” [label = “S”];
“D1.2-4.5” → “D1.2-2.12” [label = “S”];
“D1.2-4.5” → “D1.2-2.14” [label = “S”];
“D1.2-4.5” → “D1.2-2.9” [label = “S”];

“D1.2-4.5” → “D1.2-2.10” [label = “S”];
“D1.2-4.5” → “D1.2-2.20” [label = “S”];
“D1.2-4.5” → “D1.2-3.7” [label = “S”];
“D1.2-4.5” → “D1.2-3.12” [label = “S”];
“D1.2-4.5” → “D1.2-3.15” [label = “S”];
“D1.2-4.5” → “D1.2-9.16” [label = “S”];
“D1.2-4.5” → “D1.2-9.22” [label = “S”];
“D1.2-4.5” →“D1.2-2.18” [label = “D”];
“D1.2-4.5” → “D1.2-2.19” [label = “D”];
“D1.2-4.5” → “D1.2-2.21” [label = “A”];
“D1.2-4.5” → “D1.2-7.24” [label = “A”];

“D1.2-4.6” → “D1.2-3.10” [label = “S”];
“D1.2-4.6” → “D1.2-2.18” [label = “D”];
“D1.2-4.6” → “D1.2-2.19” [label = “D”];

“D1.2-4.7” → “D1.2-2.5” [label = “S”];
“D1.2-4.7” → “D1.2-2.10” [label = “S”];
“D1.2-4.7” → “D1.2-2.11” [label = “S”];
“D1.2-4.7” → “D1.2-2.12” [label = “S”];
“D1.2-4.7” → “D1.2-3.14” [label = “A”];

“D1.2-4.8” → “D1.2-2.11” [label = “S”];
“D1.2-4.8” → “D1.2-2.12” [label = “S”];
“D1.2-4.8” → “D1.2-2.10” [label = “S”];
“D1.2-4.8” → “D1.2-2.13” [label = “S”];
“D1.2-4.8” → “D1.2-3.3” [label = “S”];
“D1.2-4.8” → “D1.2-9.3” [label = “S”];
“D1.2-4.8” → “D1.2-9.14” [label = “S”];

“D1.2-4.9” → “D1.2-5.1” [label = “S”];
“D1.2-4.9” → “D1.2-2.10” [label = “S”];
“D1.2-4.9” → “D1.2-5.3” [label = “S”];
“D1.2-4.9” → “D1.2-5.4” [label = “S”];

F.3 Interactions of WP5

“D1.2-5.1” → “D1.2-9.21” [label = “S”];
“D1.2-5.1” → “D1.2-9.22” [label = “S”];
“D1.2-5.4” → “D1.2-10.11” [label = “S”];
“D1.2-5.5” → “D1.2-3.1” [label = “D”];
“D1.2-5.5” → “D1.2-3.13” [label = “D”];

“D1.2-5.6” → “D1.2-7.12” [label = “D”];
“D1.2-5.6” → “D1.2-7.15” [label = “D”];
“D1.2-5.6” → “D1.2-7.13” [label = “D”];

“D1.2-5.9” → “D1.2-2.12” [label = “S”];
“D1.2-5.9” → “D1.2-2.13” [label = “S”];
“D1.2-5.9” → “D1.2-4.3” [label = “S”];
“D1.2-5.9” → “D1.2-8.4” [label = “S”];
“D1.2-5.9” → “D1.2-9.6” [label = “S”];
“D1.2-5.9” → “D1.2-7.13” [label = “I”];

“D1.2-5.10” → “D1.2-7.3” [label = “I”];

F.4 Interactions of WP7

“D1.2-7.1” → “D1.2-3.7” [label = “A”];

“D1.2-7.3” → “D1.2-5.10” [label=“A”];
“D1.2-7.3” → “D1.2-9.16” [label=“S”];
“D1.2-7.3” → “D1.2-9.17” [label=“S”];
“D1.2-7.3” → “D1.2-9.18” [label=“S”];
“D1.2-7.3” → “D1.2-9.19” [label=“S”];
“D1.2-7.3” → “D1.2-9.20” [label=“S”];
“D1.2-7.3” → “D1.2-9.21” [label=“S”];

“D1.2-7.6” → “D1.2-2.20” [label=“S”];
“D1.2-7.6” → “D1.2-4.5” [label=“S”];
“D1.2-7.6” → “D1.2-9.1” [label=“S”];
“D1.2-7.6” → “D1.2-9.22” [label=“S”];
“D1.2-7.6” → “D1.2-9.23” [label=“A”];

“D1.2-7.7” → “D1.2-3.11” [label=“S”];
“D1.2-7.7” → “D1.2-4.1” [label=“A”];
“D1.2-7.7” → “D1.2-9.2” [label=“S”];
“D1.2-7.7” → “D1.2-9.6” [label=“A”];
“D1.2-7.7” → “D1.2-9.8” [label=“S”];
“D1.2-7.7” → “D1.2-9.12” [label=“S”];

“D1.2-7.9” → “D1.2-3.10” [label=“S”];

“D1.2-7.11” → “D1.2-9.17” [label=“A”];

“D1.2-7.12” → “D1.2-5.6” [label=“S”];
“D1.2-7.12” → “D1.2-9.3” [label=“S”];

“D1.2-7.13” → “D1.2-5.6” [label=“S”];
“D1.2-7.13” → “D1.2-9.3” [label=“S”];

“D1.2-7.15” → “D1.2-5.6” [label=“S”];

“D1.2-7.17” → “D1.2-5.6” [label=“S”];

“D1.2-7.19” → “D1.2-3.6” [label=“S”];
“D1.2-7.19” → “D1.2-3.7” [label=“S”];
“D1.2-7.19” → “D1.2-3.13” [label=“S”];

“D1.2-7.20” → “D1.2-3.6” [label=“S”];
“D1.2-7.20” → “D1.2-3.7” [label=“S”];

“D1.2-7.24” → “D1.2-9.5” [label=“S”];

“D1.2-7.27” → “D1.2-3.8” [label=“S”];

F.5 Interactions of WP8

“D1.2-8.1” → “D1.2-2.3” [label=“S”];
“D1.2-8.1” → “D1.2-2.4” [label=“S”];
“D1.2-8.1” → “D1.2-2.5” [label=“S”];
“D1.2-8.1” → “D1.2-2.6” [label=“S”];
“D1.2-8.1” → “D1.2-2.9” [label=“S”];
“D1.2-8.1” → “D1.2-2.13” [label=“S”];
“D1.2-8.1” → “D1.2-9.2” [label=“S”];
“D1.2-8.1” → “D1.2-9.14” [label=“S”];
“D1.2-8.1” → “D1.2-3.12” [label=“S”];
“D1.2-8.1” → “D1.2-3.14” [label=“S”];
“D1.2-8.1” → “D1.2-7.18” [label=“S”];
“D1.2-8.1” → “D1.2-2.21” [label=“D”];
“D1.2-8.1” → “D1.2-2.23” [label=“D”];
“D1.2-8.1” → “D1.2-7.2” [label=“D”];
“D1.2-8.1” → “D1.2-7.1” [label=“D”];
“D1.2-8.1” → “D1.2-7.3” [label=“D”];
“D1.2-8.1” → “D1.2-7.6” [label=“D”];
“D1.2-8.1” → “D1.2-7.14” [label=“D”];

“D1.2-8.2” → “D1.2-7.18” [label=“S”];

“D1.2-8.3” → “D1.2-3.12” [label=“S”];
“D1.2-8.3” → “D1.2-3.14” [label=“S”];
“D1.2-8.3” → “D1.2-3.1” [label=“D”];
“D1.2-8.3” → “D1.2-3.2” [label=“D”];
“D1.2-8.3” → “D1.2-3.3” [label=“D”];
“D1.2-8.3” → “D1.2-3.6” [label=“D”];
“D1.2-8.3” → “D1.2-3.5” [label=“D”];
“D1.2-8.3” → “D1.2-3.7” [label=“D”];
“D1.2-8.3” → “D1.2-3.8” [label=“D”];
“D1.2-8.3” → “D1.2-3.9” [label=“D”];
“D1.2-8.3” → “D1.2-3.11” [label=“D”];

“D1.2-8.4” → “D1.2-9.14” [label=“S”];
“D1.2-8.4” → “D1.2-9.16” [label=“S”];
“D1.2-8.4” → “D1.2-3.1” [label=“D”];
“D1.2-8.4” → “D1.2-3.2” [label=“D”];
“D1.2-8.4” → “D1.2-3.3” [label=“D”];

“D1.2-8.6” → “D1.2-9.16” [label=“S”];

F.6 Interactions of WP9

“D1.2-9.1” → “D1.2-2.20” [label = “S”];
“D1.2-9.1” → “D1.2-2.23” [label = “S”];
“D1.2-9.1” → “D1.2-2.14” [label = “S”];
“D1.2-9.1” → “D1.2-2.15” [label = “S”];
“D1.2-9.1” → “D1.2-3.6” [label = “D”];
“D1.2-9.1” → “D1.2-3.7” [label = “D”];
“D1.2-9.1” → “D1.2-3.8” [label = “D”];
“D1.2-9.1” → “D1.2-3.10” [label = “D”];
“D1.2-9.1” → “D1.2-2.1” [label = “D”];

“D1.2-9.1” → “D1.2-2.2” [label = “D”];
“D1.2-9.1” → “D1.2-2.5” [label = “D”];
“D1.2-9.1” → “D1.2-6.12” [label = “D”];
“D1.2-9.1” → “D1.2-7.11” [label = “D”];
“D1.2-9.1” → “D1.2-8.1” [label = “D”];
“D1.2-9.1” → “D1.2-8.2” [label = “D”];
“D1.2-9.1” → “D1.2-2.4” [label =“A”];
“D1.2-9.1” → “D1.2-8.6” [label =“A”];
“D1.2-9.1” → “D1.2-6.6” [label=“I”];
“D1.2-9.1” → “D1.2-10.8” [label=“I”];
“D1.2-9.1” → “D1.2-10.9” [label=“I”];

“D1.2-9.2” → “D1.2-2.15” [label=“S”];
“D1.2-9.2” → “D1.2-2.20” [label=“S”];
“D1.2-9.2” → “D1.2-3.6” [label=“S”];
“D1.2-9.2” → “D1.2-4.4” [label=“S”];
“D1.2-9.2” → “D1.2-4.5” [label=“S”];
“D1.2-9.2” → “D1.2-6.3” [label=“S”];
“D1.2-9.2” → “D1.2-6.6” [label=“S”];
“D1.2-9.2” → “D1.2-7.6” [label=“S”];
“D1.2-9.2” → “D1.2-7.26” [label=“S”];
“D1.2-9.2” → “D1.2-2.11” [label =“D”];
“D1.2-9.2” → “D1.2-2.12” [label =“D”];
“D1.2-9.2” → “D1.2-3.14” [label =“D”];
“D1.2-9.2” → “D1.2-4.1” [label =“D”];
“D1.2-9.2” → “D1.2-4.8” [label =“D”];
“D1.2-9.2” → “D1.2-5.9” [label =“D”];
“D1.2-9.2” → “D1.2-12.13” [label =“D”];
“D1.2-9.2” → “D1.2-2.14” [label=“A”];
“D1.2-9.2” → “D1.2-3.11” [label=“A”];
“D1.2-9.2” → “D1.2-7.7” [label=“A”];
“D1.2-9.2” → “D1.2-7.11” [label=“A”];

“D1.2-9.3” → “D1.2-2.12” [label=“S”];
“D1.2-9.3” → “D1.2-4.3” [label=“S”];
“D1.2-9.3” → “D1.2-6.12” [label=“S”];
“D1.2-9.3” → “D1.2-7.3” [label=“I”];

“D1.2-9.5”→“D1.2-2.15” [label=“S”];
“D1.2-9.5”→“D1.2-2.22” [label=“S”];
“D1.2-9.5”→“D1.2-4.4” [label=“I”];
“D1.2-9.5”→“D1.2-6.9” [label=“S”];
“D1.2-9.5”→“D1.2-6.10” [label=“S”];
“D1.2-9.5”→“D1.2-7.21” [label=“S”];
“D1.2-9.5”→“D1.2-7.25” [label=“S”];
“D1.2-9.5”→“D1.2-10.2” [label=“S”];
“D1.2-9.5”→“D1.2-12.4” [label=“S”];
“D1.2-9.5”→“D1.2-12.10” [label=“S”];
“D1.2-9.5”→“D1.2-12.13” [label=“S”];
“D1.2-9.5”→“D1.2-12.15” [label=“S”];
“D1.2-9.5”→“D1.2-3.4” [label=“S”];
“D1.2-9.5”→“D1.2-2.17” [label=“I”];

“D1.2-9.6”→“D1.2-2.11” [label=“S”];
“D1.2-9.6”→“D1.2-2.14” [label=“S”];
“D1.2-9.6”→“D1.2-2.20” [label=“S”];
“D1.2-9.6”→“D1.2-4.1” [label=“I”];

“D1.2-9.6”→“D1.2-4.4” [label=“S”];
“D1.2-9.6”→“D1.2-4.5” [label=“S”];
“D1.2-9.6”→“D1.2-6.4” [label=“S”];
“D1.2-9.6”→“D1.2-6.6” [label=“S”];
“D1.2-9.6”→“D1.2-7.1” [label=“S”];
“D1.2-9.6”→“D1.2-7.23” [label=“S”];
“D1.2-9.6”→“D1.2-12.15” [label=“S”];
“D1.2-9.6”→“D1.2-4.8” [label=“D”];
“D1.2-9.6”→“D1.2-7.7” [label=“I”];
“D1.2-9.6”→“D1.2-12.13” [label=“D”];
“D1.2-9.6”→“D1.2-2.10” [label=“A”];
“D1.2-9.6”→“D1.2-3.14” [label=“A”];
“D1.2-9.6”→“D1.2-7.11” [label=“A”];

“D1.2-9.8”→“D1.2-2.10” [label=“S”];
“D1.2-9.8”→“D1.2-2.11” [label=“S”];
“D1.2-9.8”→“D1.2-2.20” [label=“S”];
“D1.2-9.8”→“D1.2-4.3” [label=“S”];
“D1.2-9.8”→“D1.2-5.5” [label=“S”];
“D1.2-9.8”→“D1.2-6.6” [label=“S”];
“D1.2-9.8”→“D1.2-6.9” [label=“S”];
“D1.2-9.8”→“D1.2-6.10” [label=“S”];
“D1.2-9.8”→“D1.2-4.6” [label=“S”];
“D1.2-9.8”→“D1.2-7.28” [label=“S”];
“D1.2-9.8”→“D1.2-2.13” [label=“D”];
“D1.2-9.8”→“D1.2-2.17” [label=“D”];
“D1.2-9.8”→“D1.2-3.11” [label=“D”];
“D1.2-9.8”→“D1.2-3.15” [label=“D”];
“D1.2-9.8”→“D1.2-4.1” [label=“D”];
“D1.2-9.8”→“D1.2-5.10” [label=“D”];
“D1.2-9.8”→“D1.2-7.6” [label=“D”];
“D1.2-9.8”→“D1.2-7.16” [label=“D”];
“D1.2-9.8”→“D1.2-7.24” [label=“D”];

“D1.2-9.9”→“D1.2-3.11” [label=“S”];
“D1.2-9.9”→“D1.2-4.1” [label=“D”];
“D1.2-9.9”→“D1.2-6.6” [label=“S”];

“D1.2-9.9”→“D1.2-2.9” [label=“D”];
“D1.2-9.9”→“D1.2-2.10” [label=“D”];
“D1.2-9.9”→“D1.2-2.11” [label=“D”];
“D1.2-9.9”→“D1.2-2.14” [label=“D”];
“D1.2-9.9”→“D1.2-4.8” [label=“D”];
“D1.2-9.9”→“D1.2-7.28” [label=“D”];
“D1.2-9.9”→“D1.2-3.15” [label=“A”];
“D1.2-9.9”→“D1.2-6.7” [label=“A”];
“D1.2-9.9”→“D1.2-7.26” [label=“I”];

“D1.2-9.12”→“D1.2-2.10” [label=“S”];
“D1.2-9.12”→“D1.2-2.11” [label=“S”];
“D1.2-9.12”→“D1.2-2.13” [label=“S”];
“D1.2-9.12”→“D1.2-2.17” [label=“S”];
“D1.2-9.12”→“D1.2-2.20” [label=“S”];
“D1.2-9.12”→“D1.2-3.6” [label=“S”];
“D1.2-9.12”→“D1.2-6.6” [label=“S”];
“D1.2-9.12”→“D1.2-6.8” [label=“S”];
“D1.2-9.12”→“D1.2-7.2” [label=“S”];

“D1.2-9.12”→“D1.2-7.3” [label=“S”];
“D1.2-9.12”→“D1.2-7.6” [label=“S”];
“D1.2-9.12”→“D1.2-4.6” [label=“S”];
“D1.2-9.12”→“D1.2-7.26” [label=“S”];
“D1.2-9.12”→“D1.2-2.18” [label=“D”];
“D1.2-9.12”→“D1.2-2.19” [label=“D”];
“D1.2-9.12”→“D1.2-7.4” [label=“A”];
“D1.2-9.12”→“D1.2-7.5” [label=“A”];
“D1.2-9.12”→“D1.2-7.16” [label=“A”];
“D1.2-9.12”→“D1.2-5.10” [label=“I”];

“D1.2-9.14”→“D1.2-2.4” [label=“S”];
“D1.2-9.14”→“D1.2-2.10” [label=“S”];
“D1.2-9.14”→“D1.2-2.11” [label=”C”];

“D1.2-9.16”→“D1.2-2.15” [label=“S”];
“D1.2-9.16”→“D1.2-2.16” [label=“S”];
“D1.2-9.16”→“D1.2-6.3” [label=“S”];
“D1.2-9.16”→“D1.2-6.12” [label=“S”];
“D1.2-9.16”→“D1.2-8.2” [label=“D”];
“D1.2-9.16”→“D1.2-8.6” [label=“D”];
“D1.2-9.16”→“D1.2-6.4” [label=“A”];
“D1.2-9.16”→“D1.2-2.16” [label=“S”];

F.7 Interactions of WP10

“D1.2-10.1”→“D1.2-2.1” [label=“D”];
“D1.2-10.1”→“D1.2-2.2” [label=“D”];
“D1.2-10.1”→“D1.2-2.5” [label=“D”];
“D1.2-10.1”→“D1.2-2.6” [label=“D”];
“D1.2-10.1”→“D1.2-12.1” [label=“D”];
“D1.2-10.1”→“D1.2-12.11” [label=“D”];
“D1.2-10.1”→“D1.2-12.9” [label=“A”];
“D1.2-10.1”→“D1.2-12.14” [label=“A”];
“D1.2-10.2”→“D1.2-2.16” [label=“S”];
“D1.2-10.2”→“D1.2-2.23” [label=“D”];
“D1.2-10.2”→“D1.2-5.6” [label=“D”];
“D1.2-10.2”→“D1.2-7.4 ” [label=“D”];
“D1.2-10.2”→“D1.2-7.6” [label=“D”];
“D1.2-10.2”→“D1.2-12.11” [label=“D”];
“D1.2-10.2”→“D1.2-12.14” [label=“A”];

“D1.2-10.3”→“D1.2-12.14” [label=“S”];
“D1.2-10.3”→“D1.2-12.15” [label=“S”];
“D1.2-10.3”→“D1.2-2.23” [label=“D”];

“D1.2-10.8”→“D1.2-4.7” [label=“S”];
“D1.2-10.8”→“D1.2-12.14” [label=“S”];
“D1.2-10.8”→“D1.2-12.15” [label=“S”];
“D1.2-10.8”→“D1.2-2.23” [label=“D”];
“D1.2-10.8”→“D1.2-12.13” [label=“I”];
“D1.2-10.8”→“D1.2-12.17” [label=“I”];

“D1.2-10.9”→“D1.2-2.16” [label=“S”];

“D1.2-10.9”→“D1.2-2.1” [label=“D”];
“D1.2-10.9”→“D1.2-2.2” [label=“D”];
“D1.2-10.9”→“D1.2-12.13” [label=“I”];
“D1.2-10.9”→“D1.2-12.14” [label=“I”];
“D1.2-10.9”→“D1.2-12.15” [label=“I”];