

SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies



Trusted Architecture for Securely Shared Services

Document Type: Deliverable

Title: **TAS³ Design Requirements**

Work Package: WP1

Deliverable Nr: D1.4

Dissemination: Public,

Preparation Date: December 31 2011

Version: 4.0

Legal Notice

All information included in this document is subject to change without notice. The Members of the TAS³ Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the TAS³ Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.



The TAS³ Consortium

Benef. Nr	Beneficiary name	Benef. short name	Country	Date enter project	Date exit project
1	Katholieke Universiteit Leuven (Proj. Coord)	KUL	BE	M1	M48
2	Synergetics nv/sa	SYN	BE	M1	M48
3	University of Kent	KENT	UK	M1	M48
4	University of Karlsruhe	KARL	DE	M1	M48
5	Technical University Eindhoven	TU/E	NL	M1	M48
6	Consiglio Nazionale delle Ricerche	CNR	IT	M1	M48
7	University of Koblenz-Landau	UNIKOLD	DE	M1	M48
8	Vrije Universiteit Brussel	VUB	BE	M1	M48
9	University of Zaragoza	UNIZAR	ES	M1	M48
10	University of Nottingham	NOT	UK	M1	M48
11	SAP research (S&T Coord.)	SAP	DE	M1	M48
12	Eifel asbl	EIF	FR	M1	M30
13	Intalio Ltd	INT	UK	M1	M18
14	Risaris Ltd	RIS	IR	M1	M48
15	Kenteq	KETQ	NL	M1	M48
16	Oracle	ORACLE	NL	M1	M48
17	Custodix nv/sa	CUS	BE	M1	M48
18	Medisoftware bv	MEDI	NL	M1	M12
19	Karlsruhe Institute of Technology (KIT)	KARL	DE	M1	M48
20	Sym Labs SA	SYM	PT	M18	M30

Contributors

	Name	Organisation
1	Magali Seguran, Julien Massiera, Gilles Montagnon	SAP
2	Seda Guerses	KU Leuven
3	Andreas Paschalidis	KU Leuven
4	David Chadwick	University of Kent
5	Jutta Mülle, Christian Hütter	University of Karlsruhe
6	Jerry den Hartog	Eindhoven University of
7	Guglielmo De Angelis	CNR/ISTI
8	Marc Santos	University of Koblenz-Landau
9	Carlos Flavian	University of Zaragoza
10	Sandra Winfield	University of Nottingham
11	Sampo Kellomäki	Sym Labs
12	Marc Van Coillie	Eiffel

13	Luk Vervenne	Synergetics
14	Brendan Van Alsenoy	K.U.Leuven
15	Quentin Reul	VUB
16	Lex Polman, Dries Pruis	Kenteq

Contents

1 EXECUTIVE SUMMARY	7
2 INTRODUCTION.....	8
2.1 SCOPE AND OBJECTIVES	8
2.2 DOCUMENT OVERVIEW	9
3 SCENARIOS FOR DEMONSTRATORS.....	11
3.1 ACCREDITATION OF PRIOR LEARNING (APL).....	11
3.1.1 Actors	12
3.1.2 Business risk analysis	12
3.1.3 Secure Tropos trust model.....	13
3.1.4 Process.....	15
3.1.5 Step-by-step description	16
3.2 MASS LAYOFF SCENARIO	17
3.2.1 Actors	17
3.2.2 Business risk analysis	18
3.2.3 Secure Tropos trust model.....	19
3.2.4 Processes	21
3.2.5 Step-by-step description	22
3.3 STUDENT WORK PLACEMENT	24
3.3.1 Actors	25
3.3.2 Business risk analysis	25
3.3.3 Secure Tropos trust model.....	27
3.3.4 Processes	28
3.3.5 Step-by-step description	28
3.4 EMERGENCY ADMISSION FOLLOWING AN ACCIDENT ON THE ROAD	30
3.4.1 Actors	31
3.4.2 Business risk analysis	31
3.4.3 Secure Tropos trust model.....	33
3.4.4 Process.....	34
3.4.5 Step-by-step description	34
4 DESIGN REQUIREMENTS	36
4.1 BUSINESS PROCESS	36
4.2 TRUST REQUIREMENTS.....	37
4.3 IDENTITY MANAGEMENT, AUTHENTICATION AND AUTHORISATION	39
4.4 "TRUSTED APPLICATION INFRASTRUCTURE"	40
5 ARCHITECTURAL AND TECHNICAL DESIGN REQUIREMENTS .	41
5.1 BUSINESS PROCESS	41
5.1.1 Architectural.....	41
5.2 IDENTITY MANAGEMENT, AUTHENTICATION AND AUTHORIZATION	42

5.2.1 Architectural	42
5.2.2 Dependencies	43
5.3 TRUST	43
5.3.1 Dependencies	44
5.4 TRUSTED APPLICATION INFRASTRUCTURE	45
5.4.1 Architectural	45
5.4.2 Dependencies	45
5.5 INTEGRATION REQUIREMENTS	45
6 LEGAL REQUIREMENTS	47
6.1 ENROLMENT AND CONTRACTUAL BINDING	49
6.2 ASSIGNMENT OF ROLES AND RESPONSIBILITIES	50
6.3 LEGITIMACY OF PROCESSING	51
6.4 FINALITY	51
6.5 DATA MINIMIZATION	52
6.6 DATA ACCURACY	54
6.7 CONFIDENTIALITY AND SECURITY OF PROCESSING	55
6.8 TRANSPARENCY AND NOTICE	57
6.8.1 Direct collection	57
6.8.2 Indirect collection.....	58
6.8.3 Implementation.....	59
6.9 DATA SUBJECT RIGHTS OF ACCESS, RECTIFICATION, BLOCKING AND ERASURE	60
6.9.1 Right of access.....	60
6.9.2 Rectification, blocking and erasure	61
6.9.3 Notification to third parties.....	61
6.9.4 Implementation.....	61
6.10 ACCOUNTABILITY AND COMPLIANCE VERIFICATION	62
6.10.1 Logging.....	62
6.10.2 Audit & oversight.....	63
6.10.3 Other accountability mechanisms	63
6.10.4 Complaint handling	64
6.11 NOTIFICATION & PRIOR CHECKING	64
7 ON-LINE COMPLIANCE TESTING	66
7.1 ON-LINE COMPLIANCE TESTING	66
7.1.1 Requirements for the TAS ³ Infrastructure	66
7.1.2 Requirements on the TAS ³ Infrastructure Registry Component.....	67
7.1.3 Requirements on Services deployed over the TAS ³ Infrastructure ...	67
7.2 OFF-LINE TESTING PHASE	68
7.2.1 Testing of XML-based interchange and communication formats	68

7.2.2 Testing of response-time and availability of services (optional requirements).....	68
8 GLOSSARY.....	69
9 REFERENCES	71
10 ANNEXES.....	73
10.1 MODELLING WITH SECURE TROPOS.....	73
10.1.1 The Key Concepts	73

1 Executive summary

The objective of this deliverable is defined in the DoW [4] as “modelling the legal framework and regulatory compliance requirements; collecting and defining the application domain and user requirements from test beds; and, defining the system requirements for all TAS³ components according to software engineering specification standards.”

WP01 “Design Requirements” (D1.4) has been updated concurrently with the “Requirements Report (D1.2)”. Whereas “Design Requirements” links in detail scenario and design requirements, the “Requirement Report” focuses on unsolved problems. Both “Requirement Report” and “Design Requirements” are cross-referenced to provide refinement, support or additional information. The “Design Requirements” document and the “Requirements Report” takes as input the “State of the Art” (D1.1) and “Pilots Specifications and Use Case Scenarios” (D9.1) to ensure that the future design is achievable and consistent with TAS³’s expectations. These Design Requirements directly impact the Architecture Design (D2.1) and must be fulfilled within the future framework’s architecture. “Requirement Reports” and “Design Requirements” are the outcome of multiple meetings and discussions involving all partners.

To give a wider approach and a better understanding, specific Legal Requirements have been included. Legal aspects have been checked in relevant Design Requirements, however describing specific legal issues in the design document gives better visibility of what should be part of contractual agreements or IT solutions. The same approach has been taken for Technical Validation, which defines requirements to ensure that the framework will be testable.

A complete Risk Analysis of the whole TAS³ project is provided as an annex to deliverable D2.1. The second iteration of this document was submitted in March 2010 and provided a list of necessary features for the TAS³ architecture. The included Design Requirements are derived from a set of scenarios selected as having the most common requirements among the different demonstrators’ domains.

This third iteration submitted in December 2010 contains an update of the scenarios for which a complete analysis has been redone. The document contains fresh detailed scenarios. Major updates are provided for “APL”, “Mass-Layoff” and “UK employability” scenarios, which are presented in a separate part. These revised scenarios reflect the development of WP09 work with Employability stakeholders for the demonstrator and pilot work for the project. For the “Emergency Admission” scenario only a minor update has been provided.

In this final iteration submitted for December 2011, following the request of the reviewers, we have retained only the final versions of detailed scenarios and updated the requirements accordingly to ensure a global and final coherence in the document.

2 Introduction

2.1 Scope and objectives

The primary objective of this document is to elicit and specify the requirements for each scenario.

These scenarios are:

- NL Employability: Accreditation of Prior Learning and Mass Layoff (Kenteq)
- UK Employability: Student work placement (Nottingham)
- e-Health: Emergency admission (Custodix)

Furthermore, it also provides the refinement and, in some cases, an extension of the scenario story, thereby painting a clearer picture of the scenario itself. Requirements are used as inputs for the design phases of the system development process. In order to elicit and specify the security and trust requirements, we adopt classical software engineering approaches [1][2][3].

Requirements provide descriptions of the problems rather than specifications of the possible solutions to the problems. As an example, we avoid describing the security mechanisms (e.g., digital signature) as a requirement since it is a service fulfilling a requirement and not a requirement itself (for instance an appropriate requirement would be, “the information in the Customer Information File shall not be shown without customer authorization”).

A requirement is expressed as a sentence in natural language representing a single logical statement. Ideally, it should be simple and precise enough so that it is not possible to break it down. As a rule, a requirement might contain parts that describe a “cause” and an “effect” namely “if something happens, then react as follows”. Many processes in the development phase of a product depend on the quality of the requirements. As a consequence requirements must be easily understandable so as to avoid ambiguity and prevent misinterpretation by the people that will use them. Writing quality requirements implies separation multiple requirements that may have been aggregated in one single statement. Even more important, it must be testable to see if each requirement has been met. We can devise tests or use other verification approaches, such as inspection or demonstration, to determine whether each requirement is properly implemented in the product. If a requirement is not objectively verifiable, determining whether it was correctly implemented or not is a matter of human interpretation and this can endanger the entire development phase. Requirements that are not consistent, feasible, and unambiguously specified are not objectively verifiable.

The specification of requirements is a difficult but well-known process. The methodology behind it has been improved over time and a standard terminology language has been proposed. According to this language each sentence written to express a requirement must contain some keywords. The keywords to be used are:

“SHALL” or “MUST”: this feature is mandatory and will be tested,

“SHOULD”: this feature is appreciated but not mandatory,
 “NOTE”: it could be used in order to better explain a requirement,
 “AUTOMATICALLY/MANUALLY”: it could make a requirement clearer.

On the contrary the following keywords are not acceptable in a requirement: “MAY”, “MAYBE”, “POSSIBLY”, “WILL” as they may introduce some uncertainty.

2.2 Document overview

The rest of this document is articulated in two main sections:

Scenarios from demonstrators: these scenarios contain the updated requirements from the latest iteration of the WP09 demonstrators.

As with the original version of this document, these scenarios contain the requirements from the WP09 demonstrators with a summary which briefly explains what happens in the scenario. It then presents:

- A description of the actors and their respective tasks: This activity consists of identifying the main stakeholders of the scenario along with the roles they play and the tasks that they have to perform.
- A business risk analysis. This activity consists of identifying the threats that may compromise the security of the system. In particular, along the lines given in [10][11][13], we analysed the situations in which actors become malicious and assessed the potential consequences of their actions. This activity served as a starting point for security risk analysis, which was then executed by another workpackage.

A Secure Tropos model of the scenario (described in D1.1 State of the Art). Secure Tropos notation is described in Annexes 10.1. *SI** /Secure Tropos is a formal framework and a methodology for modelling and analysing security requirements [12]. The main advantages of the Tropos methodology is that it allows capture of not only the *what* or the *how*, but also the *why* a piece of software is developed. This, in turn, allows for a more refined analysis of the system dependencies and, in particular, for a much better and uniform treatment not only of the system functional requirements, but also of its non-functional requirements. This methodology has been used to analyse and refine (security) dependencies among scenario stakeholders; however, due to its static nature, the analysis of temporal aspects was not possible. To overcome this limitation, UML sequence diagrams have been used to analyse the interactions among scenario stakeholders for sequences of activities that may lead to security problems.

- The sequence diagram of the scenario (the tool used is Enterprise Architect 7). A step-by-step description which presents the various steps to be performed under the scenario. Each step gives additional information that is used to elicit requirements. Scenario and processes are

fully described in the demonstrator's deliverables for more details (see D9.1).

Capturing requirements: This activity was achieved using classical RE approaches [1][2][3]. We defined detailed guidelines for the specification of requirements which included: a controlled vocabulary (shall, should, and must), describing problems instead of solutions, disjoining amalgamated requirements, etc.

- **Design requirements**, a list of requirements that will be elucidated using the methodology (Classic engineering approach) that has been briefly detailed above.
- **Architectural and Technical Design Requirements** will focus on the framework's overall requirements as well as requirements' dependencies.
- **Legal Requirements** will provide a comprehensive understanding of legal issues. These have an impact on the design and so are described in this document. Other design requirements have been cross-checked for legal issues.
- **Technical Validation Requirements** for the testing phase. These requirements are dependent on the framework rather than the demonstrator scenarios.

Many concepts and solutions used in this document are described in detail in the "State of the Art" (D1.1) or in the "Requirements assessments report" (D1.2) from WP01.

3 Scenarios for demonstrators

This chapter outlines the latest revisions to the scenarios “Accreditation of Prior Learning”, “Mass layoff”, “Student Work Placement” and “Emergency Admission.

3.1 Accreditation of Prior Learning (APL)

We chose to describe new variants of the use cases APL and Mass layoff because these scenarios are also used in the third iteration of D9.1 to demonstrate the functionalities of the TAS³ infrastructure. Thus we ensure that a good match is obtained between the demos and the design requirements.

Compared to the previous one, this APL scenario does not use a branch office. This feature is in this scenario replaced by an employability provider.

Description of the Use Case scenario APL:

1. A company wants employees to develop themselves.
2. All employees are given the opportunity to do an employability scan.
3. The employability scan is executed by an employability provider.
4. One employee wants to do an APL.
5. Therefore he searches for a trusted APL provider
6. The employee selects Kenteq as APL provider
7. His employability data (from de scan) are exchange to Kenteq
8. Kenteq executes the APL process.
9. The APL results are exchanged with his ePortfolio
10. In his ePortfolio he describes his Personal Development Plan.

3.1.1 Actors

Scenario Actor	Person	Task
Company	HR manager	Wants to promote the development of the staff
End user	Employee	Wants to develop himself
Employability Provider	Employability coach	Helps to do the employability scan
APL Provider	Organizer Kenteq Assessor Kenteq	Organize the APL process Execute the APL process
ePortfolio provider	Personal coach	Supports the development of the employee

3.1.2 Business risk analysis

RISK ANALYSES			
Actor	Event	Result	Remark
Employability coach	falsifies information	Employee will not get his APL or Employability provider will not get paid for his services.	
Employee	uses a false ID	Employee will not get his APL or Employability provider will not get paid for his services.	
Employee	gives false search information	Wrong employability provider might be selected	
Employability coach	steals PII from employees	Abuse of PII possible.	
Employee	provides false information in APL process	Undeserved certificate and ePortfolio information possible.	
Personal coach	steals PII from employees	Abuse of PII possible.	
Personal coach	falsifies portfolio information	Undeserved certificate and ePortfolio information possible.	coach bribed by employee
Assessor	steals PII from employees	Abuse of PII possible.	
Assessor	falsifies assessment	Undeserved certificate and ePortfolio information possible.	assessor bribed by employee
Employer (HRM)	steals PII from employees	Abuse of PII possible.	

3.1.3 Secure Tropos trust model

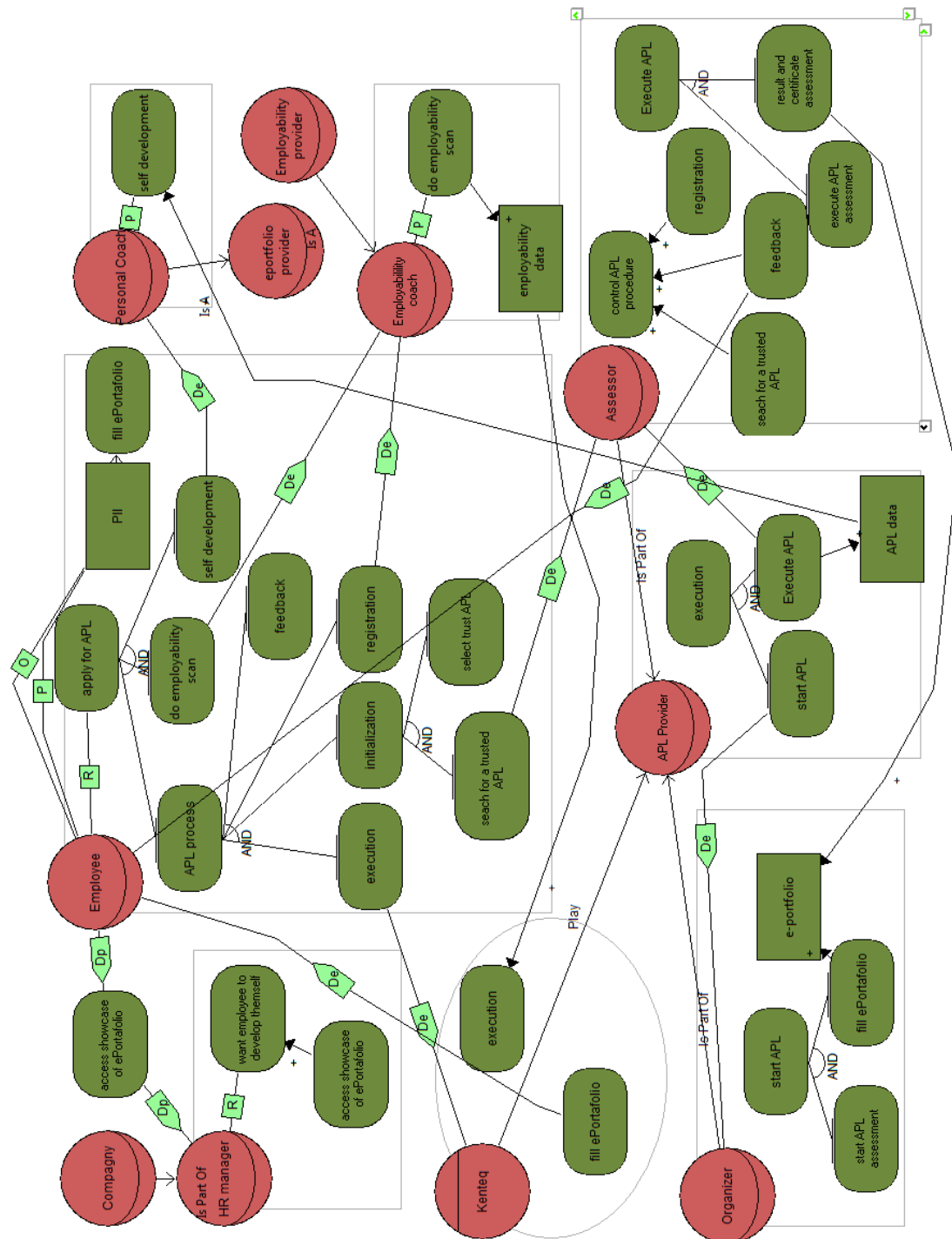


Figure 1 : APL Secure Tropos Diagram

In Figure 1, one can see the following actor diagrams: Employee, Company, HR manager, Personal Coach, ePortfolio provider, Employability provider, Employability coach, APL Provider, Organizer, Assessor and Kenteq. An actor diagram represents internal goals of actors, goal decomposition and delegations. The Employee Requests to achieve the goal “apply for APL” (“R” relation indicates the desire of an actor for the achievement of a goal, the execution of a task, or the provision of a resource). For that he needs to do a self development (the self development is delegated, “De”, to the Personal Coach.). The Employee initializes the APL process (corresponding requirement is Req 3.1a). The execution of the APL process is delegated to Kenteq. In the figure with arrow “Play” is shown that actor Kenteq plays an APL Provider role. Role is a collective description of actors which act within the scopes of the role. A group of actors can play the same role (Req 3.4: if one actor is on vacation, another actor can play the role).

To enforce separation of duties, the employability coach and APL provider are represented as two separate roles (req 3.2a, 3.2b and 3.5a). These two roles should be executed by two separate actors that we can call Agent A and Agent B.

3.1.4 Process

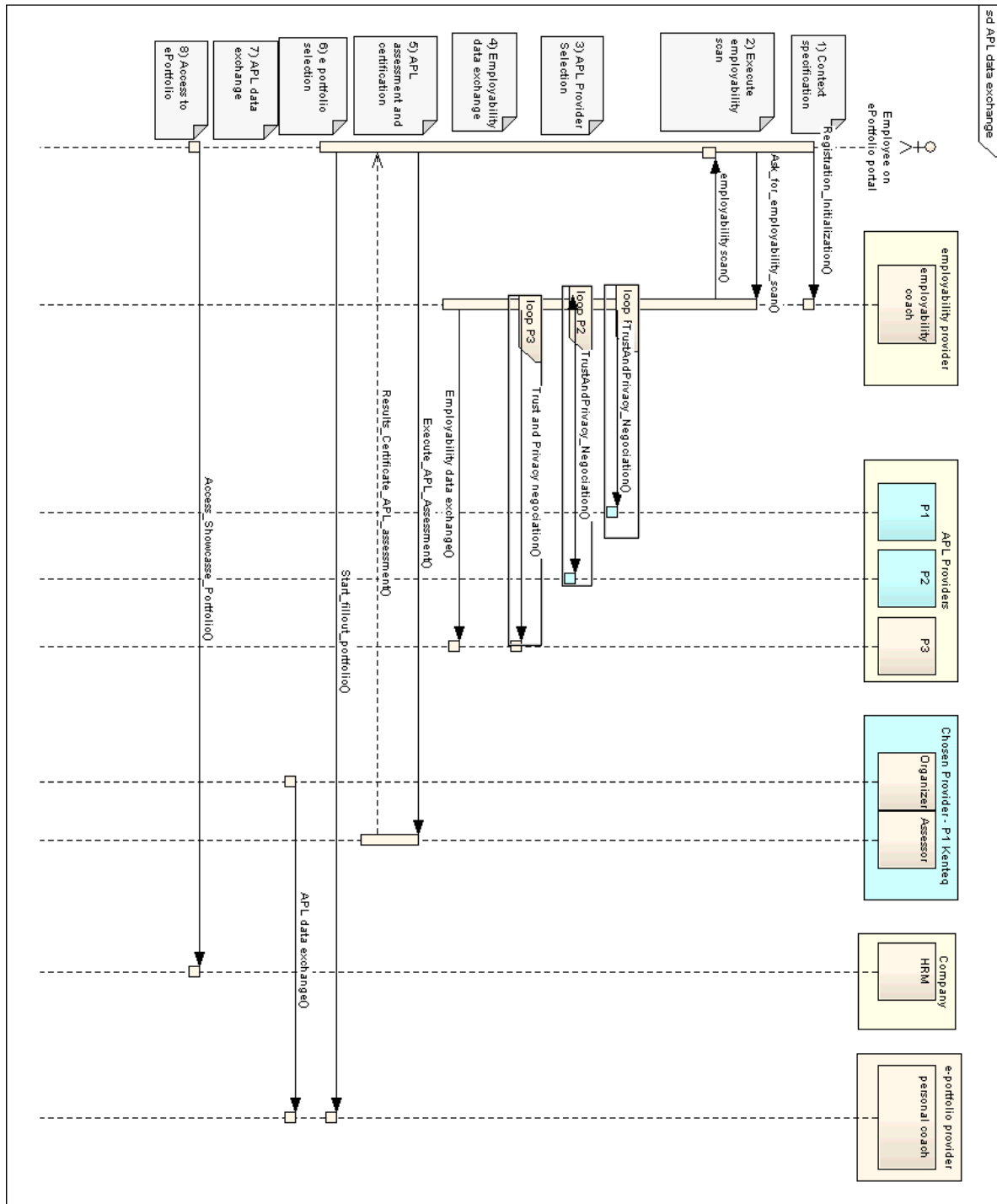


Figure 2 : APL Process

3.1.5 Step-by-step description

More information on the 9 major sequences:

1.
 - Employee (user) authenticates to Portal SSO.
 - Mutual Authentication and Authorisation to access service.
2.
 - He selects an employability provider (there is only one)
 - Accepts the policies of the employability provider
 - Does the employability scan
3.
 - Employee selects an APL provider (1 out of 3)
 - Find out which are trustworthy
 - User evaluates trustworthiness of Employability Providers and chooses one.
 - Sets his policies at the APL provider
4.
 - He gives consent to exchange his data from the employability scan
 - Data exchange from employability provider to APL provider
5.
 - Execute APL assessment
 - He checks with the coach his employability data
 - Assessor provides the APL results and the APL certificate
6.
 - He selects an ePortfolio provider (only one)
 - Accepts the policies of the ePortfolio provider
7.
 - He gives consent to exchange his APL data
 - Data exchange from APL provider to ePortfolio provider
8.
 - The employee authorizes his employer (HR manager) to access the showcase of his ePortfolio

3.2 Mass Layoff Scenario

The biggest difference in mass layoff scenario to the previous one is that the role of mobility centre and the employment office is taken over by the Tripod consortium. Tripod is a consortium of employability providers, who aim to help workers to another job. From job to job without being unemployed.

Description of the Mass Layoff scenario:

1. The company stops production and the employees face redundancy in 6 months
2. A job seeker does an intake at Tripod (consortium of employability providers)
3. His HR data is exchanged between the company and the employability provider
4. He does an assessment which results in his Personal Competency Profile (PCP)
5. His PCP is exchanged between the employability provider and his ePortfolio
6. Via his ePortfolio he gets access to a Vacancy data provider (database with Vacancy Competency Profiles -VCP-)
7. He searches for a well matched vacancy (Match between PCP and VCP)
8. He applies for a job
9. He checks if his data policies have been complied with
10. He finds a new job

3.2.1 Actors

Scenario Actor	Person	Task
Company	HR Manager	Inform Redundant staff
End user	Job Seeker	Find a job
Tripod	Organizer	Do the intake
Employability provider	Assessor Kenteq	Execute the assessment
ePortfolio provider	Job coach	Provide ePortfolio services
Vacancy providers	Admin werk.nl	Maintain and provide Vacancy database

3.2.2 Business risk analysis

RISK ANALYSIS			
Actor	Event	Result	Remark
HR manager	Falsifies HR data	Job Seeker will not get his assessment or Employability/Vacancy Data provider will not get paid for his services.	personal coach bribed by employee
Job coach	falsifies information	(Best) matching vacancies might not be provided.	
Job Seeker	uses a false ID	Job Seeker will not get his assessment or Employability/Vacancy Data provider will not get paid for his services.	
Job Seeker	falsifies information	(Best) matching vacancies might not be provided.	
Job Seeker	provides false information in assessment process	(Best) matching vacancies might not be provided.	
Organizer	steals PII from Job Seekers	Abuse of PII possible.	
Job coach	steals PII from Job Seekers	Abuse of PII possible.	
Organizer	falsifies information	(Best) matching vacancies might not be provided.	
Assessor	steals PII from Job Seekers	Abuse of PII possible.	
Assessor	falsifies information	(Best) matching vacancies might not be provided.	
Vacancy Data provider	steals PII from Job Seekers	Abuse of PII possible.	
Vacancy Data provider	favours one vacancy above others	Best matching vacancies might not be provided.	

3.2.3 Secure Tropos trust model

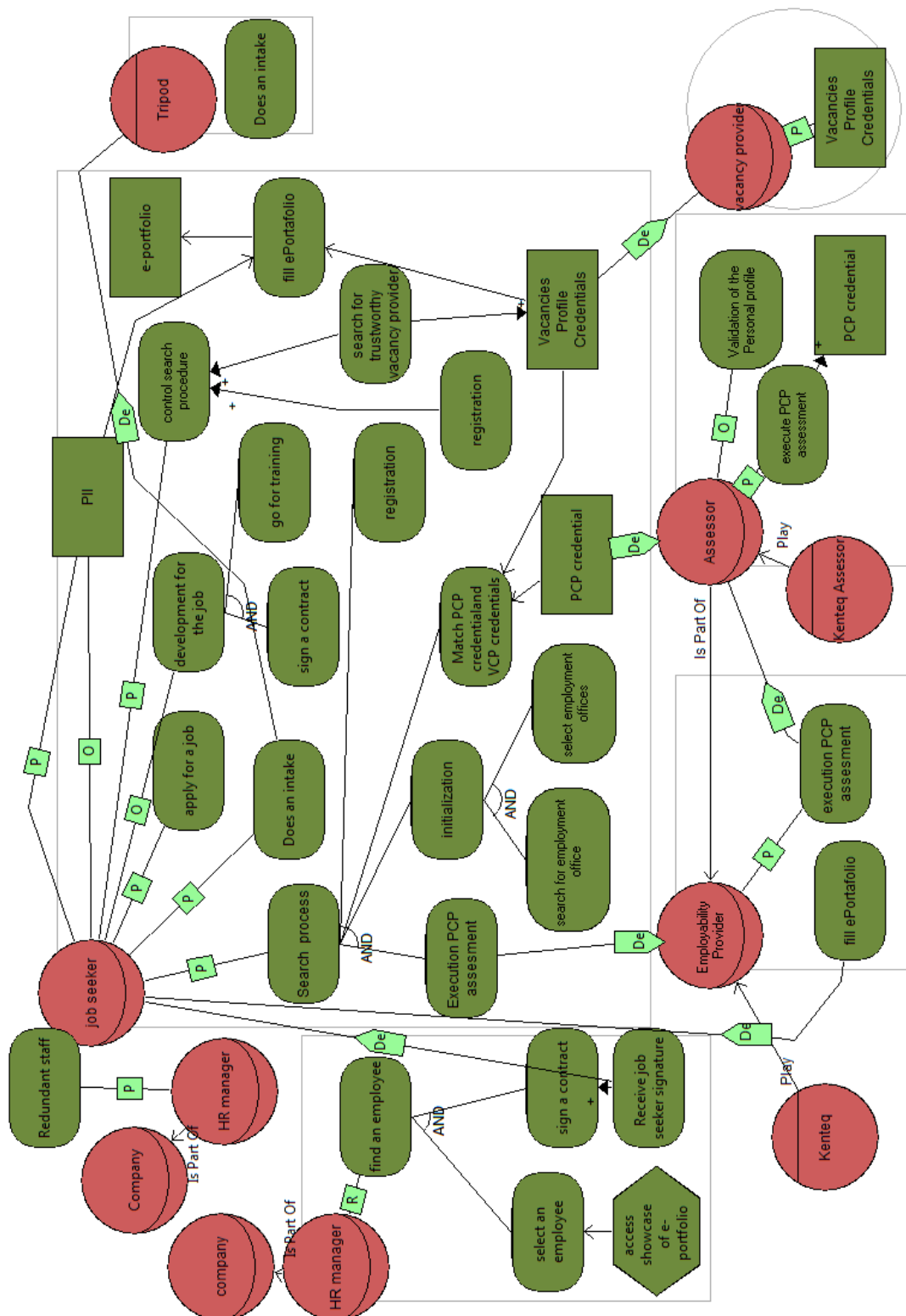


Figure 3 : Mass Layoff Secure Tropos Diagram

The Job Seeker has to fulfil the goal “apply for a job” (“P” relation means Provisioning, which indicates that the actor has the capability to achieve some goal, execute some plan, or deliver a resource).

3.2.4 Processes

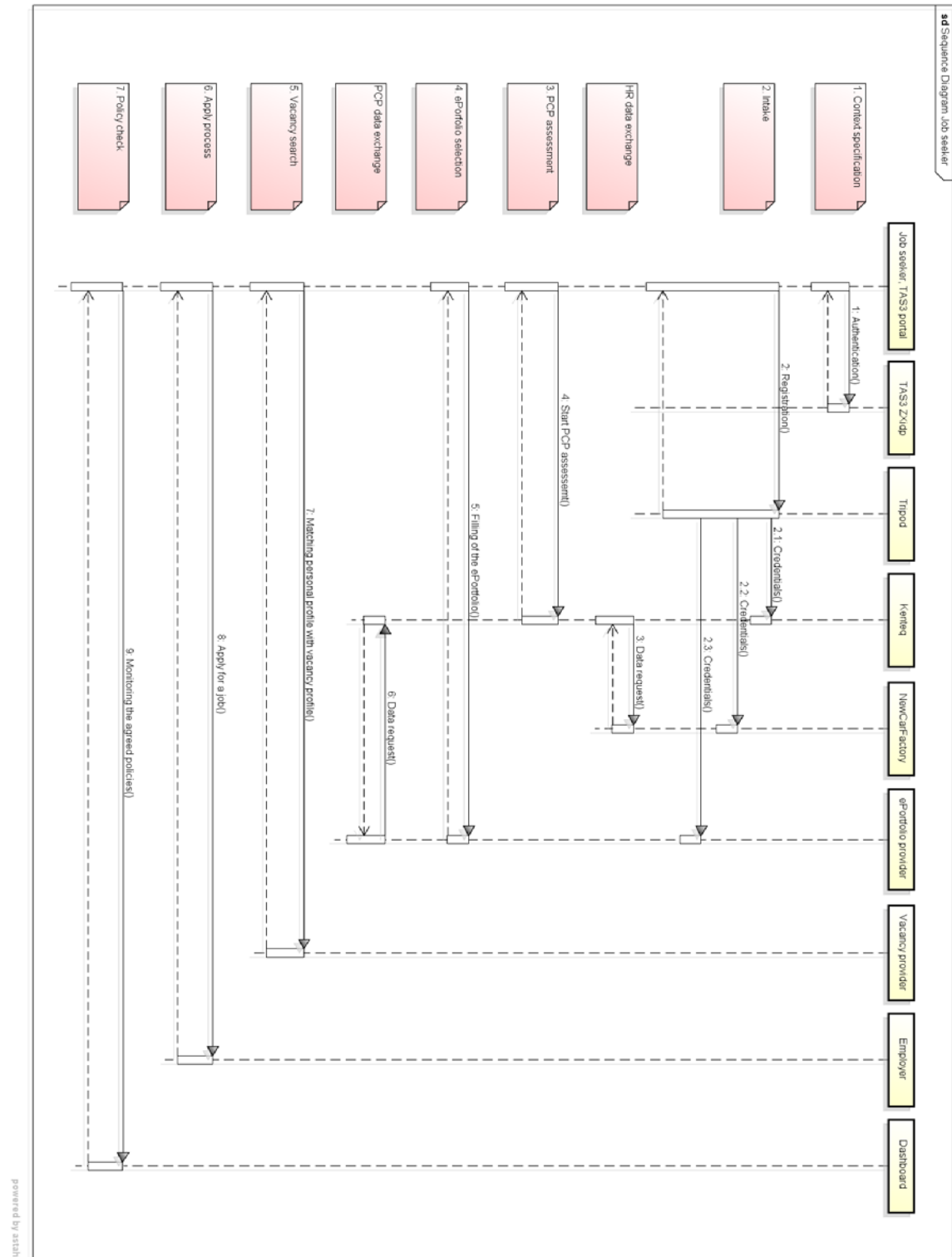


Figure 4 : Mass Layoff Process

3.2.5 Step-by-step description

More information on the 9 major sequences:

1.
 - Job Seeker (end user) is redundant in 6 month at employer 1
 - Job Seeker Authenticates to Portal SSO
 - Gets his credentials
 - Mutual Authentication and Authorisation to access the services
2.
 - Does the intake to the Tripod portal
 - Selects a PCP Provider (Personal Competency Profile) (only one)
 - Accepts the policies of PCP Provider
 - Give consent to exchange his HR data to the PCP Provider
3.
 - Execute PCP assessment
 - The submitted Profile must be tamperproof and forwardable to ePortfolio providers
 - User must be able to act with different personas
 - Assessor makes the PCP results
4.
 - He selects an ePortfolio Provider (only one)
 - Accepts the policies of the ePortfolio Provider
 - Give consent to exchange his PCP data to his ePortfolio
5.
 - He selects a Vacancy Provider (only one)
 - Accepts the Term & Conditions of the vacancy provider
 - Fills in his search data
6.
 - Matching personal profile with vacancy profile
 - Results are well fitting vacancies
7.
 - He selects a vacancy and apply for that job

- He sends a link of the showcase from his ePortfolio (CV) to the new employer

8.

- Job Seeker checks if the service providers has complied with his policies at the TAS3 dashboard

9.

- User must have a means of signing the contract
- New Employer must have means of signing

3.3 Student work placement

This scenario shows the simultaneous use of TAS³ by two users, one of whom is a novice user, the other with previous experience of TAS³. The ePortfolio in the previous version is replaced by a TAS³-enabled Personal Data Store (PDS) and the Trust negotiation phase has become more sophisticated, involving use of the Ontology Service and OCT to poll service reliability.

This new, expanded scenario is explained more fully in the latest iteration of deliverable D9.1. The requirements given in this document have been updated from previous iterations to take this revision into account.

Description of the Use Case scenario:

1. Both Learner1 and Learner 2 are studying on a university course and want to enhance their employability by doing a work placement. This can be either to fulfil a particular skills requirement or set of requirements which is mandatory for the course, or a voluntary decision to improve the Learner's employability prospects once the course is completed.
2. Learner1 has never used TAS³ before. She identifies a Placement Co-ordinator authorised by the university and registers with this Co-ordinator, providing details via an application form. At this point a basic contractual agreement is established, including the agreement that transactions will use TAS³.
3. The Placement Co-ordinator verifies the Learner's identity, and checks that the Learner is eligible to participate in one of the placement programmes administered by the Co-ordinator.
4. If Learner1 is eligible, the Placement Co-ordinator sets her up with a PDS and data from her application form is stored there. A default policy is applied to this data.
5. Learner2 has used TAS³ before and has a TAS³-enabled PDS provided by his institution. His university sets up the link from the PDS to the placement co-ordinator so that he can apply for a placement. The PDS is already linked to the IDP and uses SSO.
6. Learner2 activates this functionality to apply for a placement and the appropriate data is pushed to the placement co-ordinator
7. The Placement Co-ordinator chooses a programme for each Learner based on the information submitted and tells each Learner which programme he or she is being entered for.
8. Learners can then fine-tune their policies and agree to any additional terms and conditions specific to the programme.
9. Learners can delegate choice of Matching Service to the Placement Co-ordinator. The Placement Co-ordinator takes the Learner's policies and data and uses these, together with his own policies, to perform a discovery service to find suitable Service Providers offering a Matching Service.

10. If he has been delegated to, the Placement Co-ordinator chooses the most appropriate service for each Learner.
11. The Matching Service uses the Learner's data to match the Learner to profiles of vacancies.
12. The list of returned matches is stored in the Learner's PDS. The Placement Co-ordinator receives notification that results are available and alerts the learners to check in their PDS.
13. The Learner chooses those he or she is interested in. Further 'soft' matching then takes place, including a face-to-face interview.

3.3.1 Actors

Scenario Actor	Person	Task
Learner1,	Student with no PDS who has never used TAS ³ before	Make application; provide access to personal data; set personal security and trust policies, choose placements to apply for
Learner2	Student who already has a PDS and has used TAS ³ before	Make application; provide access to personal data; set personal security and trust policies, choose placements to apply for
Higher Education institution	University	Identity provider; verify that learner is a genuine student
Placement co-ordinator	University-approved service provider	Administration of the process
Placement provider	Organisation offering placement vacancies	Provide vacancy profile
Matching service	Service provider	Provide anonymous matches between vacancy profiles and learner profiles

3.3.2 Business risk analysis

RISK ANALYSIS			
Actor	Event	Result	Remark
Learner	Uses false credentials	Incorrect match, potential identity theft	
Learner	Submits false PII	Incorrect match; fraudulent application made	
Learner	Sets inappropriate policies on data	Insufficient data available to perform service	Learner should be alerted to this
Higher Education Institution	Incorrectly fails to verify learner	Learner is denied access to process	
Higher Education	Returns incorrect	Match performed using	

Institution	identity	incorrect information	
Placement Co-ordinator	Exports learner data to third party without authorisation	Abuse of learner PII	e.g. directly to placement providers
Placement Co-ordinator	Favours one matching service	Lower quality service for Learner	Distortion of competition; possible financial collusion
Matching Service	Uses incomplete learner profile data for match	Lower quality service for Learner; possible incorrect matches	Service may do this to enhance number of results returned
Matching Service	Distorts learner profile data	Incorrect matches returned	
Matching Service	Uses incomplete vacancy profile data for match	Inappropriate matches returned	Service may do this to enhance number of results returned
Placement Provider	Provides incorrect or incomplete profile information	Lower quality service for learner; inappropriate matches may be returned	Placement provider may have something to hide

3.3.3 Secure Tropos trust model

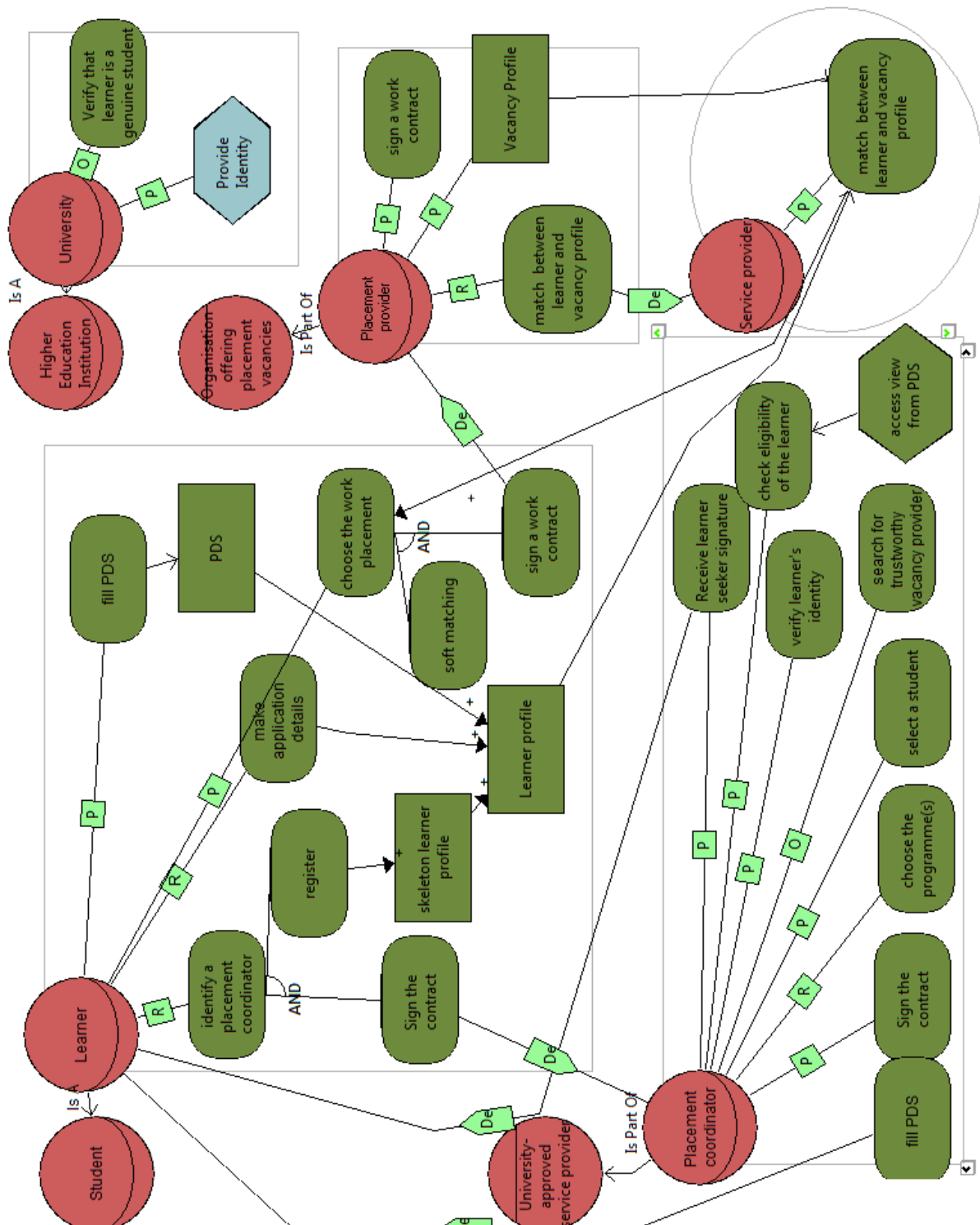


Figure 5 : Student Work Placement Secure Tropos Diagram

The Learner delegates the execution (De) to sign the contract to the Placement Coordinator. The signature of the work contract (De) is delegated to the Placement Provider. The Service Provider is responsible for the match between Learner and vacancy profile; the resources Vacancy profile and Learner profile are necessary.

3.3.4 Processes

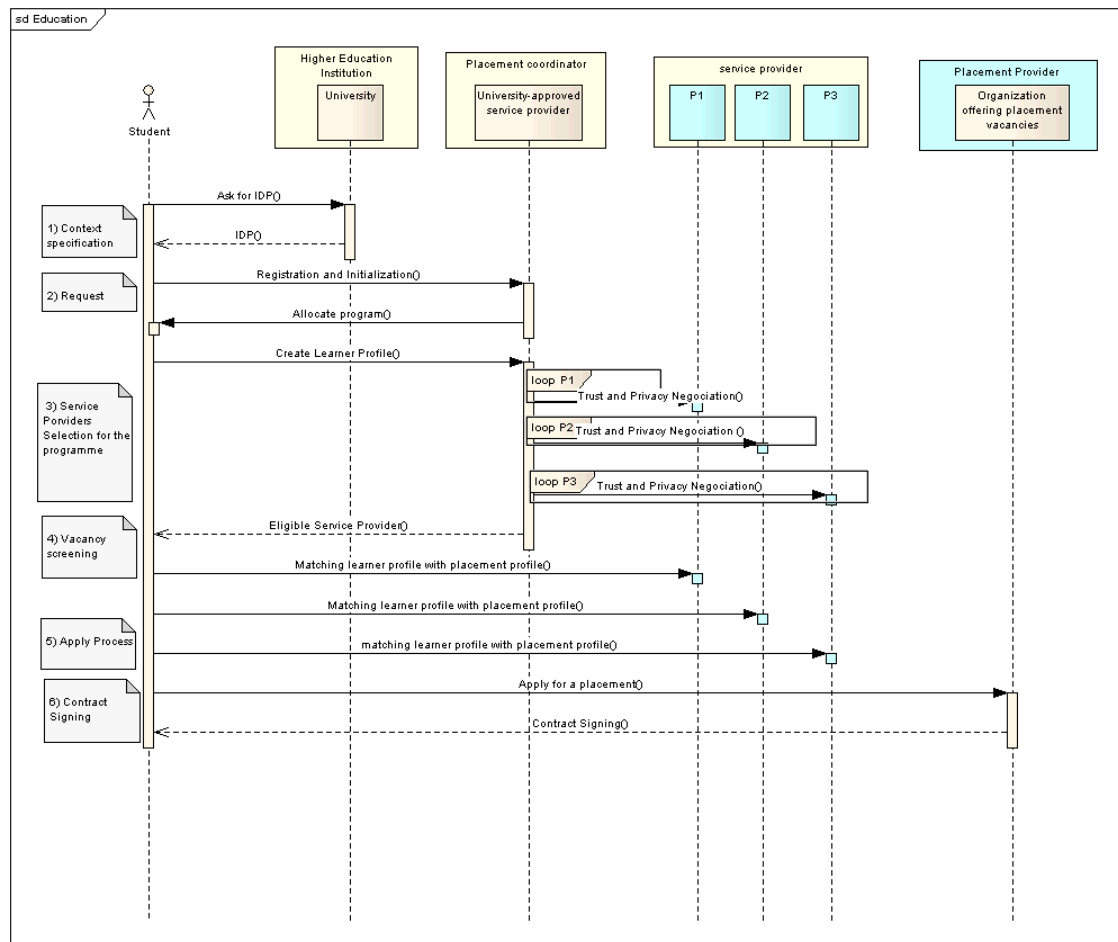


Figure 6 : Student Work Placement Process

3.3.5 Step-by-step description

More information on the major sequences:

1. Learner1 signs up with an approved placement Co-ordinator via SSO
 - a. Provides authentication credentials from a participating university
2. University IDP token used to authenticate
 - a. Student ID used to contact home IDP
 - b. Return will verify that the student is genuine
3. Learner1 fills in an application form

- a. If genuine and eligible, Placement Co-ordinator sets Learner1 up with a new TAS³-enabled PDS
 - b. Application form data is stored in the new PDS with a default policy attached
4. Learner2 logs into PDS: this already uses SSO. PDS has a link to the Placement Co-ordinator
 - a. Learner2 selects application information from PDS that Placement Co-ordinator needs and grants access to Placement Co-ordinator
5. Placement Co-ordinator matches each Learner to placement programme he/she is eligible for and informs learner. From now on the process is the same for both Learners.
6. Learner provides further specific application details from PDS if needed
 - a. Learner fine tunes privacy policies and attaches to PDS data
 - b. Learner sets acceptable trust ranking levels for matching service
 - c. Learner chooses whether to delegate choice of matching service to Placement Co-ordinator
7. Discovery service finds service providers for matching service for the programme
 - a. Trust and privacy negotiation with service providers using learner and Placement Co-ordinator policies
 - b. Placement Co-ordinator (if delegated)/Learner is returned a list of suitable service providers
 - c. Placement Co-ordinator (if delegated)/Learner selects which service providers he/she wishes to release his/her profile to
8. Selected matching service providers receive anonymised learner profile and match to available placement profiles
 - a. Retrieve placement details and appropriate sticky policies associated with the placement data
 - b. Perform match with Learner's data and policies
 - c. Aggregate results and return to Learner's PDS
 - d. Placement Co-ordinator sends notification to learner via email
9. Learner confirms with the Placement Co-ordinator receipt of matches made and requests formal application for any chosen placements
 - a. More detailed placement profile information is retrieved and presented to learner
 - b. Learner makes formal application for specific placements, followed by further selection processes, including face-to-face interview or tests
 - c. If the Learner is unsuccessful, he or she can choose for the process to loop back to allow further applications to be made
10. Transaction is closed on the system and logs are written
 - a. Learner, Placement Co-ordinator and Service Provider are issued with a receipt for the process
 - b. Once placement is completed the Learner can give feedback.

3.4 Emergency admission following an accident on the road

The first iteration of the D9.1 deliverable describes Personal Health Record (PHR) related scenarios. However since the writing of that text, the subcontractor responsible for delivering the Personal Healthcare Record implementation withdrew from the project (Medisoft). A compatible backup scenario was chosen (over which the remaining partners have full control). This scenario will be implemented first, and integrated with the PHR scenario later in the project.

The backup scenario deals with the “Patient Summary Record”. Roughly speaking, such a summary is the minimal set of data that a physician needs in order to understand the medical status of the patient in a few minutes and to ensure the continuity of care. In the pilot, the record is updated by one designated physician (common practice for a summary record) and can be viewed by patients and physicians (depending on their role in a patient’s therapy). Summary records can be used by replacement physicians, in emergency situations, by pharmacists, etc.

In fact, the overlap with the initial D9.1 PHR pilot is large: the PHR repository is merely replaced with another repository (summary). The use of the PILS (Patient Information Locator Service) front-end service remains the same. When the PHR scenario is piloted in a second step, it will be merged with the summary record pilot architecture (with the PHR as “just another medical data source”). The use case explained below is the case in which the summary record is used as sole and immediate source of information available in an emergency situation, which also illustrates the “break-the-glass” requirement.

1. A patient has an accident on the road. The paramedic arrives with the ambulance. They try to find the patient ID. Within this scenario we have to take into account that the only way the patient can be identified could be an identity piece with only name and address (the latter one could be limited to the locality). In the worst case a business card could be the starting point for identification.
2. As soon as the Paramedic knows the identity of the patient and has got confirmation for admission to an A&E (Accident & Emergency) department, he transmits the ID data to the A&E department. The emergency physician connects to the Patient Summary server via the PILS (Master Patient Functionality is partially provided through the PILS which forwards name searches to the repositories).
3. In this Use Case no Patient Consent exists, the emergency physician can apply for an override action (breaking-the-glass procedure).
4. As the emergency physician has to know the health status of the patient, prior to treatment, he can start a procedure to get access to the Patient Summary. At that moment a detailed logging starts registering all actions undertaken by the A&E physician. The logging will be used for postfactum

auditing purposes by the responsible healthcare authority and to report back to the patient and its GMD holder.

5. When accessing the Patient Summary, important life saving information could become available (risk factors) that needs to be transmitted to the people in the ambulance. When the patient arrives at the A&E department of the hospital, appropriate care delivery can be given thanks to the information found in the Patient Summary Record.

3.4.1 Actors

Scenario Actor	Person	Task
Paramedic	Paramedic	The Paramedic is acting within the ambulance service
A&E Physician	Physician	Physician working in Accident and Emergency department
PILS – Patient Information Location Service	The PILS presents a user interface	A service which contains pointers to data repositories. In these use cases, it does not index patient information, only the location of potential sources of patient data.
Data Repository	HR Manager	Supports the development of the Medical data repositories, one of which is the Patient Summary.

3.4.2 Business risk analysis

This analysis will not take into account :

- Malfunctioning of TAS³ (requirements of scenarios are assumed to be fulfilled by TAS³)
- Denial of Service by malicious actors
- Threats with negligible probability of occurrence or with no real relation to TAS³ (e.g. physician provides false information under his own name)

RISK ANALYSIS			
Actor	Event	Result	Remark
Repository Service Provider	Exports data to third party without authorisation	Abuse of medical PII	
PILS Service Provider	Exports data to third party without authorisation	Abuse of medical PII	The PILS has only access to information that it needs to visualise.
Physician	Unlawfully uses break-the-glass to access a summary	Abuse of medical PII	e.g. for use in his function of insurance physician, selling the

			data, ...
Physician	Unlawfully uses the PILS lookup to find patient demographics	Abuse of non-medical PII	e.g. to recruit patients
Patient	Provides Physician with wrong identity (identity theft)	Physician bases his decisions on wrong information. Patient Safety issue.	Patient wants to commit insurance fraud.
Any Actor	Is able to steal physician credentials and impersonates physician	Abuse of medical PII	"Download"
Any Actor	Is able to steal physician credentials and impersonates physician	Corruption of medical PII	"Upload"
Any Actor	Is able to steal patient credentials, impersonates patient	Could modify TAS ³ policies to access data or provide access to (colluding) third parties.	
Any Actor	Is able to steal patient credentials, impersonates patient	Abuse of medical PII	Once a patient is given access to his own summary record. Although this is not yet foreseen in the scenario, this is a probable evolution (patient empowerment)

3.4.3 Secure Tropos trust model

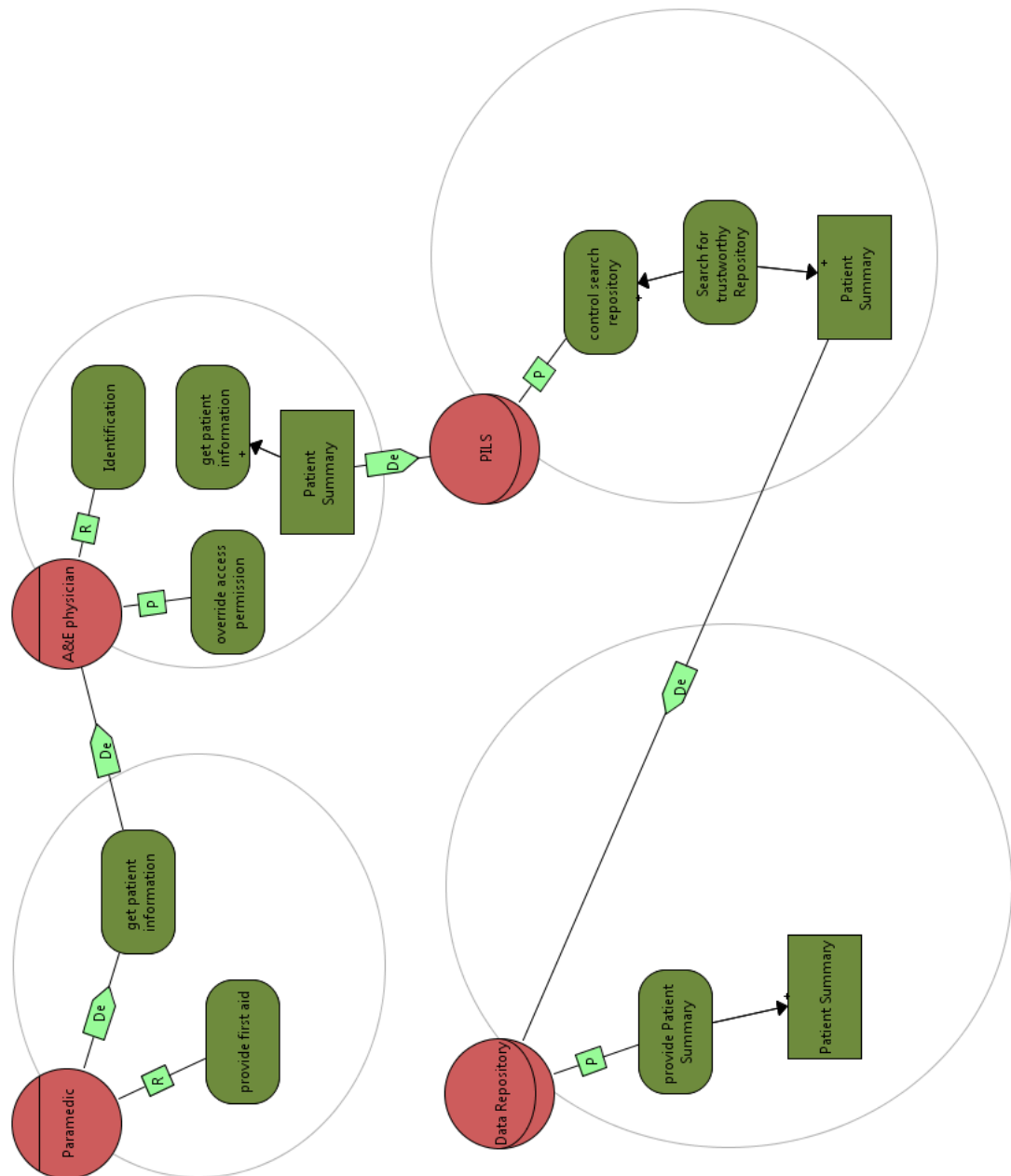


Figure 7 : Emergency Admission Secure Tropos Diagram

The Paramedic delegates the execution (De) of getting the patient information to the A&E physician. The A&E physician delegates to PILS (De) the access to patient data. PILS delegates to the data repository the goal of providing the Patient Summary.

3.4.4 Process

Figure 8 : Emergency Admission Process

3.4.5 Step-by-step description

The process can be described in 5 major sequences:

1. Identify Patient and Request for information

In case of non availability of the required Patient ID at the location of the accident, a name search has to be launched to acquire the patient ID (business card case). This could already initiate the Breaking the Glass event.
2. Trust establishment between PILS and repositories,
 - Repositories need to trust PILS to accept the request, in case of multiple PILS, or a new PILS registering the TAS3 network, a trust evaluation may allow a request.
 - When a PILS is trusted, it may select one or another repository based on some metrics. e.g, a repository may not have all necessary information for an emergency need; this could be a metric for a choice.
3. Try to retrieve patient data without his consent.

4. Break the glass to access patient data in emergency case
5. Provide the patient data

4 Design Requirements

This chapter describes requirements with a focus on scenario's steps. As scenario have a major overlap from a TAS³ perspective, the list of requirements may refer to any or all scenarios.

For easier access, requirements are split and numbered by work package.

4.1 Business Process

Business process specific requirements are based on the "APL" scenario.

- Req 3.1: People **SHOULD** be able to use their existing accounts when taking part in processes of organisations they did not have contact with before (see also requirement in D1.2-3.4).
 - Req 3.1a: The Employee **SHOULD** be able to log into the system of the employability using his existing account from his company.
- Req 3.2: The assignment of users to workflow tasks and roles needs to be flexible. Assignment **SHOULD** be possible based on a mapping to organisational roles and by explicit modelling in the process (this requirement supports D1.2-3.5).
 - Req 3.2a: The employee's coach for the APL process can be chosen based on the fact that he is assigned the role "Employability coach" at the employability provider.
 - Req 3.2b: The employee's assessor will be chosen by the APL provider (or, later, possibly automatically) after he or she has signed up for APL.
- Req 3.3: It **MUST** be possible to delegate access to resources connected with the business process to process participants. Access **MUST** be limited to the data actually needed and **SHOULD** be available only as long as needed (this requirement abstracts D1.2-3.6, requires D1.2-3.10).
 - Req 3.3a: The Employability coach **SHOULD** be able to grant access to e-learning resources to the employee.
 - Req 3.3b: The employee **MUST** be able to grant his coach and his assessor access to his portfolio until they have completed the coaching/assessment.
 - Req 3.3c: A coach **MUST** only have access to the portfolios of employees he is actually coaching.
- Req 3.4: It **MUST** be possible to delegate workflow roles or tasks (see also requirement in D1.2-3.7).
 - Req 3.4a: When the employability coach responsible for a employee is on vacation, he **SHOULD** be able to delegate his responsibilities regarding the APL of that employee to someone else.

- Req 3.4b: Delegations **MUST** be subject to a delegation policy. With such a delegation policy, it **MUST** be possible to specify to whom delegation may occur, if chained delegation is allowed, and which application-dependent constraints **MUST** be fulfilled. Such application-dependent conditions can also be based on whether data in the process contains certain categories of specifically sensitive information (e.g., medical information).
 - Req 3.4c: The Assessor at Kenteq might be allowed to delegate the assessment to a junior assessor, but only in order for basic qualifications or specific parts of the qualifications to be accredited.
- Req 3.5: It **MUST** be possible to specify separation of duty constraints, i.e. that some tasks may not be performed by the same person (see also requirement in D1.2-3.8).
 - Req 3.5a: The employee **SHOULD** not be coached and assessed by the same person, because there is a conflict of interests between these two tasks: The assessment of the employee's performance after coaching is implicitly also about the quality of the coaching.
- Req 3.6: It **MUST** be possible to change permissions to individually identifiable information at any time, and the updated permissions **MUST** be honoured immediately (defines the first part of D1.2-3.11).
 - Req 3.6a: The employee discovers that he included the certificate of a Norwegian language course that he visited for fun some years ago into his portfolio. Since neither the grade was very good, nor he remembers any of it, he does not really want this certificate to be looked at by third parties. He **MUST** be able to revoke access rights with immediate effect.
 - Req 3.6b: The coach informs the employee that detailed grades from his high school diploma are not available to him, and that the employee's training might be able to be reduced if these grades prove abilities he needs for his new qualification. The employee **SHOULD** be able to grant access to the coach, who **MUST** then be able to access it.
- Req 3.7: Business processes **MUST** be able to act on behalf of other entities (humans or computer systems), e.g., by using appropriate credentials.
 - Req 3.7a: In steps 5 and 6 of the mass layoff scenario, the employability provider interacts with a vacancy provider on behalf of the job seeker.

4.2 Trust Requirements

The requirements related to the Trust-PDP are elaborated below: general requirements of the T-PDP are given here, followed by corresponding specific requirements based on the "Mass Layoff" (Section 3.2) and "Emergency Admission" (Section 3.4) scenarios. Steps refer to the former scenario unless marked with EA which indicates they refer to the general steps in the later scenario (not to be confused with the step-by-step process description in section 3.4.5).

- Req 5.1 the Trust-PDP MUST support user selected policies.
 - Req 5.1a A Job Seeker MUST be able to choose trust requirements for access to his PII and preferences (Steps 2)
 - Req 5.1b A Vacancy Data Provider MUST be able to express the job profile in a policy and attach as trust requirements to the full project description and the application process. (Steps 6,7)
 - Req 5.1c The Trust-PDP MUST support structural trust rules
 - Req 5.1d A Job Seeker MUST be able to express trust in only Vacancy Data Providers Certified by a trusted Accreditation agency. (Step 6)
 - Req 5.1e A Vacancy Data Provider MUST be able to require a degree from a certified Higher Learning Institution in the policy expressing the job profile requirements. (Steps 6,7)
 - Req 5.1f a patient MUST be able to specify trust requirements for consent. (EA: Specification before scenario, use in EA Step 2)

Design: The Trust PDP can evaluate policies from any source, including the user. Support for sticky policies, allowing the users policy to travel with the data, will need support for embedding policies in request which requires use of the v3 of the XACML standard (currently under development) for requests sent to the Trust-PDP.

The trust policy language used by the Trust-PDP supports the features mentioned in points a-e.

Implementation: The Trust-PDP can be configured with any set of policies (including those of the user) though no support for sticky policies is available yet (see also remark in design).

- Req 5.2 the Trust-PDP SHOULD support trust decisions based on dynamic data such as KPIs (cf. Glossary).
 - Req 5.2a A Vacancy Data Provider SHOULD be able to define the weighted KPI metric and use this in his trust requirements. (Step 6,7). Part of job profile could be e.g. good performance on number of patents applied for and billable hours. Only employees which satisfy the basic requirement will be allowed to see the full project description

Design: Supports these requirements.

Implementation: Versions of the components needed to support this functionality is basically available but had not been enabled yet; requires configuration and implementation of some basic connectors.

- Req 5.3 the Trust-PDP SHOULD be able to fetch required KPI data from external sources.
 - Req 5.3a Evaluating a Vacancy Data Providers trust policy the Trust-PDP SHOULD determine the KPI information needed and download the KPI statistics from a web service and thus use up-to-date information in its trust decision. (Steps 6,7)
 - Req 5.3b a (web) service SHOULD provide normalized KPI factors

Design: The Trust-PDP has a KPI Service which fetches live data from online sources.

Implementation: A first version of the KPI Service is available but not yet connected to the Trust-PDP.

- Req 5.4 the Trust-PDP MUST support reputation based on different behavioural factors (cf. Glossary).
 - Req 5.4a A Vacancy Data Provider SHOULD be able to define the required reputation; e.g. a good score on the facets 'cooperation' and 'communication' within feedback on the applicants' performance. (Steps 6, 7)
 - Req 5.4b The Trust-PDP SHOULD evaluate the reputation of a Job Seeker and incorporate it in the trust decision (Step 6,7). Evaluation can be done by calculating the value of the reputation metric defined by the vacancy data provider (req 5.4a)
 - Req 5.4c The Trust Information Collector (cf. Glossary) SHOULD collect and store reputation and performance feedback information and make this available to the Trust-PDP for evaluating reputations.
 - Req 5.4d. A Job Seeker SHOULD be able to provide feedback to be used in determining the reputation of the Employment office. (Step 9)
 - Req 5.4e. A Job Seeker SHOULD be able to provide feedback to be used in determining the reputation of the Vacancy Providers. (Step 9)
 - Req 5.5f. Feedback based on inspecting logs after the break the glass SHOULD be usable to evaluate reputations. (EA Step 4,5 and after)

Design & Implementation: A reputation trust management service which supports different ways of computing reputations based on given feedback is available to Trust-PDP.

- Req 5.5 the Trust-PDP SHOULD be able to request required credentials from external sources.
 - Req 5.5a The Trust-PDP SHOULD be able to fetch and validate additional credentials needed to establish trust worthiness of requestor of PILS data (EA Step 2)

Design: A credential trust management service which supports discovering required credentials is available to the Trust-PDP.

Implementation: A first version of the credential trust management service supplying basic functionality is available and supported by the Trust-PDP.

4.3 Identity Management, Authentication and Authorisation

Note: Requirements given here are based on the APL and Mass Layoff scenarios.

- Req 7.1 User SHALL be able to delegate access permissions to their private resources to other users (step 8 of APL)

- Req 7.2 The authorisation system SHALL be able to support an escape mechanism (called Break The Glass) that allows unauthorised users to access protected information under specified conditions (step 4 of Emergency Admissions).
- Req 7.3 The system SHOULD provide the users with a single sign on (SSO) capability. (Note, this is not mandatory since some experts believe that SSO is a vulnerability) (Step 1 of APL)

4.4 “Trusted Application Infrastructure”

- Req. 8.1.: A user or a web service, which functions as client, SHOULD be able to connect to TAS³ over a unified or adapted gateway. Step 1-3 of APL, Step 1-2 of Mass Layoff, Step 2 of Student Work Placement (Reference to D1.2: Req. 1.2-8.1)
- Req. 8.2.: A user or a web service, which functions as client, SHOULD be able to connect to a legacy database, which has been connected to the TAS³ infrastructure Step 4 of APL, Step 2 of Mass Layoff (Reference to D1.2: Req.1.2-8.2.)
- Req. 8.3.: A user or a web service, which functions as client, SHOULD be able to connect to TAS³ out of a business process) (Step 1 of APL and Mass Layoff, Step 4 of Student Work Placement)(Reference to D1.2: Req. 1.2-8.3.)
- Req. 8.4.: A user SHOULD be able to access TAS³ and its functionalities over a special TAS³ client (called Generic Client), which can be used, when other clients are not available. Step 3 of APL, Steps 2-5 of Mass Layoff (Reference to D1.2: Req. 1.2-8.4.)
- Req. 8.5.: A user SHOULD be able to manage (create, modify, delete) his policies Step 3 of APL, Steps 2-5 of Mass Layoff, Step 6 of Student Work Placement (Reference to D1.2: Req. 1.2-8.5)
- Req. 8.6.: A user SHOULD be able to store his person related data in dedicated TAS³ repository, when no other repository or data provider is available) Step 4 of APL, Step 4 of Mass Layoff, Step 3 of Student Work Placement (Reference to D1.2.: Req.1.2-8.6)
- Req. 8.7.: A user SHOULD be able to monitor her data using a single point of access called the TAS³ Dashboard (Step 8 of Mass Layoff, Step 10 of Student Work Placement). (Reference to D1.2: Req. 1.2-8.7)
- Req. 8.8.: A TAS³ web service SHOULD be able to access an audit service to log occurred exceptions during transactions (Step 8 of Mass Layoff, Step 10 of Student Work Placement) (Reference to D1.2: Req. 1.2-8.8)

5 Architectural and Technical Design Requirements

This chapter focuses on the overall framework design requirements needed to fulfill Employability Demonstrator requirements.

Each WP/domain describes its requirement with a dependency part allowing to highlight cross-requirement among WP's.

5.1 Business Process

5.1.1 Architectural

- Req 3.8: The architecture SHOULD provide secure data repositories.
 - Req 3.8a: The data repositories SHOULD support delegation of authority.
- Req 3.9: The architecture SHOULD provide a mechanism to identify data of designated sensitive categories (supports the second part of D1.2-3.9).
 - Req 3.9a: The architecture SHOULD provide a data format and ontology to mark such data.
 - Req 3.9b: The architecture SHOULD provide a service to check for such marks.
- Req 3.10: Processes MUST be able to react to and recover from security violations in a secure way.
 - Req 3.10a: The process execution engine MUST be notified about security violation :
 - Req 3.10b: The process execution engine MUST raise BPEL events on security violations.
 - Req 3.10c: The modelling tool MUST support modelling of security event handlers.

5.2 Identity Management, Authentication and Authorization

5.2.1 Architectural

- Req 7.5 Users MUST be able to authenticate to services using their existing authentication credentials without needing to be issued with new authentication credentials by each new service they wish to access
- Req 7.5a The system SHALL support multiple Identity Providers (IDPs) and multiple Service Providers (SPs) that have mutually agreed trust relationships between them. If the IDP sends the attribute assertion to the SP, then it has to trust the SP since it is providing it with an attribute assertion. There are privacy issues here – the IDP MUST trust the SP to protect this information. If the IDP gives the assertion to the user, the IDP trusts the user to act responsibly with this, and allows the user to give it to anyone the user trusts.
- Req 7.5 Users MUST be enrolled with an Identity Provider in order to use the services of its mutually trusted Service Providers.
- Req 7.6 Users SHALL be allowed to enrol with multiple Identity Providers under different unrelated identities
- Req 7.7 Service Providers SHALL be able to set the policies (authentication, authorisation and trust) that control access to the resources under their control
- Req 7.8 Users SHALL be able to set the policies that control access to their personal identifying information (PII), and this policy SHOULD stay with their PII regardless of where this PII is subsequently held.
- Req 7.9 Regulatory Authorities SHALL be able to set the policies that control legal access to PII
- Req 7.10 The Authorisation system SHALL support the setting of multiple authorisation policies by multiple authorities and be able to resolve any conflicts between these in a mutually acceptable manner
- Req 7.11 The authorisation system SHALL be able to support history based access control decision making i.e. where the current decision is based on both the current context and previous decisions.
- Req 7.12 The system SHALL support a tamper proof audit capability in which the audit logs are visible to trusted third parties
- Req 7.13 The system SHOULD provide users with a single sign off capability.
- Req 7.14 The authorisation system SHALL allow policy administrators to dynamically update their policies.

5.2.2 Dependencies

- Req 7.17 All system components **MUST** be able to write to the audit function.
- Req 7.18 The authorisation component **SHALL** be able to make use of information from the Trust component when making an authorisation decision
- Req 7.19 All services and applications **SHALL** depend upon the same agreed IDM, authentication and authorisation infrastructure
- Req 7.20 There **SHALL** be a simple easy to use service oriented interface between the application dependent code and the IDM, authentication and authorisation application independent infrastructure
- Req 7.21 The information that is sent to the audit function **SHOULD** be dependent upon the state of the system, and events (external or internal) **MUST** be able to dynamically effect what information is sent to the audit function.

5.3 Trust

- Req 5.6 the architecture **SHALL** provide a facility (PEP) to determine when trust policies need to be evaluated and call the appropriate component (the Trust PDP).

Design: The architecture design specifies a PEP which calls a Master PDP which determines whether trust policies are to be evaluated and calls the Trust PDP if needed. Thus the design fully supports this requirement.

Implementation: The project is in the process of implementing an application independent PEP which will greatly reduce the effort needed for building a PEP for a specific application. A master PEP will be built but is not yet available but a direct call of the Trust PDP is possible. The current implementation partly satisfies this requirement.

- New Req The architecture **SHOULD** support ranking service providers based on trustworthiness score when offering a choice of services to the user.
 - New Req sub a) The architecture **SHALL** include a Trust Data Access Service Provider which provides trustworthiness scores of service providers.
 - New Req b) Users **SHOULD** be able to use the trustworthiness score of Employability Providers when selecting. (APL step 5)

Design: Service discovery supports ranking by evaluating each of the suitable providers using a scoring service. A Trust Data Access Service Provider has been added to the Trust Tool set.

Implementation: A Trust Data Access Service Provider which can evaluate single trust metrics (which may be nested) has been implemented.

- Req 5.7 the Trust-PDP **SHOULD** provide sufficient performance.

- Req 5.7a The Trust-PDP SHOULD be able to handle high load traffic.
- Req 5.7b The Trust-PDP SHOULD perform well in a distributed and heterogeneous environment.
- Req 5.7c The Trust-PDP SHOULD be able to support mechanisms for caching decisions and determining the need for re-evaluation.

Design: The trust PDP design specifies different policy levels allowing a trade-off between complexity (and corresponding performance) and expressiveness. The Trust PDP does not have to be run local to the resource but can be offloaded to a high performance machine.

Implementation: The trust PDP implementation provides a caching mechanism for credentials. The dynamicity of reputations and KPIs implies that caching should occur on the trust service side.

- Req 5.8 the Trust-PDP SHOULD be open and flexible enough to support multiple systems.

Design: The trust PDP is open ended; it only specifies the basic requirements that a trust service should fulfil to be useable in the system.

Implementation: The trust PSP is easily extendable with additional services; a template needs to be provided with a java wrapper around an actual connection to the service and a specification of the supported function to support a new service. Generalization of this template will further reduce the effort needed to support a new trust service.

- Req 5.8a the Trust-PDP interface definition SHOULD be open.

Design and Implementation: Standard and open XACML interface is used, fully satisfying this requirement.

- Req 5.8b the Trust-PDP SHOULD be implementable without imposing proprietary solutions.

Design is open and the prototype implementation is built using open source software and is itself open source.

5.3.1 Dependencies

- Req 5.9 the Trust-PDP SHOULD integrate well in the TAS3 middleware and be implementable on different systems.
 - Req 5.9a the Trust-PDP SHOULD accept queries expressed in XACML request style format.
 - Req 5.9b the Trust-PDP SHOULD respond with XACML style response messages.
 - Req 5.9c the Trust-PDP SHOULD be able to retrieve trust policies and attributes from a trust policy administration/information point.

Design: The Trust-PDP design satisfies these requirements.

Implementation: The current implementation supports XACML v2 requests, responses and can use standard XACML PAP facilities for retrieving policies. Extensions will be needed to support new features of the v3 of the standard (under development) such as policies embedded in the request.

5.4 Trusted Application Infrastructure

5.4.1 Architectural

Components of the “Trusted Application Infrastructure” are built as web services and therefore they need clearly designed interfaces.

- Req. 8.3: “Obligations Watchdog Service”: a service SHOULD be able to attach obligations to requests or responses.

5.4.2 Dependencies

- Req. 8.4: “Audit Guard Service”: a service SHOULD be able to log outgoing requests, policies, and transactions.

5.5 Integration Requirements

- Req 12.1 All components of the system SHALL be constructed and configured in such a way that no single failure of any component can reduce the security and trustworthiness level of any other component or the system as a whole. NOTE this does not mean that the system SHALL be reliable in terms of uptime or throughput performance.
- Req 12.2 If any component encounters trouble, the system SHALL be able to correctly identify the root cause of the problem using log escalation and other techniques.
- Req 12.3 to improve trustworthiness, the system SHALL have a clear time limit on failure fix attempts. Beyond the time limit, a routine rollback to a known-secure state SHALL be executed.
- Req 12.4 wherever possible, the system SHALL deploy standard software components to perform well-defined tasks instead of integrating these tasks into custom software. NOTE the reasoning is that this SHOULD reduce the chance of error and lowers the maintenance burden on the developers.
- Req 12.5 the relevant interface specifications SHALL be published on a revision-controlled system with mandatory subscription, so that any changes can be guaranteed to reach the relevant developers.
- Req 12.6 All components of the system SHALL be built using strict quality assurance procedures, with evidence of the process available.
- Req 12.7 All components of the system SHALL be certified for compliance with TAS3 security requirements (“play the game”) and evidence SHALL be available that these components have not seen uncertified changes since the certification.

- Req 12.8 to improve trustworthiness, the system SHALL implement Audit Guards in all relevant places as early as possible.
- Req 12.9 to improve trustworthiness, the system SHALL implement constellation-wide testing facilities as early as possible. These facilities will be used to do early certification testing and run-time monitoring.
- Req 12.10 to improve trustworthiness, the system SHALL have clearly distinct roles and duties for developers and administrators.

6 Legal Requirements

The legal requirements of TAS³ emanate primarily from the EU Data Protection Directive and its national implementations. While these requirements apply as a matter of law to all the actors and the transactions involved, TAS³ has chosen to specify them as requirements and incorporate them into the policy and contractual framework. The recital of these legal requirements in these instruments will help achieve compliance and oversight across TAS³ by making those requirements actionable and enforceable by the parties responsible for oversight. Obviously recourse to national data protection authorities and the courts always remains possible, but we also hope to provide the data subject with more simple paths to compliance enforcement that can be accomplished within the TAS³ network (through its architecture and participants).

Contract and Policy Framework: The combination of TAS³ policies and the contractual framework creates a data governance model for TAS³. TAS³ consistent policies will reflect both the legal requirements as well as the need to respect choices of data subjects that may create even greater restrictions on the collection and/or use of data. The policies and contractual framework are being designed to both support and complement the technical infrastructure. The contractual framework operates on three different levels. The *first level* pertains to the infrastructure or ‘ecosystem level’. This contract is signed by all users and participants and binds them to the general policies, terms and conditions related to the use of the TAS³ architecture. This contract is referred to as the ‘TAS³ Framework Agreement’ or the ‘TAS³ Ecosystem Contract’. This contract will also specify how and to which entity complaints and concerns should be addressed. The terms related to data subjects signing this contract will be limited to those expressed in the intake process, with additional obligations as needed (e.g., to take reasonable steps to maintain the security of the password/credential they use to log into the system and not to engage in prohibited/fraudulent/deceptive activities on the system).

The *second level* of the contractual framework is at the level of the participants to the TAS³ Network. This is the level at which the respective functions and roles of entities participating to the TAS³ network are contractually addressed. These contracts contain supplemental instructions and obligations in light of the specific transactions the participant is likely to engage in. The contracts of this type are referred to as ‘TAS³ Participant Contracts’, which supplement the TAS³ Ecosystem Contract.

The contracts at this level may exist in two forms. For entities that are most likely to play one or a limited number of roles with clearly delineated functions, it may be possible to draft single role-based participant contracts to supplement the Ecosystem Contract. These contracts are likely to be of a more general application and could be concluded during the intake process. For participants with more dynamic or varying functions/roles, which are more context-dependent, it will not be possible to conclude all the relevant participant contracts during the intake process. Many role-based obligations will only be definable at the moment where it is clear which transaction is envisaged. This creates the need for a more dynamic contracting process. By specifying

obligations based on roles and functions at the transactional level, we will be able to rapidly tailor the obligations of participants in accordance with the types of processing operations they are expected to perform. This contracting ‘on-the-fly’ (CotF) model will be developed based on the same concepts that underlie service oriented architectures or object-based programming. We will explore developing a automated process functions for associating predefined roles and obligations to participants based on uses of information.

The *third level* of the contractual framework is at the technical operational level. This is the level at obligations and restrictions are associated to personal data elements in the form of sticky policies.¹ . The Ecosystem Contract will ensure legal binding and effect to restrictions and obligations contained in those sticky policies by ensuring that participants agree to be bound to follow the instructions provided at the technical operational level. The latter is important as some legislation may still require the concept of a “writing” (written document) to give legal effect to such an instruction.

While beyond the scope of TAS³, participating organizations must develop appropriate clauses within their employment contracts and related policies to assure that employees are properly bound to organizational policies that correctly reflect these obligations.

The following requirements have been developed from the legal and contractual framework set forth D6.1 and D6.2. Some of these requirements were initially defined in D1.2. The current list of requirements is a refinement and further elaboration of those requirements based on the increased understanding of the architecture and the deliverables of other partners. This list is not exhaustive and will continue be updated in future versions of D6.1. For readability purposes, we have grouped the requirements below in terms of data protection and more general operational requirements. Several requirements additionally have explanatory ‘notes’ associated with them to draw attention to certain specificities or additional considerations which need be taken into account during implementation.

As to the vocabulary used in the expression of these requirements, we would like to note the following. The term ‘MUST’ is used to express that there is a direct legal obligation (emanating either from the EU Data Protection Directive 95/46/EC, national implementations or contract law) to comply with this requirement. The term ‘SHOULD’ is used to indicate that the articulated requirement does not reflect a clear and direct legal obligation, but rather is reflective of a ‘best practice’ which may enhance (but also facilitate) compliance. The term ‘SHALL’ is used where the articulated requirement is again not a clear and direct legal requirement, but will nevertheless need to be implemented in order to achieve the objectives of the TAS³.

¹ For more information concerning use of sticky policies in TAS³ see TAS³ D7.1 (Design of Identity Management, Authentication and Authorization Infrastructure) and TAS³ D2.1 (Architecture).

6.1 Enrolment and contractual binding

- Req 6.1: Intake Process (Person). The intake process **MUST** include: documentation provisioning (including notice of privacy policy, disclaimers, and general terms & conditions) and agreement to be bound; validation of identity (proofing) with an appropriate level of assurance; and specification of a technical user interface.
- Req 6.2: Intake Process (Organization). The intake process **MUST** include: documentation provisioning (terms & conditions, privacy policies, disclaimers) and agreement to be bound; validation of identity with an appropriate level of assurance; verification of policies, contracts, infrastructure and the capacity to comply; and specification of technical interfaces and protocols.
- Req 6.3: Contract management. All participants to the TAS³ network **MUST** agree to adhere to and execute the relevant TAS³ contractual documents.
 - Req 6.3.1: A versioning and archiving system **MUST** exist for contract terms.
 - Req 6.3.2: A versioning and archiving system **MUST** be in place for the informed consents given by data subjects.
 - Req 6.3.3: It **MUST** be easy to ascertain which terms were in force, after the fact, if an issue arises (e.g. pursuant to a complaint or detected anomaly).
- Req 6.4: Use of TAS³ Technology and Processes. All parties **MUST** agree to use the relevant TAS³ or TAS³ compatible technology and processes.
- Req 6.5 (EDITED): Binding Effect of technical processes & 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.
 - Req 6.5.1 (EDITED): 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).
 - Req: 6.5.1: The content of the instructions contained in (sticky or other) policies and the obligations associated with those instructions **MUST** be respected across the TAS³ architecture;
 - Req 6.5.2: It **MUST** be ensured that commitment to communicated policies and privacy preferences cannot be repudiated at a later time;
 - Req 6.5.3: In instances where personal data will be further processed outside the TAS³ network/architecture, the recipients of this data **MUST** commit to continued adherence to the content of associated sticky policies or other usage directives;
 - Req 6.5.4: Policy information **MUST** be easily accessible to all relevant parties;

- Req 6.5.5 Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience², so as to enable all relevant parties to understand their scope of application and which resources (data, services etc.) are governed by which policies³;
- Req 6.6 (EDITED): Implementation of Required Policies. Organizations participating in the TAS³ network SHALL be bound to implement TAS³ defined or compatible policies (e.g. internal privacy and security policies) or as approved during the intake process.
- Req 6.7: The TAS³ policy framework MUST cover all aspects of data processing and the associated legal data protection requirements.

6.2 Assignment of roles and responsibilities

- Req 6.8: Allocation of roles and responsibilities: Responsible entities and roles SHALL be defined for at least the following tasks:
 - receiving and registering consent;
 - providing notice and transparency;
 - performing the appropriate authentications, authorizations and checks for every processing operation;
 - the maintenance of logs for the different processing operations that take place;
 - trusted (third) party services (e.g. attribute certification, identifier conversion etc);
 - enforcement and updating of technical policies in accordance with permissions granted by data subject and legal developments;
 - front-end accommodation of the rights of data subjects such as the right of access and correction;
 - oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach.

² See: UK ICO: Privacy Notices Code of Practice (2009) at pp. 11-12; http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (for general consideration of drafting public facing documents related to privacy. These concepts are further reflected in codes of practice e.g. UK ICO Framework Code of Practice for Sharing personal information (2009 Consultation Draft at P.7): On the avoidance of legalistic language and adopting a plain-English, readable approach see http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf

³ See: UK ICO: Privacy Notices Code of Practice (2009) at pp. 11-12; http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (for general consideration of drafting public facing documents related to privacy. These concepts are further reflected in codes of practice e.g. UK ICO Framework Code of Practice for Sharing personal information (2009 Consultation Draft at P.7): On the avoidance of legalistic language and adopting a plain-English, readable approach see http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf

- Req 6.9 (NEW): Separation of duties: roles and responsibilities relating to the management of the TAS³ network, in particular those relating to policy enforcement, audit and oversight SHOULD be allocated in a way which limits the risk of conflict of interests.

6.3 Legitimacy of processing

- Req 6.10: 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.
 - Req 6.10.1: Data subject consent legitimizing the processing MUST be freely given, informed⁴, and unambiguous⁵.
 - Req 6.10.2: Where required by the competent jurisdiction (e.g. in case of processing of health data), or where this is considered desirable for later evidentiary purposes, the consent of the data subject MUST be in writing (or electronic equivalent thereof).
- Req 6.11: In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted ('legitimate') basis MUST be present to justify the processing.⁶
- Req 6.13: The TAS³ network SHALL provide the data subject, if so desired, with the ability to express his privacy preferences in a granular fashion (avoid "all or nothing" approach when possible; support individual privacy preferences)
- Req 6.14: The TAS³ network SHOULD consider technical policy enforcement mechanisms which can establish that there is in fact a legal basis for the processing prior to authorizing an action (e.g. by specifying them as policy conditions or through use of sticky policies)
- Req 6.15 (NEW): Consent revocation and modification of privacy preferences: a mechanism or procedure MUST be specified which ensures that in instances in which the data subject either revokes her consent or modifies her privacy preferences, no further processing operations shall be carried out for which the legitimacy is no longer ensured.

6.4 Finality

- Req 6.16: Purpose specification. The purpose(s) for collection and subsequent processing of personal data MUST be clearly specified.

Note: the purpose(s) of processing MUST be identified in advance (prior to initial collection, transfer, ...).

⁴ A consent may be considered informed when it satisfies all the elements listed in Req 6.50.

⁵ From a technical point of view, this requires that the user "opts in" to the processing of personal data.

⁶ See articles 7-8 of the Data Protection Directive.

- Req 6.17 (EDITED): 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 be obtained from the data subject prior to this new or changed use, unless this processing is explicitly required or permitted by law.⁷
- Req 6.18: Each participant of the TAS³ network MUST have a privacy policy that articulates restrictions and obligations with regards to subsequent use of the personal data it has under its control.
- Req 6.19: When personal data is forwarded from one TAS³ participant to another (or from a participant to a non-participant), it MUST be determined under which policies (in particular: under which restrictions and obligations) this data is being passed on.⁸
 - Req 6.19.1: Such data handling policies MUST be compatible with the TAS³ governance framework;
 - Req 6.19.2: 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);
 - Req 6.19.3: The data subject SHALL be provided with additional and explicit information if the if a requestor/future recipient of information is not a part of the TAS³ network.
- Req 6.20: Technical policy enforcement mechanisms SHALL be able to take into account the specified purpose when evaluating a processing request when appropriate. See also Req 6.21.
- Req 6.21: In order to enable verification that there has been a legitimate basis for processing, there SHALL be appropriate logging of asserted purposes and the ability to audit how the information was used against the purpose for which it was collected.

Note: Seeing as such information (the purpose for which a processing can be authorized / has taken place) can be highly-sensitive in and of itself, careful consideration MUST be given to deciding which entity shall be trusted to register and verify the asserted/permitted purposes.

6.5 Data minimization

- Req 6.22: The collection and further processing of personal data MUST be relevant and non-excessive in relation to the specified purposes (see Req 6.16).

⁷ In instances where the subsequent processing cannot be based on the consent of the data subject, an alternative legally permitted ('legitimate') basis must be present to justify the subsequent processing (see also Req 6.11).

⁸ This will typically only be a subset of the actions the forwarding entity is authorized to perform.

Note: the processed data **MUST** also be adequate to achieve the specified purpose.

- Req 6.23: Collection Limitation: The TAS³ network and related processes **MUST** install appropriate limits on personal data collection to what is needed for legitimate, identified and notified business purpose.
- Req 6.24 (EDITED): 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 (sufficient level of granularity). See also Req 6.40.
- Req 6.25: Selective attribute/personal data disclosure during authentication: Authentication protocols **MUST** be designed in a way which ensures that no more attributes/personal data than needed for the processing are verified or propagated (e.g. avoid unnecessary leaking of identifiers).
 - Req 6.25.1: 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.).
- Req 6.26: Storage limitation: Procedures **MUST** be in place to ensure destruction or anonymization of personal data once the purpose for which it was collected and/or further processed has been completed
 - Req 6.26.1: Prior to initiating any processing operation upon personal data, the storage duration of each data element **MUST** be specified, either individually or by category, for every entity that is involved in the processing. This **SHALL** be done as part of the service/process definition.
 - Req 6.26.2: Data Management. Data **MUST** be managed according to a data life cycle which describes its management from collection to deletion, and all processes in between, including which events trigger which processes.
 - Req 6.26.3: The TAS³ network **SHALL** support technical obligations languages which allow data providers to specify the time-span after which deletion is mandatory.

Note: determining appropriate storage duration **MUST** also take into account the need for accountability at a later time, as well as legally prescribed retention periods. In case the data only needs to be retained for a subset of the initially specified purposes, appropriate measures **MUST** be taken to limit the further processing to these (more limited subset of) purposes (e.g. encrypted archiving).

- Req 6.27 (NEW): Data minimization : appropriate measures **MUST** be in place to avoid unnecessary duplication of personal data in multiple repositories.

6.6 Data accuracy

- Req 6.28: Designation of authoritative sources: In order to ensure data accuracy to the fullest extent possible, an inventory **MUST** be maintained that describes which entities are authorized to act as data providers (authoritative source) for which data sets.
- Req 6.29.: Verification procedures **MUST** be in place to ensure the trustworthiness of each attribute with a level of assurance proportionate to the interests at stake.
 - Req 6.29.1: Where appropriate, review and update procedures **MUST** be in place for personal data which is being kept for an extended period of time.
- Req 6.30: Procedures **MUST** be in place on how to report and deal with suspected inaccuracies.
 - Req 6.30.1: Data subjects **MUST** have the ability to check the accuracy and quality of the data, and to report suspected inaccuracies. (see Reqs 6.58 et seq.);
 - Req 6.30.2 (EDITED): 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;
 - Req 6.30.3: In case of amendment, notification **MUST** be provided to relevant entities (e.g. entities to whom data has been forwarded / who have accessed the data and continue to rely on it) (see also Req 6.65)
- Req 6.31: Where further verification or assurance of data quality is still needed, there **MUST** be a clear indication of the need for further verification when appropriate.
 - Req 6.31.1: Indication of level of confidence: each element of personal data **SHOULD** have a 'level of confidence' associated with it (e.g. self-asserted, verified with authoritative source by trusted data manager, inaccuracy reported etc) and this level of confidence **SHOULD** be reflected in its meta-data where appropriate.
- Req 6.32: The integrity of data maintained in authoritative sources **MUST** be appropriately guaranteed.
 - Req 6.32.1: Modification rights **MUST** be restricted to authorized entities on a 'need-to-modify' basis.
- Req 6.33: Data to and from authoritative sources **MUST** be authenticated through use of data origin authentication protocols to ensure authenticity and integrity where appropriate.
- Req 6.34: Relying Parties and other data recipients **SHALL** commit to only process personal data further if there is sufficient certainty as to its origin and integrity (i.e. upon verification that it emanates from the trusted source and has not been subject to unauthorized manipulation).

- Req 6.34.1: Policies SHALL be in place which specify how a ‘sufficient level of certainty’ as to the origin and integrity of personal information is established.
- Req 6.35 (NEW): Unambiguous identification: TAS³ participants MUST ensure unambiguous identification of the data subjects with whose data they process.

Note: This requirement does not entail that data subjects must be consistently identified in the same manner across service providers. See also Req 6.44.

6.7 Confidentiality and security of processing

- Req 6.36: Confidentiality. Appropriate organizational and technical security measures MUST be in place to ensure the confidentiality of personal data.
- Req 6.37: Security. Appropriate technical and organizational measures MUST be in place to protect against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data.
- Req 6.38: An organizational framework for information security management (describing both organizational and technical measures) MUST be in place.
- Req 6.39: Identity and credential life cycle management. Policies and measures to ensure appropriate identification and authentication of entities attempting to perform a particular action MUST be in place.
 - Req 6.39.1: Identities and credentials MUST be managed in way that they continuously provide a level of assurance proportionate to the interests at stake;
 - Req 6.39.2: Common authentication approaches and rules MUST be defined and enforced;
 - Req 6.39.3: Adequate policies specifying minimum levels of entity authentication assurance in a manner that is proportionate to the interests at stake MUST be in place;
 - Req 6.39.4: Adequate procedures to ensure proper verification of relevant attributes of requesting/asserting entities (e.g. a pre-requisite professional qualification) MUST be in place (e.g. through use of authoritative sources as an integrated component in user- and access management).
 - Req 6.39.5: Adequate measures and procedures MUST be in place to properly address instances in which the levels of assurance associated with a particular identity or credential has been compromised (e.g. identity theft), or there is a reasonable likelihood thereto. Such measures might include credential revocation, notification to trust & reputation engines, etc.
- Req 6.40: Authorization. Technical policy enforcement mechanisms MUST support a sufficient level of granularity with regards to the access and further

processing rights (privileges) of each requesting entity. To this end at least the following measures **MUST** be taken (see also Req 6.24):

- Req 6.40.1: A list and directory of resources (e.g. applications, data) and categories of potential users/data recipients **MUST** be made.
 - Req 6.40.2: Personal data contained in data repositories **SHALL** be categorized according to a classification system that recognizes type and sensitivity of data.
 - Req 6.40.3: Roles and privileges of each entity **MUST** be defined based on legitimate organizational needs (in other words, on a “need-to-process” basis).
 - Req 6.40.4: For each object that qualifies as personal data a list of valid recipients **MUST** be defined or definable immediately upon request at any point in time;
 - Req 6.40.5: Acceptable purposes for access to data categories **MUST** be defined, emergency procedures for access beyond those purposes **SHALL** also be defined (break-the-glass).
 - Req 6.40.6: Authorization profiles for resources **MUST** be defined and enforced; indicating which resource is accessible to which type of entity/application in which capacity, in what situation and for what time period.
 - Req 6.40.7: Adequate measures and procedures **MUST** be in place to properly address security breaches, including notification of relevant entities (e.g. audit & oversight committee)
- Req 6.41 (NEW): Delegation authorization policy: prior to allowing a delegation of privileges to take place, it **MUST** be verified that the delegator is in fact authorized to delegate those privileges (and to the envisaged delegate).
- Req 6.42: Use of cryptography. TAS³ **MUST** support the use of cryptography to ensure confidentiality, authenticity and integrity of personal data where appropriate.
- Note: this requirement pertains both to transmission (channel security) and storage.
- Req 6.43 (NEW): Mutual authentication: appropriate safeguards must be implemented to ensure that users are not misled into providing personal data to an unauthorized entity.
- Req 6.44: 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..
- Req 6.45 (NEW): 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).
- Req 6.45.1 (NEW): 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.

- Req 6.46: Physical access restriction: Physical access to terminals and other resources MUST be restricted where appropriate.
- Req 6.47: Each participant MUST adopt internal privacy policies documenting security measures (specifying inter alia the persons responsible within the organization (e.g., security officers), what to do in the event of a security breach etc.).⁹
- Req 6.48: Confidentiality agreements. Natural persons who are employed by (or otherwise perform services for) TAS³ participants MUST be bound by a contractual duty to respect the confidentiality of data when this is required by law.¹⁰ TAS³ SHOULD consider instituting such an obligation towards all TAS³ participants.

The list of organisational and technical measures described here is by no means exhaustive. Additional examples of potential obligations pursuant to the requirements of confidentiality and security are listed below the requirements.*

6.8 Transparency and notice

- Req 6.49: Whenever personal data shall be processed, the following MUST be specified: the identity of the controller, what data is collected and how, why it is being collected (purpose of the processing), how it will be used, who it might be shared with, and how it will be managed.¹¹

6.8.1 Direct collection

- Req 6.50: Notice requirements where data is collected from data subject herself (direct collection):
 - Req 6.50.1: In case of direct collection, the data subject MUST be provided with the following information (except where he already has it):
 - the identity of the controller (and, if applicable, of his representative);
 - the purposes of the processing for which the data are intended;
 - Req 6.50.2: The data subject SHOULD also be informed of:
 - the recipients or categories of recipients of the data;

⁹ Such policies must of course be compatible with the TAS³ governance framework.

¹⁰ E.g. in certain jurisdictions such agreements are required when such employees or contractors are charged with handling of sensitive data such as health data.

¹¹ The data subject MUST in principle be notified of the elements listed in Req 6.49 prior to initiating any (entirely new or 'incompatible') processing operation involving personal data (or at least have access to this information upon request – see Req 6.53).

- whether replies to questions he is asked are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data concerning her.
- Req 6.50.3: The data subject **MUST** be provided with the information listed in Req 6.44.2 when this is necessary to guarantee fair processing in respect of the data subject, when considering the specific circumstances in which the data are collected.

6.8.2 Indirect collection

- Req 6.51: Notice requirements where data is not obtained directly from data subject herself (indirect collection):
 - Req 6.51.1: In case of indirect collection, the data subject **MUST****, at the moment of undertaking, or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, be provided with the following information:
 - the identity of the controller and of his representative, if any;
 - the purposes of the processing;
 - Req 6.51.2: The data subject **SHOULD** also always be informed of:
 - the categories of data concerned;
 - the recipients or categories of recipients;
 - the existence of the right of access to and the right to rectify the data concerning her
 - Req 6.51.3: The data subject **MUST** be provided with the information listed in req 6.28.2 when this is necessary to guarantee fair processing towards the data subject (taking into account the specific circumstances in which the data are collected) or when this is required by the applicable national legislation.

**** Note:** Requirements 6.51.1-3 **MAY** in principle be discarded where:

- where it is certain that the data subject already has such information;
- where the processing takes place for statistical purposes or for the purposes of historical or scientific research;
- the provision of such information proves impossible or would involve a disproportionate effort; or
- disclosure is expressly mandated by law.

6.8.3 Implementation

- Req 6.52: All the information elements listed in Reqs 6.44-6.45 SHALL be made readily available to (both actual and potential) data subjects in the form of a privacy policy (or policies), which is (are) both easily accessible and easy to understand.
- Req 6.53: Layered approach. In order to limit complexity, the fulfilment of Reqs 6.51-6.52 need not necessarily take the form of a single document.¹² TAS³ SHALL adopt a 'layered' approach for notice when appropriate.
 - Req 6.53.1: This approach SHALL NOT contain more than three layers of information (short – condensed – full)
 - Req 6.53.2: The sum total of these layered notices MUST meet the notice requirements imposed by the applicable national legislation.
 - Req 6.53.3: It MUST be easy to ascertain which data processing operations are governed by which policies.
- Req 6.54: Privacy policy for TAS³ portal (full notice). The privacy policy notice provided on the TAS³ portal SHALL not only cover the processing operations performed by the portal provider itself, but SHALL also include a general notice with regard to the operations of entities participating to the TAS³ network as service providers.
 - Req 6.54.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information and redress mechanisms
 - Req 6.54.2: This general privacy policy SHOULD reference and link the privacy policies maintained by TAS³ participants (see Req 6.55) when appropriate.
- Req 6.55: Each entity participating in the TAS³ network as a service provider MUST also provide notice of its own privacy policy (policies), which provides further details specific as to its particular processing operations.
 - Req 6.55.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information on redress mechanisms
 - Req 6.55.2: These privacy policies SHOULD also cross-reference the TAS³ infrastructure privacy policy where appropriate.
- Req 6.56: Consent to notices. The consent of the data subject MUST (as a rule¹³) be obtained in relation to privacy policies listed in 6.47-48 prior to any processing of his personal data, by either TAS³ Infrastructure Members or one of the participating TAS³ entities (see Req 6.10).

¹² See Article 29 Data Protection Working Party, 'Opinion on More Harmonized Information Provisions', WP100, 25 November 2004, p. 8-9.

¹³ In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted basis must be in place (see Req 6.11). This situation does not remove the obligation to inform the data subject of such processing (see Reqs 6.49 et seq.)

- Req 6.56.1: A versioning and archiving system **MUST** be in place for the informed consents given by data subjects to enable later verification that appropriate notice was given (see also Req 6.3)
- Req 6.57: If any entity within the TAS³ network intends to process personal data for an additional purpose (i.e. a purpose which has not yet been previously specified and communicated to the data subject), a subsequent notice **MUST** be provided, and the data subject **MUST** be given the ability to either accept or reject the envisaged processing, **EXCEPT** where the processing is mandated by a legal obligation (see also Req 6.17).¹⁴

6.9 Data subject rights of access, rectification, blocking and erasure

- Req 6.58: Access request process/Accuracy: a process **MUST** be in place which enables users to request access to (and possibly amend or correct) personal data relating to them which has or is being processed within the TAS³ network.
- Req 6.59: Blocking and erasure: a process **MUST** be in place which enables blocking or erasure of specific data elements upon request of the data subject, unless the processing is specifically mandated by law.

6.9.1 Right of access

- Req 6.60: Upon request, the data subject **MUST** be provided with confirmation, as to whether or not data relating to her are being processed, and information at least as to:
 - the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are (have been) disclosed;
 - the data undergoing processing and of all available information as to its source;
 - the logic involved in the processing of data particularly where automated decisions are involved.
- Req 6.61: The confirmation and information listed in Req 6.53 **MUST** be provided without constraint or excessive delays or expense.

¹⁴ Req 6.57 does not apply where the processing is based on a legally admissible basis other than consent AND where such notice is impossible or would involve a disproportionate effort. However, such instances of overriding legitimate interest **MUST** at least be generically outlined in the TAS³ privacy policy notice(s) mentioned in Reqs 6.54-55.

6.9.2 Rectification, blocking and erasure

- Req 6.62: Data subject requests to rectify, block or erase data MUST be accommodated at all times EXCEPT where an overriding legitimate interest exists.
 - Req 6.62.1: Such overriding interest SHOULD be specified in the TAS³ privacy policy notice(s).
 - Req 6.62.2: Data subject requests to rectify, block or erase data MUST in any event be accommodated in case the processing infringes upon the applicable national data protection legislation.
 - Req 6.62.3: In case of denial, the reason for denial MUST be communicated to the data subject.
- Req 6.63: The TAS³ privacy policy MUST specify:
 - to which entity in particular data subjects should address their request for access, rectification, blocking or erasure in which instance;
 - which entity shall decide these requests;
 - valid reasons for denying the request;
 - the time-frame in which this request will be processed;
- Req 6.64 (EDITED): A 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.

6.9.3 Notification to third parties

- Req 6.65: A process MUST be in place that provides notification to third parties to whom the data have been disclosed in case of corrections, erasure of blocking of processing of personal data pursuant to a request by the data subject.

6.9.4 Implementation

- Req 6.66: The TAS³ user interface ('dashboard') SHALL make all the information listed in Reqs 6.53 readily available to data subjects in a user-friendly way.
- Req 6.67: Where appropriate, the TAS³ Dashboard SHOULD also provide data subjects with more detailed information as to the processing operations performed upon their personal data (e.g. at what time individual processing operations took place, under which pretext etc.).
- Req 6.68: The TAS³ Dashboard SHOULD provide an interface which enables exercise of the data subject rights listed in Reqs 6.55 (or at least direct the user as to how those rights may be exercised).
- Req 6.69: The TAS³ Dashboard SHOULD support automatic notifications to relevant parties in case of corrections, erasure of blocking of processing of personal data pursuant to a request by the data subject

6.10 Accountability and compliance verification

6.10.1 Logging¹⁵

- Req 6.70: Processing operations involving personal data **MUST** be logged with a sufficient level of detail.
- Req 6.71: The level of detail of log files **MUST** be sufficient as to enable compliance verification and oversight of processing operations with the governing policies
 - Req 6.71.1: Log files **MUST** detail which entity performed which action upon which resource, and at what time;
 - Req 6.71.2: Where appropriate, log files **SHALL** also record for which purpose (under which pretext the action took place/was authorized);
 - Req 6.71.3: Log files **MUST** contain explicit information as to the recipients to whom personal data has been transferred.

Note: Separation of duties **MUST** be considered to avoid situations where a single entity might have the ability to profile all the activities of end-users.

- Req 6.72: Reliability: Appropriate measures **MUST** in place to ensure the authenticity, accuracy, integrity and completeness of the logs.
- Req 6.73: Transparency. The fact that processing operations are logged **MUST** be transparent towards users through appropriate notification (see Reqs 6.49 et seq).
- Req 6.74: Proportionality: Logging **MUST** organized in a proportionate manner (e.g. storage in a pseudonymized or de-identified format, separation of duties).
- Req 6.75: Confidentiality: Appropriate measures **MUST** be in place to ensure the confidentiality of the logs. See also Req 6.36 et seq.
 - Req 6.75.1: Privileges to access nominative log information **SHOULD** in principle only authorize selective access (no ‘free search’);
 - Req 6.75.2: In case of non-targeted compliance verification (e.g. detection of anomalies through dedicated algorithms), the log data **MUST** first be de-identified/pseudonymized. Only after an anomaly has been detected may the log information be re-identified.

¹⁵ The logging of actions performed by entities within the TAS³ network will often also amount to processing of personal data. Where this is the case, such logging must also take into the requirements listed in this section.

6.10.2 Audit & oversight

- Req 6.76: The proper implementation and functioning of all technical mechanisms and organisational measures **MUST** be documented and audited on a regular basis.
- Req 6.77: Definition of roles & responsibilities (see Req 6.8) **MUST** also include assignment of tasks with regards to audit and oversight.
- Req 6.78: Each participant **MUST** be bound to provide co-operation to entities in the TAS³ network charged with oversight & audit.

6.10.3 Other accountability mechanisms

- Req 6.79: Both within the TAS³ network and within each participating entity internal responsibility and accountability mechanisms **MUST** be adopted (e.g. designating 'owners' for both equipment and processing operations where personal data is involved).
- Req 6.80: Technical non-repudiation mechanisms **MUST** be supported when appropriate. For example:
 - Req 6.80.1: When forwarding personal data, it **SHALL** be ensured that the sender is not able to later deny having forwarded it;
 - Req 6.80.2: It **SHALL** be ensured that the commitment to communicated policies and privacy preferences cannot later be repudiated at a later time.
- Req 6.81: Automated notifications **SHALL** be instituted for extraordinary processing operations (e.g. break-the-glass), and procedures **SHALL** be in place to further follow up such notifications (e.g. through audit & oversight committee).
 - Req 6.81.1: Automated notifications **SHOULD** also be considered for certain types of processing operations (e.g. access to particularly sensitive data)
- Req 6.82: Procedures **MUST** be in place to ensure that when requested it is possible to indicate the source of the personal data that is being processed, as well as what the reason for processing has been.
- Req 6.83 (NEW): 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.
 - Req 6.83.1 (NEW): 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.
 - Req 6.83.2 (NEW): 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:

- that the processor shall act only on instructions from the controller;
- that the processor is subject to the confidentiality and security obligations set forth by Directive 95/46/EC.
- Req 6.83.3 (NEW): processors and other recipients **MUST** be bound to only process this data in a lawful manner and in accordance with the policies of the TAS³ network. Members/participants must also ensure that the recipients adhere to all of the commitments they have themselves made towards the data subject.

6.10.4 Complaint handling

- Req 6.84: Complaint capture system: Potential abuses to the system or concerns of either users or organizations **MUST** be captured.
 - Req 6.84.1: The complaint capture system **SHOULD** include a feedback mechanism which enables users to both
 - provide information to reputation engines or other trust entities that may be evaluating service providers, and to
 - initiate procedures for privilege revocation as a consequence of intentional or uncured breach of terms, and corresponding redress.
 - Req 6.84.2: Appropriate levels of proof are required to justify the consequences listed in Req 6.84.1 and complaints should therefore be corroborated on the basis of logs and other relevant documentation
- Req 6.85: Redress/oversight Processes: Once a complaint is captured, redress **MUST** be possible. In addition, an oversight process **SHALL** be in place which **SHOULD** also be involved in pro-active detection of non-compliance.
- Req 6.86 (NEW): 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)
 - Req 6.86.1 (NEW): The operator of the Trust Reputation server **MUST** be bound to only process user feedback information in accordance with the user's policies

6.11 Notification & prior checking

- Req 6.87: Where required by the applicable law, the TAS³ network and/or its participants **MUST** ensure prior notification and/or prior checking with national data protection authorities

* Sample Service Provider Obligations: While actual contract instruments will need to be tailored to the role of the service provider, the following list measures is indicative of the types of controls which SPs may be obligated to implement:

- Use of up-to-date Anti-virus/ Spyware/ Malware detection systems
- Spam filters (may need to define settings to assure that legitimate mail is not suppressed)
- Penetration testing (may only be appropriate for largest players)ⁱ
- Encryption
 - In transit
 - At rest
- Security policies
 - Physical
 - Logical
 - Administrative
 - Separation of Duties
- Privacy policy
 - W/specific obligation to honour preferences and negotiated obligations of end-users
 - Notice
- Complaint handling policies / mechanism
- Compliance processes/officer
- Contact points
- Internet Access and Use Policies
- Training
- Code of ethics
- HR Policies (related to vetting of employees that have access to personal to the extent permitted by law)
- Service Level Agreements
- Breach Notification
- Disaster recovery / Business continuity plans/exercises
- Audit/oversight
- Exceptions and Emergencies handling policies
- Government/Law Enforcement obligations/request for information policies
- Third party agreements' obligations/requirements clauses

7 On-line Compliance Testing

7.1 On-line Compliance Testing

This section describes the requirements that concern the on-line compliance testing (OCT) activity, which is inspired by the CNR framework proposed originally under the name Audition [5][6]. The requirements are grouped in requirements imposed on the TAS³ infrastructure (Sec. 7.1.1), requirements imposed on the TAS³ registry (Sec. 7.1.2) and requirements imposed on the services that are to be deployed on the TAS³ infrastructure (Sec 7.1.3).

7.1.1 Requirements for the TAS³ Infrastructure

- Req. 10.1 Service Registration

Text: Services SHOULD undergo a registration phase.

Justification: Services providing to be accessed by other services SHOULD undergo a registration phase before accessing other services or being accessed by other services. When a service asks for registration in TAS³, an OCT session could be activated.

- Req. 10.2 Testing Robot

Text: TAS³ infrastructure MUST include a service testing robot.

Justification: In order to test services on-line, the TAS³ infrastructure MUST include a specific component able to retrieve/generate a test suite.

- Req. 10.3 Test Storage

Text: TAS³ infrastructure MUST provide a storage to save and retrieve test cases.

Justification: Test suites to be used for OCT purposes MUST be available through a suitable storage provided by the TAS³ infrastructure. Implementation of this requirement provides better guarantees over test suites control. The storage is used by the driver to retrieve test suites.

- Req. 10.4 Perpetual Testing

Text: The TAS³ architecture MUST support perpetual testing of services. (see Req. D1.2-10.1 at [7]).

Justification: 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). The OCT session SHOULD be activated periodically or event-driven.

- Req. 10.5 Mock Services

Text: TAS³ infrastructure SHOULD provide support to the definitions of mock services.

Justification: All invocations made during OCT SHOULD not lead to permanent consequences (e.g. spurious writes on databases or other undesired side-effects): proper indications of such operations and mock implementations of services might be required. Mock services will be used in place of services when a service undergoing OCT asks for references to required services.

- Req. 10.6 Machine-readable specifications

Text: Specification such as QoS constraint, policies, or service interfaces MUST be specified in a formal and agreed format, preferably using open standards.

Justification: Specification MUST be machine computable

7.1.2 Requirements on the TAS³ Infrastructure Registry Component

- Req. 10.7 Testing Registry

Text: TAS³ registry MUST be able to activate a testing phase when a service asks for registration.

Justification: To apply OCT the registry SHOULD not guarantee immediate registration to requiring services. Unless otherwise specified, registration within the directory SHOULD be linked to the results of the audition/testing phase. The registry SHOULD be able to start a testing phase when a service asks for registration.

- Req. 10.8 Service Registration

Text: Services that do not pass OCT SHOULD not be granted registration.

Justification: The registration SHOULD be denied to those services for which the associated test suite highlight some errors.

- Req. 10.9 OCT feedback to KPIs

Text: Results from OCT SHOULD be taken into account by KPIs (see Req 5.2 in this document).

Justification: The trust on a service that does not pass OCT SHOULD decrease (and viceversa).

- Req. 10.10 Pending Status

Text: TAS³ registry MUST be able to recognize services undergoing OCT.

Justification: To fully apply OCT it is required that the registry be able to put services undergoing the testing phase in a pre-publication state (“approval pending” status).

7.1.3 Requirements on Services deployed over the TAS³ Infrastructure

- Req. 10.11 Service are test-aware

Text: A Service deployed within a TAS³ choreography MUST be aware of the fact that it will undergo a testing phase.

Justification: This requirement asks the service developer to consider that the service will be submitted to a testing phase. All invocations made during the testing phase SHOULD not lead to permanent consequences (e.g. spurious writes on databases or other undesired side-effects).

7.2 Off-line Testing Phase

7.2.1 Testing of XML-based interchange and communication formats

- Req. 10.12 XML-Schema specification

All data exchanged as XML SHOULD conform to a Schema specified according to the XML-Schema standard.

Justification: Reference to a specified Schema favours interoperability and provides support for possible automated validation (e.g., by CNR's TAXI, see [8]).

7.2.2 Testing of response-time and availability of services (optional requirements)

Requirements in this section are optional. However, if off-line QoS testing MUST be carried out, all of them MUST be fulfilled.

- Req. 10.13 Service Under Test

Text: An implementation of one or more services under test MUST be available.

Justification: The test-bed generator SHOULD provide test-beds that help testers in assessing that a specific service implementation can afford a required level of QoS

- Req. 10.14 QoS property definition

Text: The definition of the QoS properties has to be considered SHOULD be given in a precise way. Also, the behavior expressed by such properties SHOULD be reproducible by an algorithm.

Justification: The test-bed generator (e.g. the CNR's Puppet, see [9]) cannot reproduce properties that are not computable

- Req. 10.15 Interactions among services

Text: Specifications describing how different services interact SHOULD be available.

Justification: Such specifications can be used to generate test-beds that mimic real-world scenarios.

8 Glossary

- **The Trust-PDP or Trust Policy Decision Point** is a component that returns a trust decision by evaluate the trust policies for a request passed to it in the form of an XACML request context. In the TAS³ architecture the Trust-PDP can be called by a master PDP so its decision can be combined with other aspects related to a request such as authorization (see also WP02 D2.1 deliverable).
- **Structural trust rules** can be simple trust statements as Provider X is trusted to supply Job Vacancies and the combinations trust relations for example when the party trusted to issue credentials is itself determined by trust rules; Provider X is trusted to supply Job Vacancies if a trusted Accreditation agency certifies them. An Accreditation agency is trusted to certify Providers if it is registered at a national registry and has a good reputation, etc.
- **Behavioural Factors** are aspects of feedback used in define a reputation. For example for a helpdesk one could consider politeness, responsiveness, usefulness of supplied information, etc. These factors may be combined into the reputation differently depending on the needs of the user.
- **KPIs or Key Performance Indicators** are combinations of different Business Performance factors such as Time to deliver, or number of patent application, etc.
- **The Trust Information Collector** is the point which gathers feedback information needed to calculate reputations (see also WP02 D2.1 deliverable).
- **PCP** Personal Competency Profile
- **SOA** : Service Oriented Architecture.
- **Audition** : Aiming at providing only high quality service to the users, the provider of a directory service can be interested in testing that the services asking for registration are of “good” quality. For this purpose, the directory could submit the service under registration to a verification step before granting the registration. The implementation of such process with respect to the technical assessment is called Audition (Automatic Model-Based Interface Testing In Open Networks).
- **Test Driver** : A dedicated software service that is able to run test suites on a service under test.
- **Test Storage** : A dedicated special software repository that stores test suites to be used by Audition.
- **Pending Status** : A service is in a pending status if it is registered to a directory service, but has not been tested by Audition yet.
- **Inactive Status** : A service is inactive if it needs to use services that are not yet available according to the registry.

- **TAXI** : Testing by Automatically generated XML Instances. It is a tool by CNR that generates XML instances from an XML Schema automatically. The methodology is largely inspired to the Category Partition testing technique.
- **PUPPET** : Pick UP Performance Evaluation Test-bed. It is an approach for the automatic generation of test-beds to empirically evaluate the QoS characteristics of a Web Service under development. Specifically, the generation exploits the information about the coordinating scenario, the service description (WSDL) and the specification of the agreed QoS properties.
- **QoS** : Quality Of Service
- **IDL** : Interface Description Language. For example within the standards of the family WS*, WSDL is an IDL.
- **Offline Testing** : Testing phase that includes the activities that are performed while no user ("paying customer") is using the service. Hence, off-line validation of a system implies that it is tested in one or more artificially evolving environments that simulate possible real interactions.
- **Online Testing** : Testing phase that concerns a set of methodologies, techniques, and tools to monitor a system after its deployment in its real working context.
- **AIPEP**, (Application independant PEP), The **AIPEP** can understand the standardised policy contents and therefore can potentially treat different outgoing messages in different ways: e.g. encrypt some, sign some, use SSL etc. The AIPEP sends the outgoing message to its peer AIPEP and includes details of the recipient application system (i.e. application endpoint) with the first message. The AIPEP at the receiving system strips off the security header and policy, enforces the policy (as before), then calls the PDP (as before). The application message is finally passed to the application dependent PEP at the specified application endpoint.

9 References

- [1] “The art of writing Specifications”. Internal SAP document from Andreas Bathelt SRM Quality Management, September 22, 2004.
- [2] “Requirements Engineering”. Second edition. Elizabeth Hull, Ken Jackson and Jeremy Dich. Springer. 2005.
- [3] “<http://www.amazon.com/exec/obidos/ASIN/0735622671/processimpact> More About Software Requirements: Thorny Issues and Practical Advice”. 2006. [Microsoft Press](#). A companion volume to *Software Requirements, 2nd Edition*. Karl Wiegers.
- [4] Trusted Architecture for Securely Shared Services, “Annex I - “Description of Work””. 29/11/2007
- [5] Bertolino and A. Polini. The Audition Framework for Testing Web Services Interoperability. In Proceedings of the 31st EUROMICRO International Conference on Software Engineering and Advanced Applications, pages 134-142, Sept. 2005.
- [6] A. Bertolino, L. Frantzen, A. Polini, J. Tretmans, Audition of Web Services for Testing Conformance to Open ~~Speci~~ Protocols. In J. Stafford, R. Reussner, C. Szyperski (Eds.), Architecting Systems with Trustworthy Components, special issue in Springer - LNCS n.3938.
- [7] The TAS3 Consortium, Report D1.2- Requirements Assessment. Seda Gurses (Eds.) Ver. 1.0 – 2009
- [8] A. Bertolino, J. Gao, E. Marchetti, A. Polini: TAXI - A Tool for XML-Based Testing. ICSE Companion 2007
- [9] A. Bertolino, G. De Angelis, L. Frantzen, and A. Polini. Model-based Generation of Testbeds for Web Services. In Proc. of the 20th IFIP Int. Conference on Testing of Communicating Systems (TESTCOM 2008), LNCS. Springer Verlag, 2008.
- [10] G. Elahi, E. Yu, and N. Zannone, “A Vulnerability-Centric Requirements Engineering Framework: Analyzing Security Attacks, Countermeasures, and Requirements Based on Vulnerabilities,” *Requir. Eng.*, 2010.
- [11] L. Liu, E. Yu, and J. Mylopoulos, “Security and Privacy Requirements Analysis within a Social Setting,” in Proc. Of RE’03. IEEE, 2003, pp. 151–161.
- [12] F. Massacci, J. Mylopoulos, and N. Zannone, “Security Requirements Engineering: the SI* Modeling Language and the Secure Tropos Methodology,” in *Advances in Intelligent Information Systems*. Springer, 2010, pp. 147–174

- [13] G. Sindre and A. L. Opdahl, "Eliciting security requirements with misuse cases," *Requir. Eng.*, vol. 10, no. 1, pp. 34–44, 2005.

10 Annexes

10.1 Modelling with Secure Tropos

10.1.1 The Key Concepts

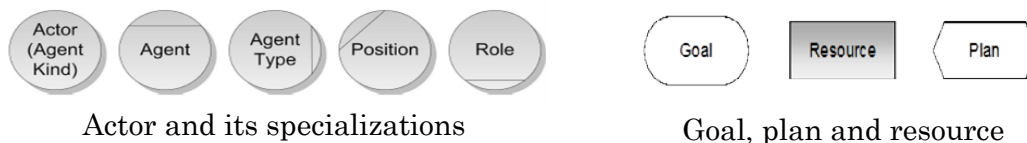
The main concepts in Tropos are: actor, goal, plan, resource and dependency. The graphical notations related to these concepts are represented in Figure 9.

An actor models an entity that has strategic goals and intentionality within the system or the organizational setting. It represents a physical or a software agent as well as a role or position. The role is defined as an abstract characterization of the behaviour of a social actor within some specialized context or domain of endeavour, and a position represents a set of roles, typically played by one agent. An agent can occupy a position, while a position is said to cover a role.

A goal represents actors' strategic interests. We distinguish hard goals from softgoals, the second having no clear-cut definition and/or criteria for deciding whether they are satisfied or not. Softgoals are typically used to model non-functional requirements.

A plan, represents, at an abstract level, a way of doing something. The execution of plan can be a means for satisfying a goal or for satisfying a softgoal. – A resource represents a physical or an informational entity. The main difference with an agent is that a resource has not intentionality.

Dependency between two actors, which indicates that one actor, depends, for some reason, on the other in order to attain some goal, execute some plan, or deliver a resource. The former actor is called the depender, while the latter is called the dependee. The object around which the dependency centers is called dependum. In general, by depending on another actor for a dependum, an actor is able to achieve goals that it would otherwise be unable to achieve on its own, or not as easily, or not as well. At the same time, the depender becomes vulnerable. If the dependee fails to deliver the dependum, the depender would be adversely affected in its ability to achieve its goals.



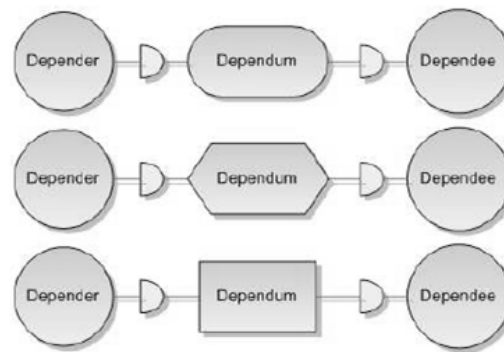


Figure 9 : Graphical Notations of Tropos concepts for dependency

Five new relationships have been introduced in Secure Tropos: ownership, provisioning, request, trust and delegation. The graphical notations corresponding to these notions are represented in Figure 10.

Ownership, which indicates that the actor is the legitimate owner of some goal, some plan, or some resource. The owner has full authority concerning to achieve his goal, execute his plan, or use his resource, and he can also delegate this authority to other actors.

Provisioning, which indicates that the actor has the capability to achieve some goal, execute some plan, or deliver a resource.

Request, which indicated that the actor intends to achieve a goal, execute a task, or requires a resource.

Trust, between two actors, which indicates the believe of one actor that the other does not misuse some goal, some plan, or some resource. The former actor is called the truster, while the latter is called the trustee. The object around which the dependency centers is called trustum. In general, by trusting another actor for a trustum, an actor is sure that the trustum is properly used. At the same time, the truster becomes vulnerable. If the trustee misuses the trustum, the truster cannot guarantee to achieve some goal, execute some plan, or deliver a resource securely.

Delegation, between two actors, which indicates that one actor delegates to the other the permission to achieve some goal, execute some plan, or use a resource. The former actor is called the delegator, while the latter is called the delegatee. The object around which the dependency centres is called delegatum. In general, delegation marks a formal passage in the domain that is currently modelled by the requirements engineers. This would be matched by the issuance of a delegation certificate such as digital credential or a letter if we are delegating permission or by a call to an external procedure if we are delegating execution.

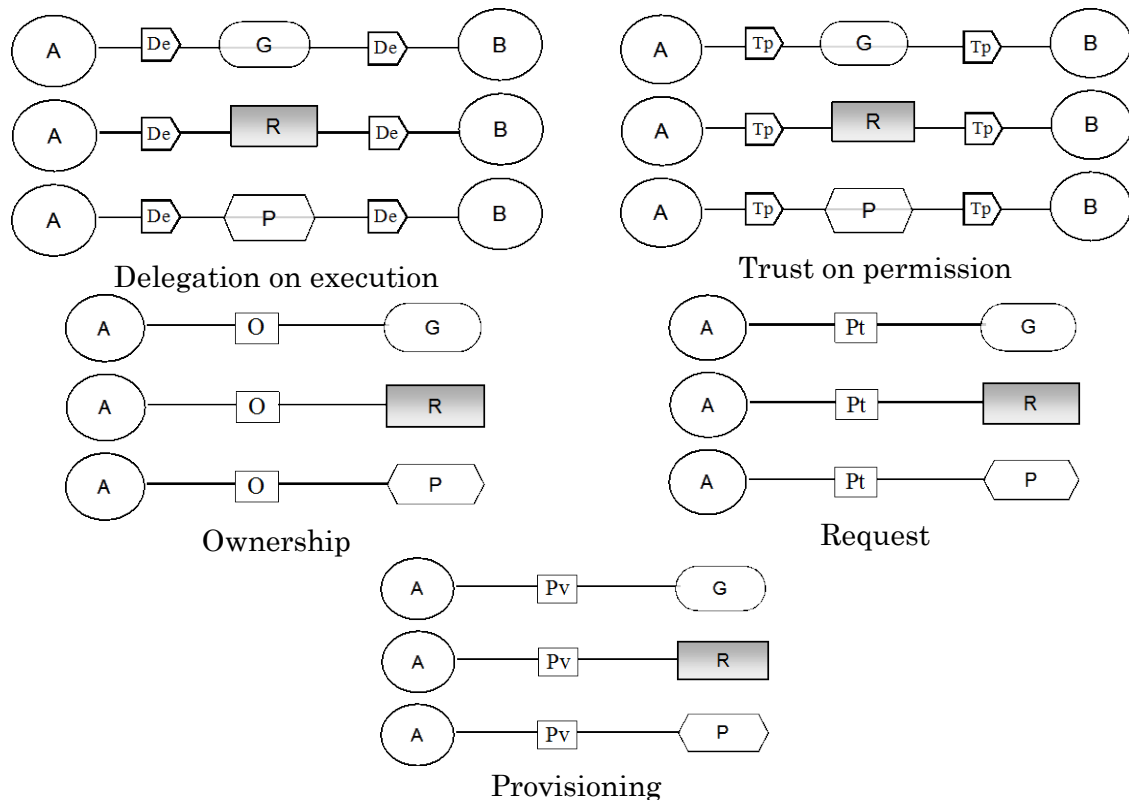


Figure 10 Graphical Notations of the Secure Tropos Concepts for Delegation, Provisioning, Request, Trust and Ownership

Modelling Activities

Various activities contribute to the acquisition of a first early requirement model, to its refinement and to its evolution into subsequent models. They are:

Actor modelling, which consists of identifying and analyzing both the actors of the environment and the system's actors and agents. In particular, in the early requirement phase actor modelling focuses on modelling the application domain stakeholders and their intentions as social actors, which want to achieve goals.

Dependency modelling, which consists of identifying actors which depend on one another for goals to be achieved, plans to be performed, and resources to be furnished. In particular, in the early requirement phase, it focuses on modelling goal dependencies between social actors of the organizational setting. New dependencies are elicited and added to the model upon goal analysis performed during the goal modelling activity discussed below. During late requirements analysis, dependency modelling focuses on analyzing the dependencies of the system-to-be actor. In the architectural design phase, data and control flows between sub-actors of the system-to-be actors are modelled in terms of dependencies, providing the basis for the capability modelling that will start later in architectural design together with the mapping of system actors to agents.

A graphical representation of the model obtained following these modelling activities is given through actor diagrams, called dependency model, which describe the actors their goals and the network of dependency relationships among actors.

Figure 11 depicts a part of an actor diagram where the APSS actor (the Trento's provincial health care authority) has a goal of integrate its software applications. This goal can be decomposed into two sub-goals, namely, "communication among unities" and "standardize software interfaces". For the sub-goal of having a communication among the unities, APSS depends on another actor (Informatica Trentina) for fulfil the sub-goal.

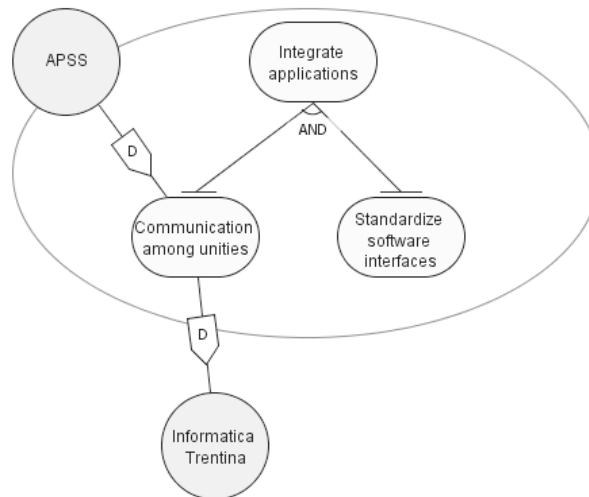


Figure 11 : Actor Diagram

Goal and plan modelling rests on the analysis of an actor goals, conducted from the point of view of the actor, by using three basic reasoning techniques: means-end analysis, contribution analysis, and AND/OR decomposition. In particular, means- end analysis aims at identifying plans, resources and softgoals that provide means for achieving a goal. Contribution analysis identifies goals that can contribute positively or negatively in the fulfilment of the goal to be analyzed. In a sense, it can be considered as an extension of means-end analysis, with goals as means. AND/OR decomposition combines AND and OR decompositions of a root goal into sub-goals, modelling a finer goal structure. Goal modelling is applied to early and late requirement models in order to refine them and to elicit new dependencies. During architectural design, it contributes to motivate the first decomposition of the system-to-be actors into a set of sub-actors.

A graphical representation of goal and plan modelling is given through goal diagrams, which appears as a balloon within which goals of a specific actor are analyzed and dependencies with other actors are established. Goals are decomposed into subgoals and positive/negative contributions of subgoals to goals are specified. Goal decomposition can be closed through a means-end analysis aimed at identifying plans, resources and softgoals that provide means for achieving the goal.

Figure 12 depicts a goal diagram where a Citizen has a set of goals (hardgoals and softgoals). Some of these goals are interrelated using contribution links (for means-end analysis) or using AND/OR decomposition links.

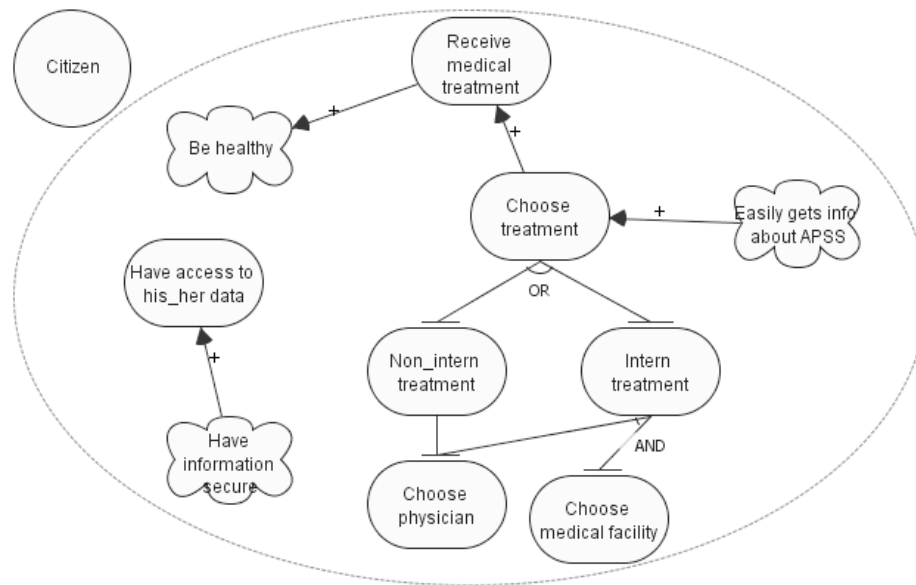


Figure 12 : Goal Diagram

The revised methodology introduces new steps that replaces the old ones:

Trust modelling which consists of identifying actors which trust other actors for goal, plans, and resources, and actors which own goal, plans, and resources. In particular, in the early requirement phase, it focuses on modelling trust relations between social actors of the organizational setting. New trust relations are elicited and added to the model upon the refinement activities discussed above. During late requirements analysis, trust modelling focuses on analyzing the trust relations of the system-to-be actor.

Delegation modelling which consists of identifying actors which delegate to other actors the permission and task of execution on goals, plans, and resources. In particular, in the early requirement phase, it focuses on modelling delegations between social actors of the organizational setting. New delegations are elicited and added to the model upon the refinement activities discussed above. During late requirements analysis, delegation modelling focuses on analyzing the delegations involving the system-to-be actor.

A graphical representation of the models obtained following these last two modelling activities is given through two different kinds of actor diagrams: trust model, and trust management implementation. Essentially, the first represents the trust network among the actors involved in the system and the latter represents which permissions are effectively delegated by actors and which actors receive such permissions. These models use the same notation for actors, goals, plans and resource used during dependency modelling. The old dependency model is replaced by the delegation of execution model.

Figure 13 presents an example of trust model diagram of a scenario of death report. Here, the APSS has a goal of having information about every death occurred in the province. This relation of an actor having a goal is represented using an ownership link. The APSS trusts that the city (Comune of Death) will

fulfil its goal. In this case, we use a trust for execution link which express that the trustee will effectively fulfil the goal. Then this trust is chained from the city to the hospital and the physician. Another aspect is that the citizen trusts the physician a resource, in this case his or hers body. This trust represents the access for the body by the physician only in the case of necessity, i.e., in the case of death. Since it is an eventual trust, we represent it using trust for permission link.

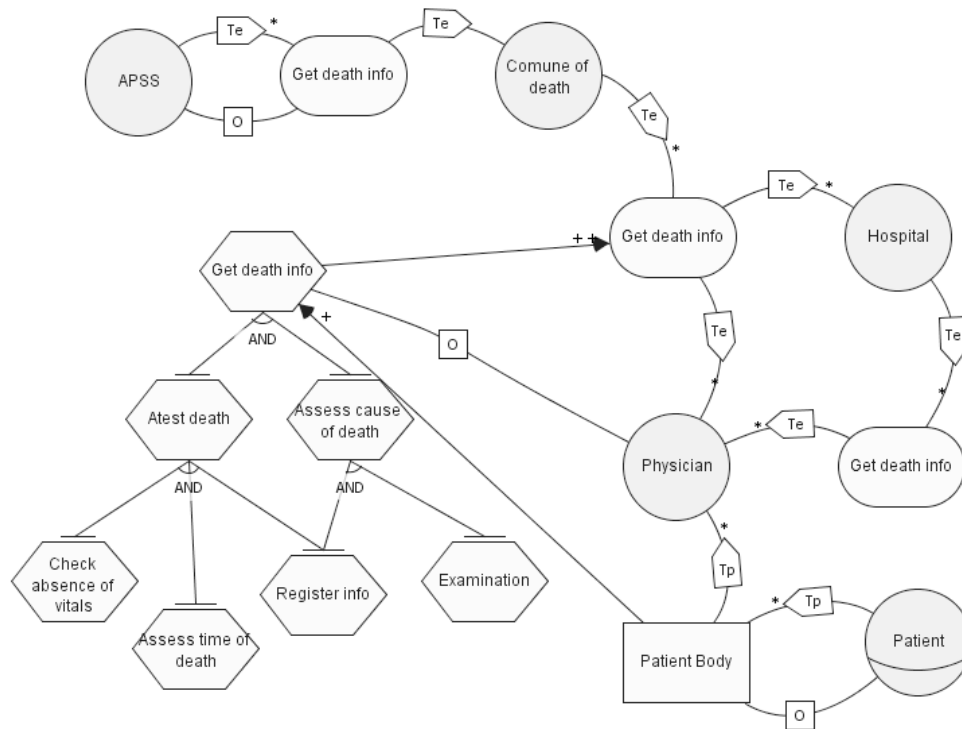


Figure 13 : Trust Model