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: Final,

Preparation Date: March, 31th 2010

Version: 1.0

The TAS³ Consortium

	Beneficiary Name	Country	Short	Role
1	KU Leuven	BE	KUL	Project coordinator
2	Synergetics NV/SA	BE	SYN	Partner
3	University of Kent	UK	KENT	Partner
4	University of Karlsruhe	DE	KARL	Partner
5	Technische Universiteit Eindhoven	NL	TUE	Partner
6	CNR/ISTI	IT	CNR	Partner
7	University of Koblenz-Landau	DE	UNIKOL	Partner
8	Vrije Universiteit Brussel	BE	VUB	Partner
9	University of Zaragoza	ES	UNIZAR	Partner
10	University of Nottingham	UK	NOT	Partner
11	SAP Research	DE	SAP	S&T coordinator
13	Intalio	UK	INT	Partner
14	Risaris	IR	RIS	Partner
15	Kenteq	NL	KETQ	Partner
16	Oracle	UK	ORACLE	Partner
17	Custodix	BE	CUS	Partner
18	Medisoft	NL	MEDI	Partner
19	Symlabs	PT	SYM	Partner

Contributors

	Name	Organisation
1	Magali Seguran	SAP
2	Seda Guerses	KU Leuven
3	Jeroen Hoppenbrouwers	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	Symlabs
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 6
2 INTRODUCTION 7
2.1 SCOPE AND OBJECTIVES 7
2.2 DOCUMENT OVERVIEW 8
3 SCENARIOS FOR DEMONSTRATORS 10
3.1 ACCREDITATION OF PRIOR LEARNING (APL) 10
3.1.1 Actors 11
3.1.2 Business Risk Analysis 11
3.1.3 Secure Tropos trust model 13
3.1.4 Process 15
3.1.5 Step by step description 15
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 20
3.2.5 Step by step description 21
3.3 UK: STUDENT WORK PLACEMENT 23
3.3.1 Actors 23
3.3.2 Business Risk Analysis 24
3.4 SECURE TROPOS TRUST MODEL 25
3.4.1 Processes 26
3.4.2 Step-by-step description 26
3.5 EMERGENCY ADMISSION FOLLOWING AN ACCIDENT ON THE ROAD 28
3.5.1 Actors 29
3.5.2 Business Risk Analysis 29
3.5.3 Secure Tropos trust model 31
3.5.4 Process 32
3.5.5 Step by step description 32
4 DESIGN REQUIREMENTS 33
4.1 BUSINESS PROCESS 33
4.2 TRUST REQUIREMENTS 34
4.3 IDENTITY MANAGEMENT, AUTHENTICATION AND AUTHORISATION 36
4.4 "TRUSTED APPLICATION INFRASTRUCTURE" 37
5 ARCHITECTURAL & TECHNICAL DESIGN REQUIREMENTS 38
5.1 BUSINESS PROCESS 38
5.1.1 Architectural 38

5.1.2 Dependencies 38
5.2 IDENTITY MANAGEMENT, AUTHENTICATION AND AUTHORISATION 39
5.2.1 Architectural 39
5.2.2 Dependencies 40
5.3 TRUST 40
5.3.1 Dependencies 41
5.4 TRUSTED APPLICATION INFRASTRUCTURE 42
5.4.1 Architectural 42
5.4.2 Dependencies 42
5.5 INTEGRATION REQUIREMENTS 42
6 LEGAL REQUIREMENTS 44
6.1 ENROLMENT AND CONTRACTUAL BINDING 46
6.2 ASSIGNMENT OF ROLES AND RESPONSIBILITIES 47
6.3 LEGITIMACY OF PROCESSING 48
6.4 FINALITY 49
6.5 DATA MINIMIZATION 50
6.6 DATA ACCURACY 51
6.7 CONFIDENTIALITY AND SECURITY OF PROCESSING 52
6.8 TRANSPARENCY AND NOTICE 54
6.8.1 Direct collection 54
6.8.2 Indirect collection 54
6.8.3 Implementation 55
6.9 DATA SUBJECT RIGHTS OF ACCESS, RECTIFICATION, BLOCKING AND ERASURE 57
6.9.1 Right of access 57
6.9.2 Rectification, blocking and erasure 57
6.9.3 Notification to third parties 58
6.9.4 Implementation 58
6.10 ACCOUNTABILITY AND COMPLIANCE VERIFICATION 58
6.10.1 Logging 58
6.10.2 Audit & oversight 59
6.10.3 Other accountability mechanisms 59
6.10.4 Complaint handling 60
6.11 NOTIFICATION & PRIOR CHECKING 61
7 ON-LINE COMPLIANCE TESTING 62
7.1 ON-LINE COMPLIANCE TESTING 62
7.1.1 Requirements on the TAS3 Infrastructure 62
7.1.2 Requirements on the TAS3 Infrastructure Registry Component 63
7.1.3 Requirements on Services deployed over the TAS3 Infrastructure ... 64

7.2 OFF-LINE TESTING PHASE 64
7.2.1 Testing of XML-based interchange and communication formats 64
7.2.2 Testing of response-time and availability of services (optional requirements) 64
8 GLOSSARY 65
9 REFERENCES 67
10 ANNEXES 69
10.1 MODELLING WITH SECURE TROPOS 69
10.1.1 The Key Concepts 69

1 Executive Summary

The objective of this first deliverable is defined in the DoW as "modeling 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."

The WP01 "Design Requirements" (D1.4) has been updated concurrently with the "Requirement 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.

This document is the second iteration due in March 2010. It provides a list of necessary features for TAS³ architecture. The included Design Requirements are derived from on a set of scenarios selected for having the most common requirements among the different demonstrator's domains.

For 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 a better visibility of what should be part of contractual agreements or IT solutions. The same approach has been taken for Technical Validation that defines requirements to ensure that the framework will be testable.

A complete Risk Analysis of the whole TAS3 project will be provided as an annex of D2.1.

2 Introduction

2.1 Scope and objectives

The primary objective of the first iteration of this document is to elicit and specify the requirements for each scenario:
Furthermore, it also provide

- employability ; Accreditation of Prior Learning and Mass Layoff (Kenteq) ; education (Nottingham)
- e-health (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 to separate 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 five sections. Sections are the following:

Scenarios from demonstrators: these scenarios contain the requirements from the business demonstrators with a summary which briefly explains what happens in the scenario. It then presents:

- A description of the actors. Identification 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 analyzed 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 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 to capture 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 analyze 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 analyze 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 system.** 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 WP09 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 shortly detailed above.
- **Architectural & Technical Design Requirements** will focus on the framework's overall requirements as well as requirements' dependencies.
- **Legal Requirements** will provide a global understanding of legal issues. These have an impact on the design thus they 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's scenario.

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

3 Scenarios for demonstrators

This chapter introduces "Accreditation of Prior Learning", "Mass layoff" and "Education "from employability and "Emergency Admission" from health care; further information is given in deliverable D9.1 from WP09. This chapter describing these scenarios elicits but does not contain the design requirements.

Following Secure Tropos method, survey's outputs provided a business risk analysis and all necessary information to check and provide a validated model. The business risk analysis does not provide any financial aspect due to the nature of assets and their possible usage.

Next iteration of this document will provide additional requirements from UK employability and health care. However, even if UK employability is not specifically part of this document, TAS3's discussions involved all employability and health care domains to avoid major updates or future inconsistencies in the architecture's design.

3.1 Accreditation of Prior Learning (APL)

Description of the Use Case scenario APL:

1. Employee wants to use an "APL voucher". He asks for an APL voucher at the Branch Office. The coach grants a voucher to the employee.
2. The employee starts the process and searches for a trusted Employability provider
3. Search criteria, trust and privacy negotiations between coordinator and employability providers.
4. Initializing APL, employee selects Kenteq as Employability provider
5. Employee receives credentials for the Kenteq APL process
6. He fills out his portfolio information
7. Kenteq executes the APL process. The APL results and the certificate are exchanged with his ePortfolio
8. Feedback from the employee to the Branch Office that the APL execution is completed.
9. The employee authorizes his employer (HR manager) to access the showcase of his ePortfolio

A video of this scenario is available at http://www.tas3.eu/videos

3.1.1 Actors

Scenario Actor	Person	Task
ePortfolio Provider	Employee	The employee (user) applies for an APL
Branch Office	Personal coach Coordinator	The coach grants an APL voucher The coordinator controls the APL procedure
Employability Provider Kenteq	(APL) coach Assessor	Helps to fill out the portfolio Execute the APL process
Employer	HR Manager	Supports the development of the employee

3.1.2 Business Risk Analysis

APL - RISK ANALYSES			
Actor	**Event**	**Result**	**Remark**
Personal coach	sells illegal vouchers	Employee will not get his APL or Employability provider will not get paid for his services.	personal coach bribed by employee
Personal coach	falsifies information	Employee will not get his APL or Employability provider will not get paid for his services.	
Employee	uses a false voucher	Employee will not get his APL or Employability provider will not get paid for his services.	
Employee	gives false information to coordinator	Wrong employability provider might be selected	
Coordinator	favours one employability provider	Distortion of competition, less quality for employee.	coordinator bribed by employability provider
Coordinator	steals PII from employees	Abuse of PII possible.	
Personal coach	steals PII from employees	Abuse of PII possible.	
Employee	provides false information in APL process	Undeserved certificate and ePortfolio information possible.	
Coach	steals PII from employees	Abuse of PII possible.	
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

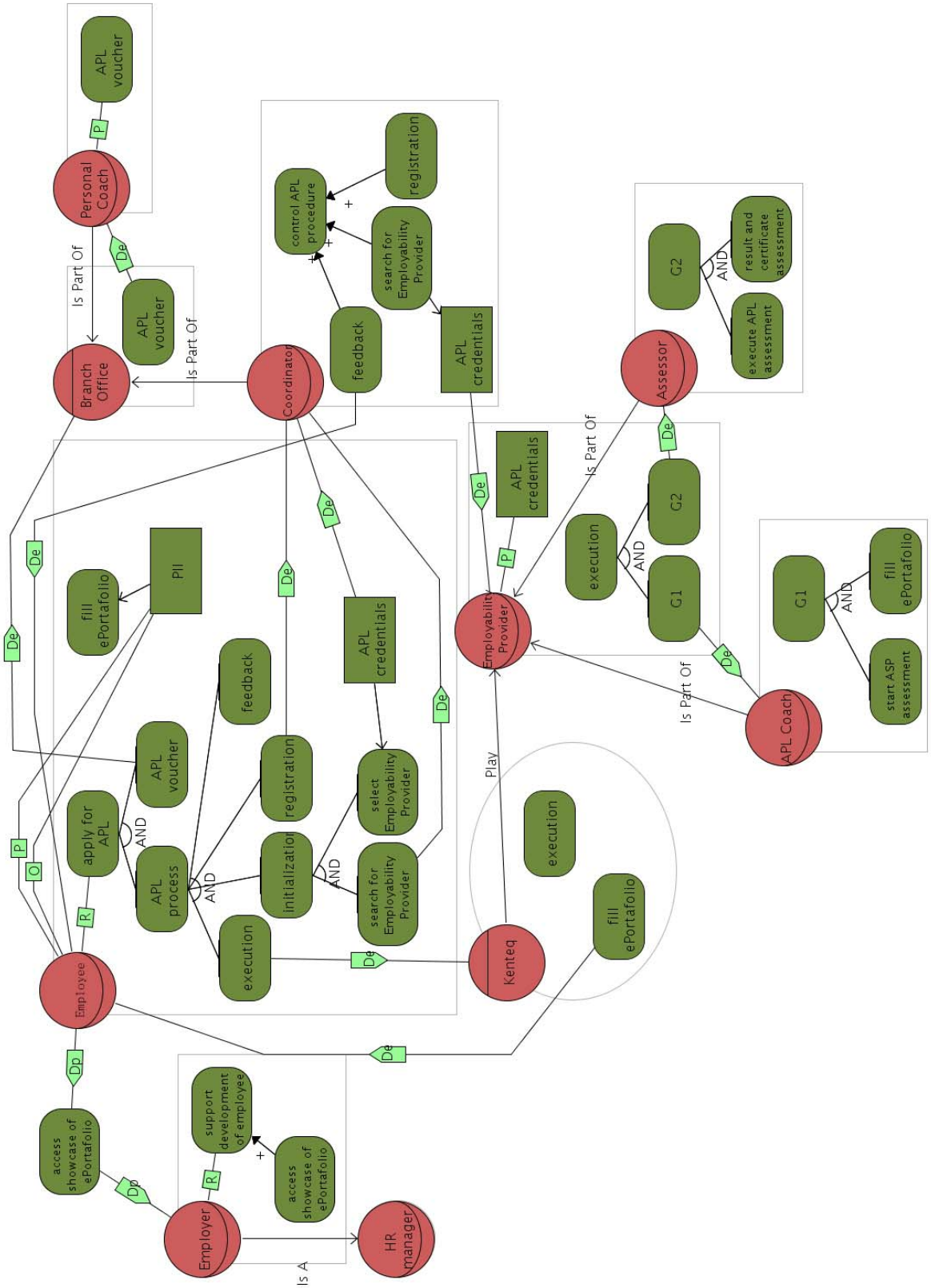


Figure 1: APL Secure Tropos Diagram

In Figure 1, one can see the following actor diagrams: Employee, Branch office, Coordinator, Employee Provider, APL Coach, assessor and Kenteq. An actor diagram represents internal goals of actors, goal decomposition and delegations. The employee Request 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 use an APL voucher (the execution APL voucher is delegated "De" to the 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 *Employability Provider* role. Role is a collective description of actors which act within the scopes of the role. A group of actor can play the same role (req 3.4: if one actor is in vacation, an another actor can play the role).
The APL coach as well as the Assessor is a part of the employability provider (req 3.2a, 3.2b). To enforce separation of duties, assessor and APL coach are represented as two separate roles. Then these two roles should be executed by two separates actors that we can call Agent A and Agent B.

3.1.4 Process

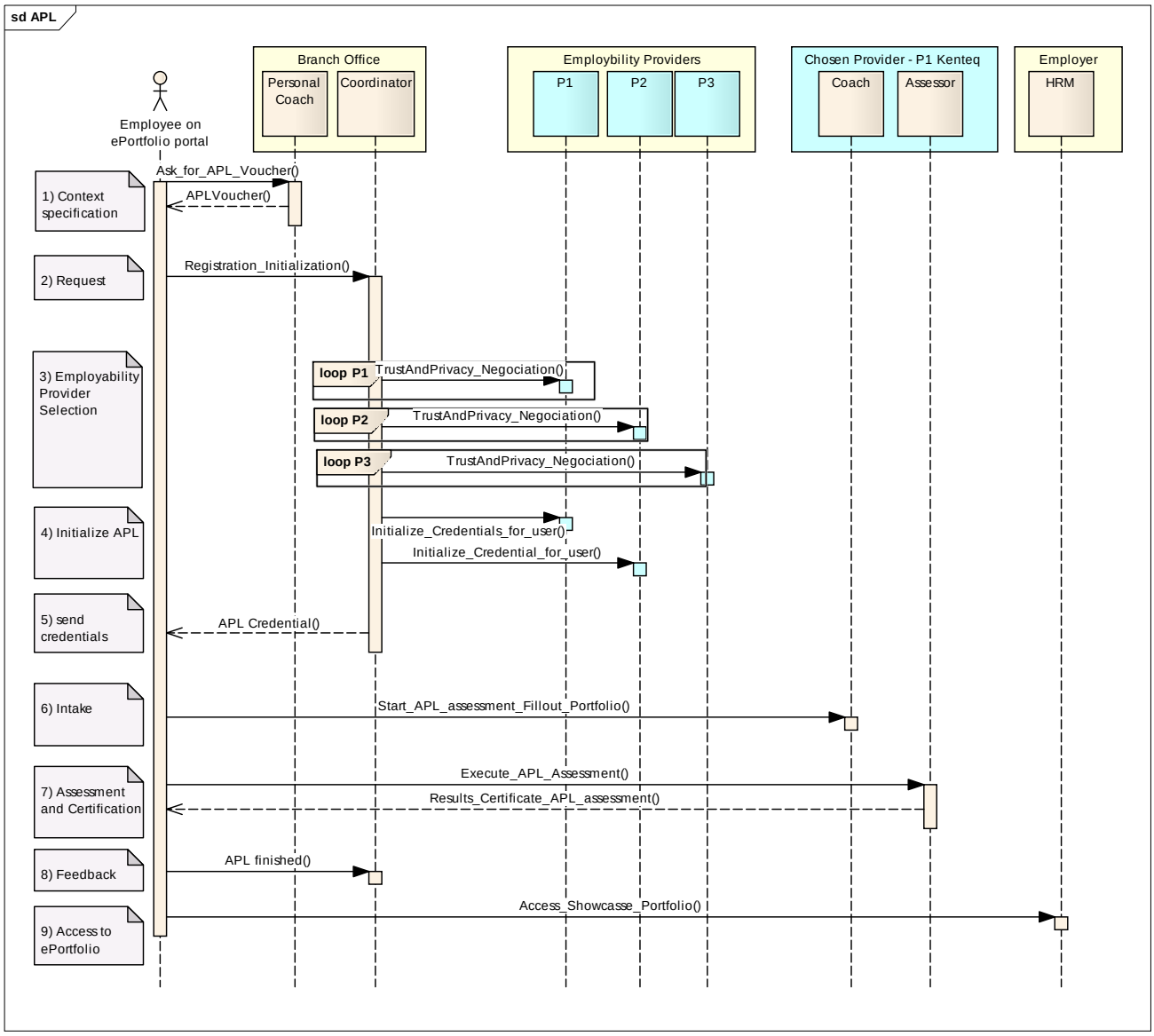


Figure 2 - APL Process

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.
- He contacts his coach and asks for an APL voucher.
- Check if authorised to have a voucher
- The APL voucher is granted (provided by human)

2.

- The user contacts the coordinator in the Branch Office

- Mutual Authentication
- Attribute aggregation of credentials
- Minimum of credentials in order to Register required by National Criteria from Social Partners
- Set the user's privacy policy for Personal Identifying Information (PII) and consent to use this PII
- Indirection between service names and locations to enable change of location and addressing information and evolution

3.

- Find possible Employability Providers that provide the APL the employee wants to do.
- Find out which are trustworthy
- Neither party must reveal too much information about themselves.

4.

- Employability Providers should not be able (to collude) to link requests of Branch Office
- User credentials must be tamperproof, confidential and only usable by Branch Office coordinator

5.

- User evaluates trustworthiness of Employability Providers and chooses one. This performance rating is provided after using the services of the Employability provider and used in future computations of the reputation of the EP.
- Delegation from the user to the portal
- Employability provider may have to merge policies of employee and itself.

6 / 7.

- Portal must be able to understand that additional user credentials/certificates are required
- Portal may need to discover the providers of these certificates
- Requirement for portal intermediary to pass messages between service providers without fully understanding their contents
- Role based signing is required

8.

- The user gives feedback to the Branch Office that the APL execution is finished
- The user should have the opportunity of rating the service (i.e. providing feedback on perceived quality of the service).

9.

- The employee authorizes his employer (HR manager) to access the showcase of his ePortfolio

3.2 Mass Layoff Scenario

Description of the Use Case scenario Job seeking:

1. Job seeker asks a "search voucher"
2. Job seeker does an intake in the mobility centre
3. He does an assessment which result in his Personal Competency Profile (PCP)
4. His PCP is exchanged with his ePortfolio
5. He gets access to a certified Vacancy data provider (database with Vacancy Competency Profiles -VCP-)
6. He searches for a good fitting vacancy (Match between PCP and VCP)
7. He applies for a Job
8. He signs a contract
9. (He starts a course of training)

3.2.1 Actors

Scenario Actor	Person	Task
ePortfolio provider	Job Seeker	find a job
Mobility centre	Personal coach	grant a voucher
Employment Office	Employment coordinator	Provide vacancies profile credentials
Employability provider	Assessor Kenteq	Executes the assessment
Vacancy providers	Randstad, CWI, Nationale vacaturebank, etc..	Maintenance and providing Vacancy database
Employer	HR Manager	Searches for new staff

3.2.2 Business Risk Analysis

MASS LAY-OFF - RISK ANALYSES			
Actor	**Event**	**Result**	**Remark**
Personal coach	sells illegal vouchers	Job Seeker will not get his assessment or Employability/Vacancy Data provider will not get paid for his services.	personal coach bribed by employee
Personal coach	falsifies information	Not (best) matching vacancies might be provided.	
Job Seeker	uses a false voucher	Job Seeker will not get his assessment or Employability/Vacancy Data provider will not get paid for his services.	
Job Seeker	falsifies information	Not (best) matching vacancies might be provided.	
Employment Coordinator	favours one Vacancy Data provider	Distortion of competition, less quality for Job Seeker.	employment coordinator bribed by Vacancy Data provider
Employment Coordinator	steals PII from Job Seekers	Abuse of PII possible.	
Personal coach	steals PII from Job Seekers	Abuse of PII possible.	
Job Seeker	provides false information in assessment process	Not (best) matching vacancies might be provided.	
Personal Coach	steals PII from Job Seekers	Abuse of PII possible.	
Assessor	steals PII from Job Seekers	Abuse of PII possible.	
Vacancy Data provider	steals PII from Job Seekers	Abuse of PII possible.	
Vacancy Data provider	favours one vacancy above others	Not best matching vacancies might be provided.	
Employer (HRM)	steals PII from Job Seekers	Abuse of PII possible.	

3.2.3 Secure Tropos trust model

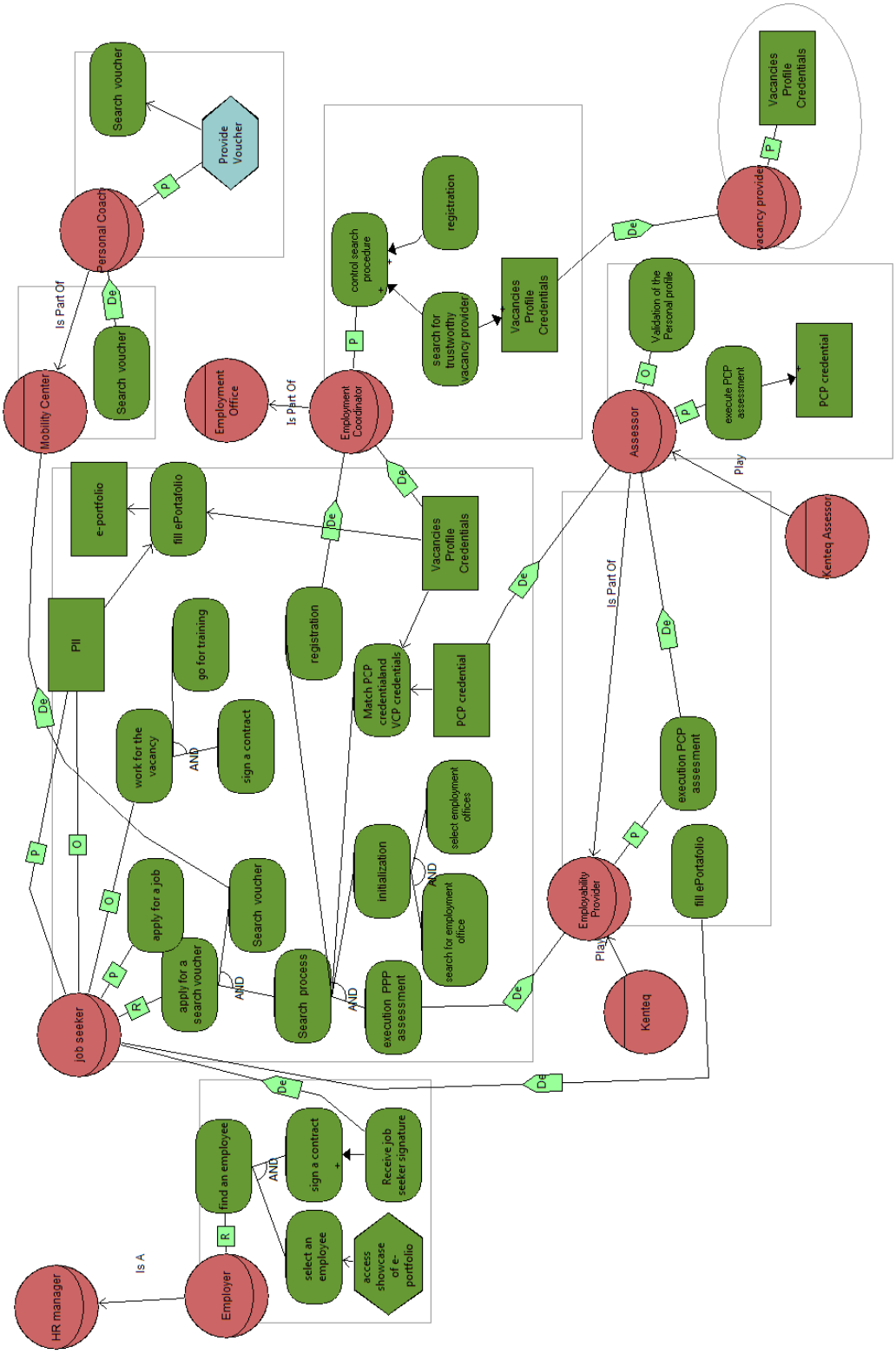


Figure 3: Mass Layoff Secure Tropos

The job seeker has to fulfil the goal “apply for a job” and “work for the vacancy” (“P” relation means Provisioning, which indicates that the actor has the capability to achieve some goal, execute some plan, or deliver a resource).
The employee Request to achieve the goal « apply for a search voucher». The job seeker delegates the interaction with the vacancy provider to the employment coordinator (Req. 3.12a).

3.2.4 Processes

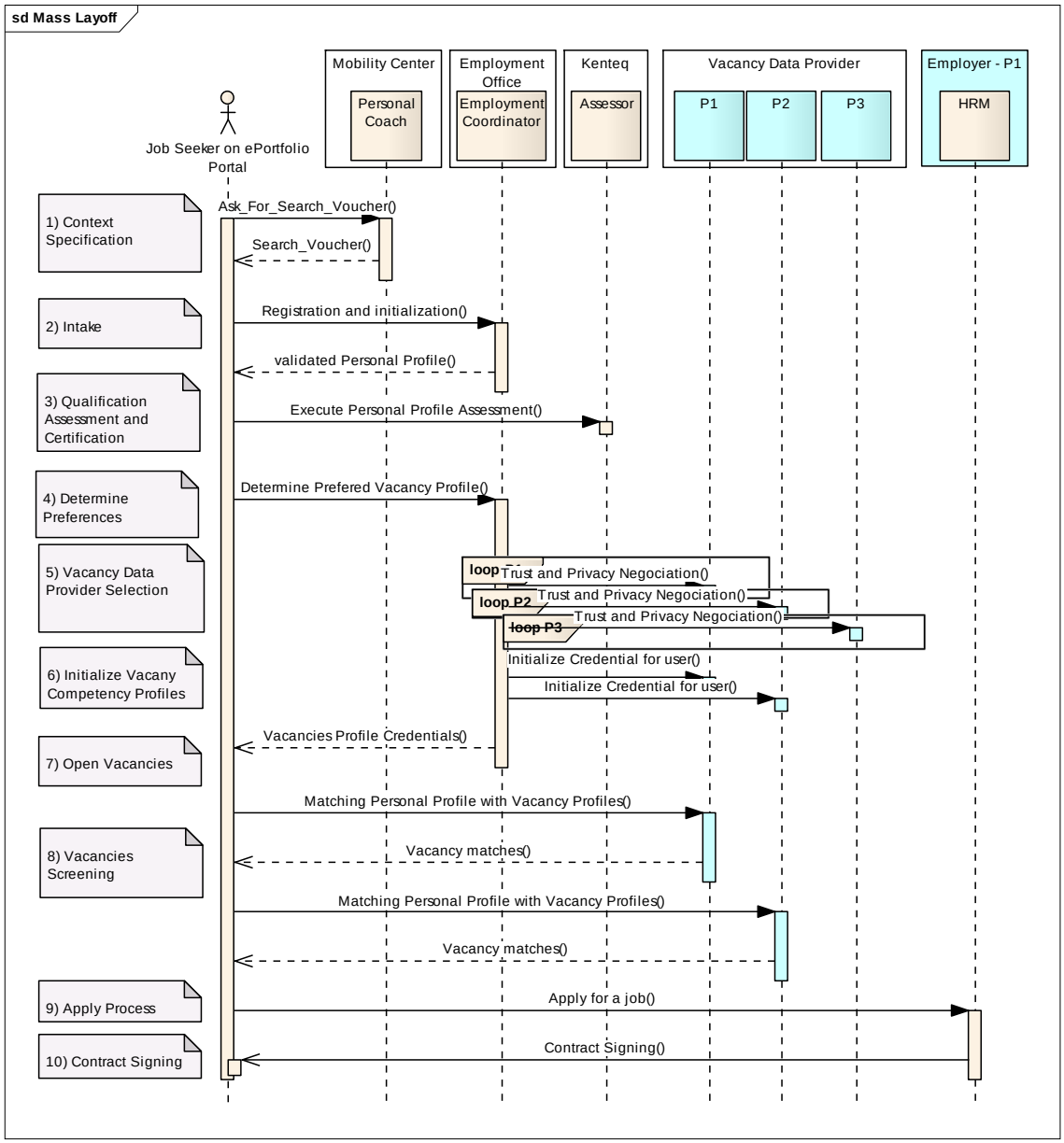


Figure 4 - Mass Layoff process

3.2.5 Step by step description

More information on the 9 major sequences:

1.
   - Job Seeker (user) Authenticates to Portal SSO
   - Find a Coach
   - Mutual Authentication and Authorisation

2.
   - Find Employment Offices
   - Attribute aggregation of credentials
   - Minimum of credentials in order to Register
   - Set the user's privacy policy for Personal Identifying Information (PII) and consent to use this PII
   - Indirection between service names and locations to enable change of location and addressing information and evolution

3.
   - Collect self asserted preferences from the user and the privacy policy regarding these preferences
   - Consent to collect additional PII or ask user to provide it
   - The submitted Profile must be tamperproof and forwardable to Vacancy providers
   - User must be able to act with different personas with different vacancy profiles

4.
   - Find possible Service Providers that provide the right sort of jobs via the portal.
   - Find out which are trustworthy
   - Neither party must reveal too much information about themselves

5.
   - Vacancy providers must not be able (to collude) to link requests of employment office

6.
   - User ranks reputation of Employment office

7.
   - Requirement to handle very large data sets
   - User ranks reputation of Vacancy Provider
   - Delegation from the user to the portal
   - Vacancy provider must be able to stick policies to the returned vacancies
   - Vacancy provider may have to merge policies of employer and itself.

8.
   - Portal must be able to understand that additional user credentials/certificates are required
   - Portal may need to discover the providers of these certificates

- Requirement for portal intermediary to pass messages between service providers without fully understanding their contents
- Role based signing is required.

9.

- User must have a means of signing the contract
- Employer must have means of signing
- Employer must have means of sending contract to user.

3.3 UK: student work placement

Description of the Use Case scenario:

1. A Learner studying on a university course wants to enhance his or her 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. The Learner identifies a placement co-ordinator authorised by the university and registers with this co-ordinator. At this point a basic contractual agreement is established.
3. The placement co-ordinator verifies the learner's identity, and checks that the learner is eligible to participate in one or more of the placement programmes administered by the co-ordinator.
4. The placement co-ordinator tells the learner which programmes he or she is eligible for.
5. The learner chooses which programme(s) he or she is interested in and completes a specific application form, including access to PII in the form of a CV or ePortfolio
6. The learner's data is used to match the learner to profiles of vacancies which are included in the programme. This matching process can be performed in house by the placement co-ordinator or by an external matching service
7. The matches are collated by the placement co-ordinator and presented to the learner. The learner chooses those he or she is interested in. Further 'soft' matching then takes place, including a face-to-face interview.
8. If the learner is accepted for a specific placement, he or she signs contracts with the placement provider agreeing to the terms for that placement.
9. If no suitable placement is found, the learner can repeat the process.

3.3.1 Actors

Scenario Actor	Person	Task
Learner	Student	Make application; select programme; provide access to personal data; 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	
Higher Education Institution	Incorrectly fails to verify learner	Learner is denied access to process	
Higher Education Institution	Returns incorrect identity	Match performed using 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

3.4 Secure Tropos Trust Model

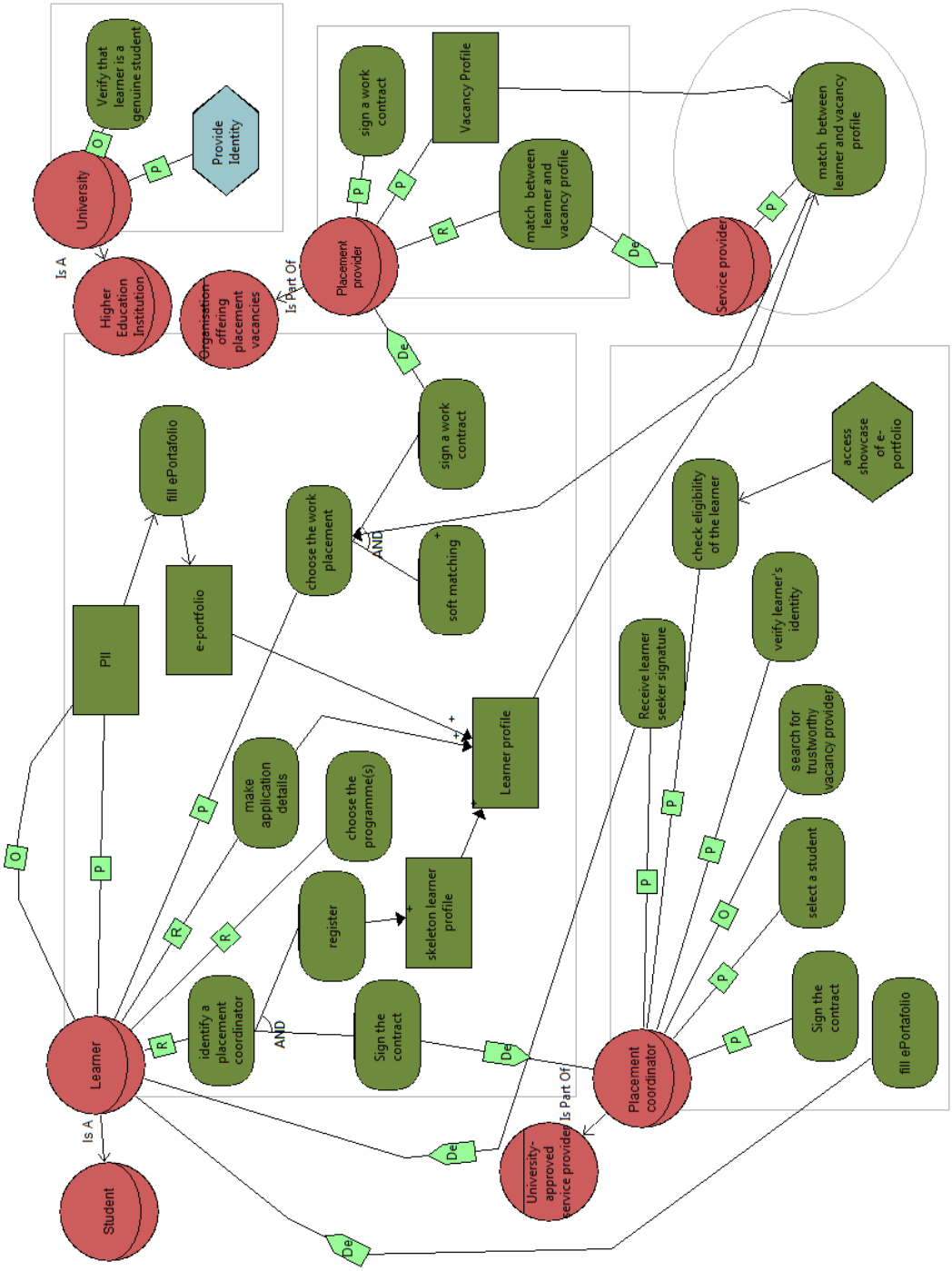


Figure 5: Education Secure Tropos Diagram

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 resource vacancy profile and learner profile are necessary.

3.4.1 Processes

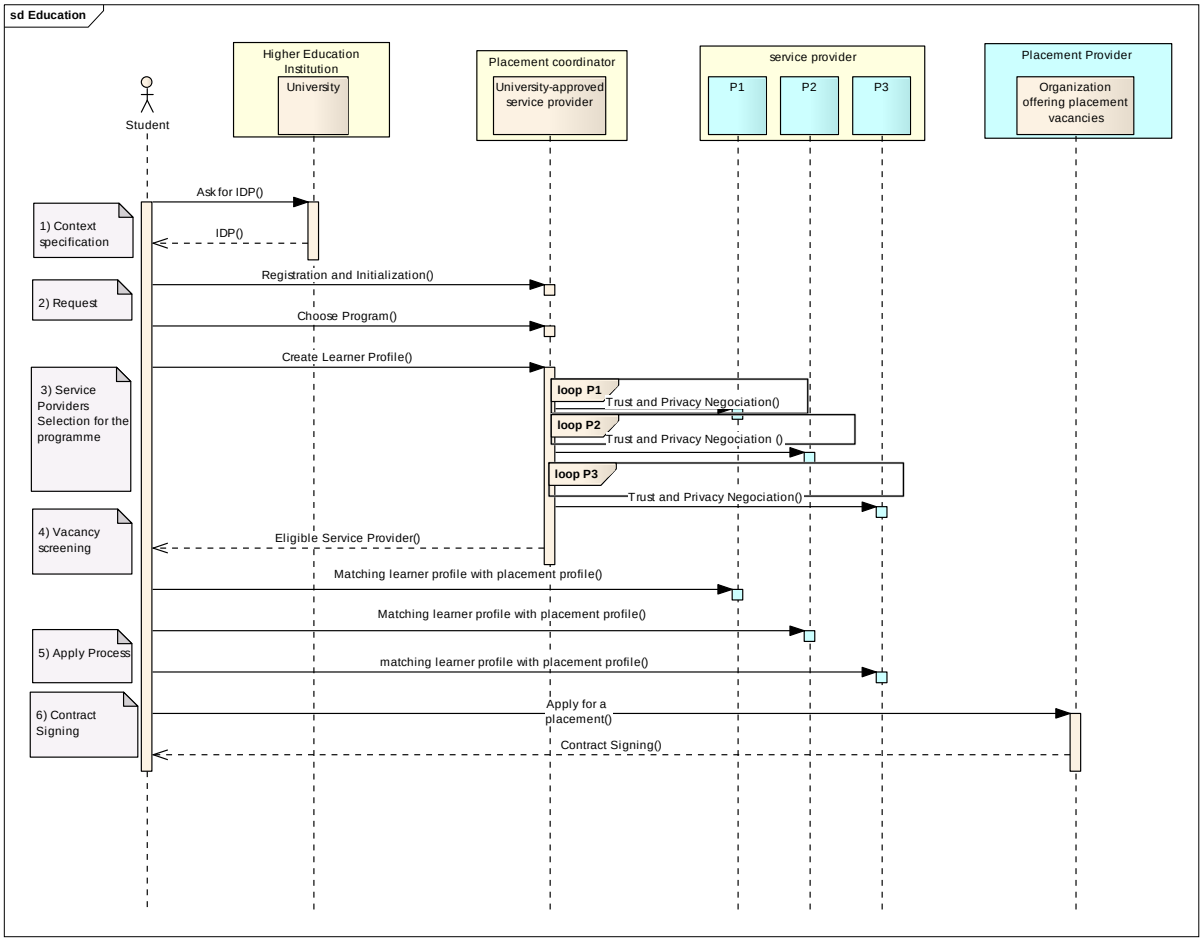


Figure 6: Education Process

3.4.2 Step-by-step description

More information on the major sequences:

1. Learner 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 and currently enrolled
    c. Basic authorisation data about the course the learner is enrolled on is retrieved

3. Placement Co-ordinator matches learner to placement programme(s) he/she is eligible for and returns results to learner

4. Learner chooses programme to apply for and provides further specific application details, including personal information via an ePortfolio
    a. Learner sets privacy policies and attaches these to personal data
    b. Learner sets acceptable trust ranking levels for matching service

5. Discovery service finds service providers for matching service for the programme
    a. Trust and privacy negotiation with service providers using learner preferences
    b. Placement Co-ordinator/Learner is returned a list of suitable service providers
    c. Learner selects which service providers he/she wishes to release his/her profile to

6. 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
    c. Aggregate results and return to placement co-ordinator
    d. Placement Co-ordinator presents anonymised results to learner

7. 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, followed by further selection processes, including face-to-face interview or tests
    c. If the learner is successful, contracts for managing the specific placement are signed between placement provider and placement service provider (this includes any health and safety information, insurance details, etc)
    d. Learner terminates any other current applications
    e. If the learner is unsuccessful, the process loops back to allow further applications to be made

8. Transaction is closed on the system and logs are written
    a. Contract signed between the learner and placement provider agreeing the terms for the placement
    b. Learner is issued with a receipt for the process
    c. Once placement completed the learner can score both the placement provider and matching service via feedback forms.

3.5 Emergency admission following an accident on the road

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 once a replacement for Medisoft has been officially appointed.

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 patients 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 is 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 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 with (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 need 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.

3.5.1 Actors

Scenario Actor	Person	Task
Paramedic	Paramedic	The Paramedic is acting within the ambulance service
A&E physician	physician	Physician working in Accident & 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.

3.5.2 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 ANALYSES			
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 visualize.
Physician	Unlawfully uses the 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 TAS3 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)

3.5.3 Secure Tropos trust model

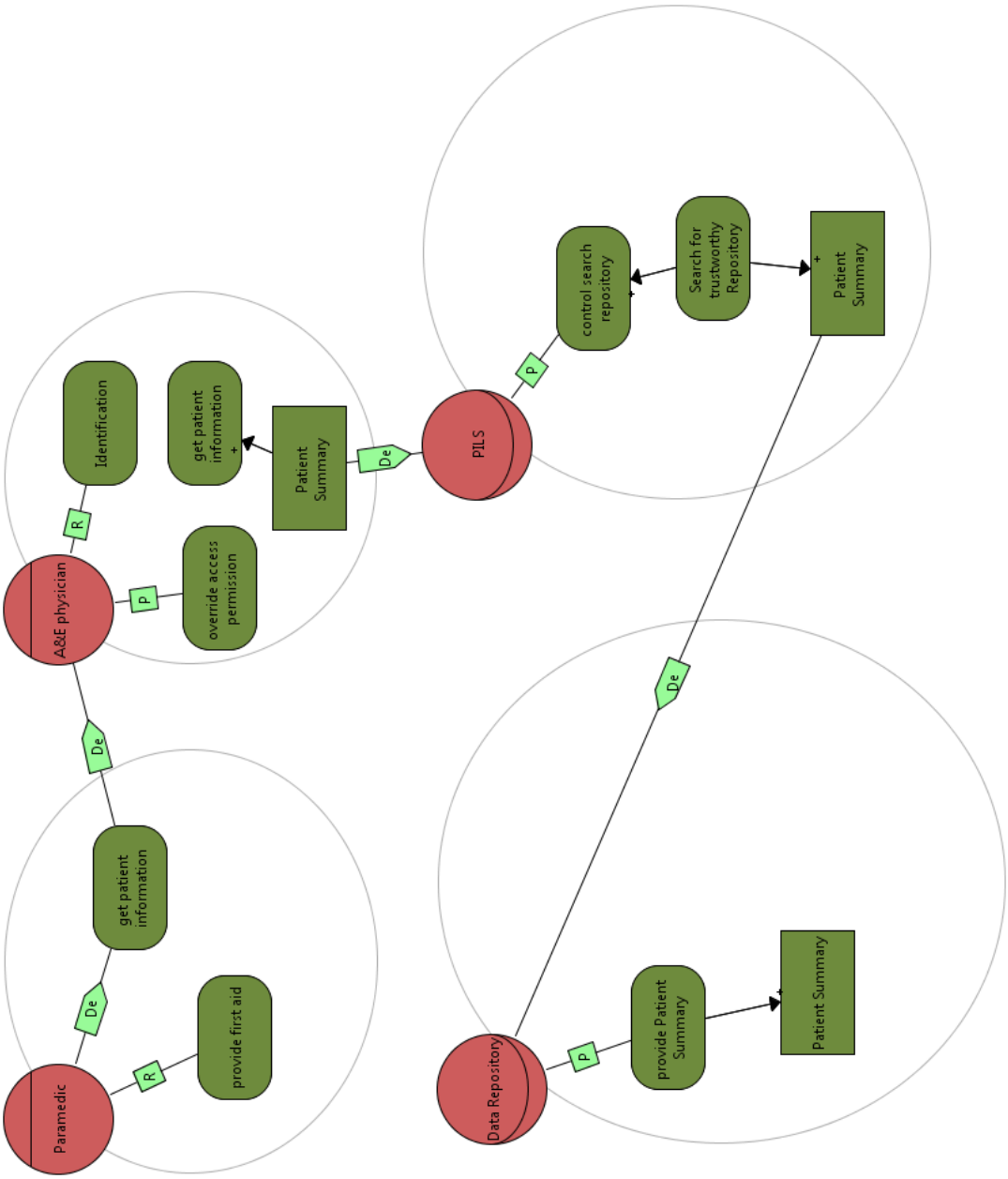


Figure 7: Health Secure Tropos Diagram

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

3.5.4 Process

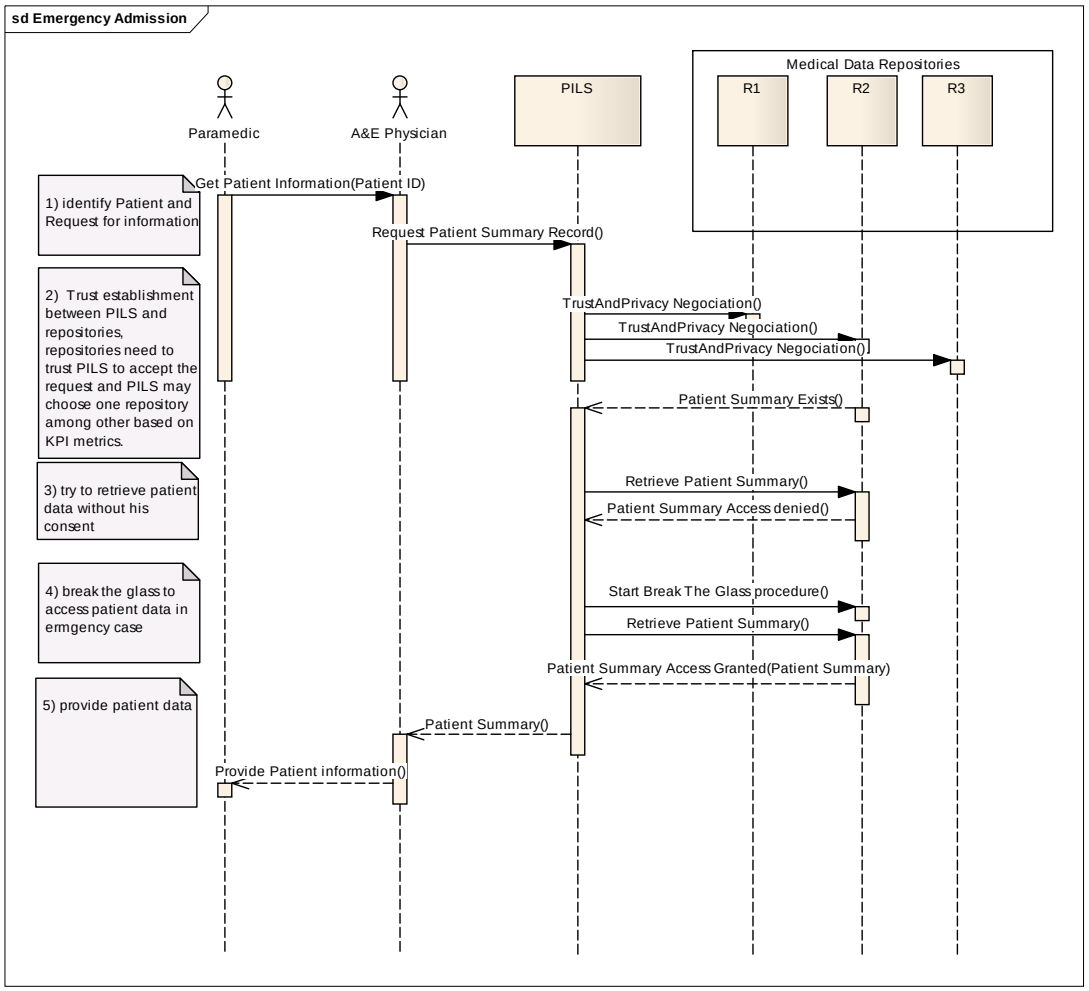


Figure 8 - Emergency Admission Process

3.5.5 Step by step description

The process can be described in 5 major sequences:

1. Identify Patient and Request for information
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. Eg, 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 either scenario or only one if indicated.

For easier access, requirements are split and numbered per 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 "APL coach" at the employability agency.
  - Req 3.2b: The employee's assessor will be chosen by the employability 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 APL 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 APL 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 might be allowed to delegate the assessment to a junior assessor, but only 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 has included the certificate of a Norwegian language course that he had 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 shortened if these grades proof 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 3.12: Business processes MUST be able to act on behalf of other entities (humans or computer systems), e.g., by using appropriate credentials.
  - Req 3.12a: In steps 5 and 6 of the mass layoff scenario, the employment office interacts with vacancy provider on behalf of the job seeker.

4.2 Trust Requirements

The architecture SHALL provide a trust policy evaluation component (Trust-PDP cf Glossary). The requirements related to the Trust-PDP are elaborated below, starting with requirements that the Trust-PDP places on the overall TAS3 architecture in which it is embedded, followed by general requirements of the T-PDP. Finally specific requirements based on "Mass Layoff" scenarios are given.

- 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 2,3)
    - 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 5, 6)
    - 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 4)
    - Req 5.1e A Vacancy Data Provider MUST by able to require a degree from a certified Higher Leaning Institution in the policy expressing the job profile requirements. (Steps 5,6)

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 op 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 5,6). 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 5,6)
    - Req 5.3b a (web) service SHOULD provide normalized KPI factors
    - Req 5.1f a patient MUST be able to specify trust requirements for consent. (Specification before scenario, use in EA Step 2)

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 5, 6)
    - Req 5.4b The Trust-PDP SHOULD evaluate the reputation of a Job Seeker and incorporate it in the trust decision, (Step 8). Evaluation can be done by calculating the value of the reputation metric defined by the vacancy data provider in step 5,6 (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 7)
    - Req 5.4e. A Job Seeker SHOULD be able to provide feedback to be used in determining the reputation of the Vacancy Providers. (Step 8)
    - 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 the Doctor assigned to perform the Medical Tests (Step 9)

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

- Req 7.1 Users SHALL be allowed to link their various identities together, at their sole discretion, in order to use their combined credentials to access Service Providers which require the combined credentials. The SP will know that the user has multiple attributes from multiple authorities but won't know the individual IDs of the user with each SP. The ID itself is of no concern unless the SP provides personalized services or wishes to track the

user between sessions. E.g. The user presents a Visa card and an IEEE card which gives him 10% discount, but the SP does not know the ID of the user with either Visa or IEEE (step 2 of APL)

- Req 7.2 User SHALL be able to delegate access permissions to their private resources to other users (step 8 of APL)
- Req 7.3 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 7.4 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 3 of APL, Step 4 of Mass Layoff)(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 3 of APL, Step 4 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 and 2)(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 aren't available. (Step 3 of APL, Step 4 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 1, 2, (3 of APL, Step 4 of Mass Layoff))(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 3 of APL, Step 4 of Mass Layoff)(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. (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 ocurred exceptions during transactions. (Reference to D1.2: Req. 1.2-8.8)

5 Architectural & Technical Design Requirements

This chapter focuses on the overall framework design's requirements needed to fulfill Employability Demonstrator requirements. Furhter requirements will emerge in future iteration.

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.

5.1.2 Dependencies

- Req 3.11: The business process execution engine MUST evaluate and enforce sticky policies as defined for the architecture.

5.2 Identity Management, Authentication and Authorisation

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 system SHALL allow two entities (typically an IDP and SP) that do not have a trust relationship to dynamically create one
- Req 7.15 The authorisation system SHALL allow policy administrators to dynamically update their policies without requiring any system components to be stopped and restarted
- Req 7.16 Policy administrators SHALL be able to delegate the management of (parts of) their policies to others.

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 IDM, authentication and authorisation infrastructure and not invent their own.
- 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 in 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 & 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 can be broken out into three main sections, namely: intake processes, legal requirements and contractual framework requirements.

Intake Processes (enrolment): All participants will need to be vetted and contractually enrolled in the system (intake processes) so that their obligations are clarified and made binding on the participating entities (individuals and organizations).

Individuals will need to be identified and registered in the system and provided with appropriate access rights and credentials that will allow them to use the system. Processes related to identification, levels of assurance, the types of external credentials and review/validation methods will be specified as part of the development of the intake process. During the intake process they must also subscribe to using the system client software as well as agree to be bound by the choices and transactions they engage in. Prior to executing any instrument or transaction, they must of course also be provided with a complete notice related to privacy in the system, their ability to exercise control as well as the compliance, redress and oversight functions.

Organizations will also need to go through an intake process, but in addition to notice, identification and validation, the ability of the service provider to use and deploy the TAS³ Architecture, their policies and their ability to comply with the requirements of TAS³ shall also be reviewed.

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 an additional obligation 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.

[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).

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.

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: Agreement to be bound. All parties MUST agree to be bound to the obligations they take on both by becoming and being part of the TAS³ network, as well as those which are the result of transactions or choices they exercise through the TAS³ Architecture.
- Req 6.6: Binding Effect of technical processes & policies. All parties MUST agree to be bound by the technical processes in the architecture, including technical policy enforcement and logging mechanisms (to the extent that they are working properly and their properties have been appropriately disclosed and consented to).
    - Req: 6.6.1: 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 6.6.2: It MUST be ensured that commitment to communicated policies and privacy preferences cannot be repudiated at a later time;
    - Req 6.6.3: 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 6.6.4: Policy information MUST be easily accessible to all relevant parties;
    - Req 6.6.5 Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience[2];
    - Req 6.6.6: The policies SHALL be drafted in a way which enables all parties to understand their scope of application and which resources (data, services etc.) are governed by which policies
- Req 6.7: Implementation of Required Policies. Organizational participants in the TAS³ network MUST implement TAS³ defined or compatible policies specified in the contractual framework (e.g. internal privacy and security policies) or as approved during the intake process.
- Req 6.8: 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 6.9: 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;

[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

- 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.

6.3 Legitimacy of processing

- Req 6.10: Consent: Collection, use, and subsequent use, of personal data MUST be compatible with the purposes specified and 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, informed[3], and unambiguous[4].
    - 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 evidentiairy 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.[5]
- Req 6.12: Consent Capture for New or Changed Use: If the use of information changes or if there is a new use of information there MUST be a new informed consent obtained prior to the new or changed use of information. (see also Req 6.16).[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)

[3] A consent may be considered informed when it satisfies all the elements listed in Req 6.44.
[4] From a technical point of view, this requires that the user "opts in" to the processing of personal data.
[5] See articles 7-8 of the Data Protection Directive.
[6] In instances where the subsequent processing cannot be based on the consent of the data subject, an alternative legally permitted ('legitmate') basis must be present to justify the subsequent processing (see Req 6.11).

- 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)

6.4 Finality

- Req 6.15: 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, etc.).
- Req 6.16: Purpose binding/limitation: If the use of information changes or if there is a new use of information which cannot objectively be considered as compatible with the originally specified purpose there MUST be a new consent obtained prior to the new or changed use of information (unless this processing is explicitly required or permitted by law).[7]
- Req 6.17: 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 6.18: 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 6.18.1: Such data handling policies MUST be compatible with the TAS³ governance framework;
    - Req 6.18.2: The data recipient MUST be legally bound to restrict itself to authorized usage and to execute the specified obligations specified in these data handling policies (see also Reqs 6.5-6.6);
    - Req 6.18.3: 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 6.19: Technical policy enforcement mechanisms SHALL be able to take into account the specified purpose when evaluating a processing request when appropriate. See also Req 6.20.
- Req 6.20: 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 (see also Reqs 6.63-6.65).

  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

[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.

consideration MUST be given to deciding which entity shall be trusted to register and verify the asserted/permitted purposes.

6.5 Data minimization

- Req 6.21: The collection and further processing of personal data MUST be relevant and non-excessive in relation to the specified purposes (see Req 6.15).

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

- Req 6.22: 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 6.23: 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 is authorized to receive (sufficient level of granularity). See also Req 6.37.
- Req 6.24: 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 6.24.1: Mechanisms SHALL be in place to enable the user to choose which identity providers and/or attributes shall be used for a particular service, subject to applicable policy (e.g. minimum level of assurance, prerequisite attributes for authorization decision etc.).

- Req 6.25: 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 6.25.1: 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 6.25.2: 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 6.25.3: 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).

6.6 Data accuracy

- Req 6.26: 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 6.27.: 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 6.27.1: Where appropriate, review and update procedures MUST be in place for personal data which is being kept for an extended period of time.
- Req 6.28: Procedures MUST be in place on how to report and deal with suspected inaccuracies.
    - Req 6.28.1: Data subjects MUST have the ability to check the accuracy and quality of the data, and to report suspected inaccuracies. (see Reqs 6.51, 6.53, 6.55 and 6.61);
    - Req 6.28.2: In the event of indirect collection, prior to further processing the accuracy of the data SHOULD be verified with the data subject where this is both possible and appropriate;
    - Req 6.28.3: 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 6.58)
- Req 6.29: 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 6.29.1: 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 6.30: The integrity of data maintained in authoritative sources MUST be appropriately guaranteed.
    - Req 6.30.1: Modification rights MUST be restricted to authorized entities on a 'need-to-modify' basis.
- Req 6.31: Data to and from authoritative sources MUST be authenticated through use of data origin authentication protocols to ensure authenticity and integrity where appropriate.
- Req 6.32: 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 6.32.1: Policies SHALL be in place which specify how a 'sufficient level of certainty' as to the origin and integrity of personal information is established.

6.7 Confidentiality and security of processing

- Req 6.33: Confidentiality. Appropriate organizational and technical security measures MUST be in place to ensure the confidentiality of personal data.
- Req 6.34: 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 6.35: An organizational framework for information security management (describing both organizational and technical measures) MUST be in place.
- Req 6.36: 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 6.36.1: Identities and credentials MUST be managed in way that they continuously provide a level of assurance proportionate to the interests at stake;
    - Req 6.36.2: Common authentication approaches and rules MUST be defined and enforced;
    - Req 6.36.3: 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 6.36.4: 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 6.36.5: 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 6.37: 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 6.9):
    - Req 6.37.1: A list and directory of resources (e.g. applications, data) and potential users/data recipients MUST be made.

- Req 6.37.2: Personal data contained in data repositories SHALL be categorized according to a classification system that recognizes type and sensitivity of data.
- Req 6.37.4: Roles and privileges of each entity MUST be defined based on legitimate organizational needs (in other words, on a "need-to-process" basis).
- Req 6.37.5: 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 6.37.6: 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 6.37.7: 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 6.37.10: Adequate measures and procedures MUST be in place to properly address security breaches, including notification of relevant entities (e.g. audit & oversight committee)
- Req 6.37.11: Adequate measures and procedures MUST be in place to support enforcement of authorization policies at both central and local levels.

- Req 6.38: 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 6.39: Avoid unnecessary linkability. TAS³ SHALL support advanced pseudonym management to limit the level of linkability or correlation among personal data where appropriate.
- Req 6.40: Physical access restriction: Physical access to terminals and other resources MUST be restricted where appropriate.
- Req 6.41: 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 6.42: 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.

[9] Such policies must of course be compatible with the TAS³ governance framework (see Req 6.7).
[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.

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 6.43: 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 6.44: Notice requirements where data is collected from data subject herself (direct collection):
    - Req 6.44.1: 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 6.44.2: The data subject SHOULD also be informed of:
        - the recipients or categories of recipients of the data;
        - 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 6.44.3: 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 6.45: Notice requirements where data is not obtained directly from data subject herself (indirect collection):
    - Req 6.45.1: In case of indirect collection, the data subject MUST**, at the moment of undertaking, or if a disclosure to a third party is

[11] The data subject MUST in principle be notified of the elements listed in Req 6.43 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). The instances and modalities of the notice obligations are described in more detail in subsections 8.1-8-2. Subsection 8-3 provides some additional guidance towards the implementation of these requirements in TAS³.

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 6.45.2: 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 6.45.3: 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 6.45.1-3 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 6.46: 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 6.46: Layered approach._In order to limit complexity, the fulfilment of Reqs 6.44-6.45 need not necessarily take the form of a single document.[12] TAS³ SHALL adopt a 'layered' approach for notice when appropriate.
  - Req 6.46.1: This approach SHALL NOT contain more than three layers of information (short – condensed – full)
  - Req 6.46.2: The sum total of these layered notices MUST meet the notice requirements imposed by the applicable national legislation.
  - Req 6.46.3: It MUST be easy to ascertain which data processing operations are governed by which policies.

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

- Req 6.47: 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 6.47.1: 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 6.47.2: This general privacy policy SHOULD reference and link the privacy policies maintained by TAS³ participants (see Req 6.48) when appropriate.

- Req 6.48: 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 6.48.1: 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 6.48.2: These privacy policies SHOULD also cross-reference the TAS³ infrastructure privacy policy where appropriate.

- Req 6.49: Consent to notices. The consent of the data subject MUST (as a rule[13]) 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).
    - Req 6.49.1: 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 6.50: 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 Req 6.12).[14]

[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 to obligation to inform the data subject of such processing (see Reqs 6.43 et seq.)

[14] Req 6.50 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 legitmate interest MUST at least be generically outlined in the TAS³ privacy policy notice(s) mentioned in Reqs 6.47-48.

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

- Req 6.51: 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.[15]
- Req 6.52: 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 6.53: Upon request, the data subject MUST be provided with confirmation, as to whether or not data relating to a particular data subject 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 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 6.54: The confirmation and information listed in Req 6.53 MUST be provided without constraint or excessive delays or expense.

6.9.2 Rectification, blocking and erasure

- Req 6.55: Data subject requests to rectify, block or erase data MUST be accommodated at all times EXCEPT where an overriding legitimate interest exists.
    - Req 6.55.1: Such overriding interest SHOULD be specified in the TAS³ privacy policy notice(s).
    - Req 6.55.2: 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 6.55.3: In case of denial, the reason for denial MUST be communicated to the data subject.

- Req 6.56: 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;

[15] This also helps assure the accuracy and integrity of the data, which MUST be maintained in a manner appropriate to the specified purposes (see Reqs 6.26 et seq.).

- which entity shall decide these requests;
- valid reasons for denying the request;
- the time-frame in which this request will be processed;

- Req 6.57: A procedure SHOULD be in place to adequately deal with the situation in which a data subject submits his/her request to a TAS³ actor which is not competent to decide that particular request.

6.9.3 Notification to third parties

- Req 6.58: 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 6.59: 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 6.60: 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 6.61: 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 6.62: 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 Logging[16]

- Req 6.63: Processing operations involving personal data MUST be logged with a sufficient level of detail.
- Req 6.64: 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 6.64.1: Log files MUST detail which entity performed which action upon which resource, and at what time;

[16] 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.

- Req 6.64.2: Where appropriate, log files SHALL also record for which purpose (under which pretext the action took place/was authorized);
- Req 6.64.3: 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 6.65: Reliability: Appropriate measures MUST in place to ensure the authenticity, accuracy, integrity and completeness of the logs.
- Req 6.66: Transparency. The fact that processing operations are logged MUST be transparent towards users through appropriate notification (see Reqs 6.43 et seq).
- Req 6.67: Proportionality: Logging MUST organized in a proportionate manner (e.g. storage in a pseudonymized or de-identified format, separation of duties).
- Req 6.68: Confidentiality: Appropriate measures MUST be in place to ensure the confidentiality of the logs. See also Req 6.33 et seq.
    - Req 6.68.1: Privileges to access nominative log information SHOULD in principle only authorize selective access (no 'free search');
    - Req 6.68.2: 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.

6.10.2 Audit & oversight

- Req 6.69: The proper implementation and functioning of all technical mechanisms and organisational measures MUST be documented and audited on a regular basis.
- Req 6.70: Definition of roles & responsibilities (see Req 6.9) MUST also include assignment of tasks with regards to audit and oversight.
- Req 6.71: 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 6.72: 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 6.73: Technical non-repudiation mechanisms MUST be supported when appropriate. For example:
    - Req 6.73.1: When forwarding personal data, it SHALL be ensured that the sender is not able to later deny having forwarded it;

  - Req 6.73.2: It SHALL be ensured that the commitment to communicated policies and privacy preferences cannot later be repudiated at a later time.

- Req 6.74: 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 6.74: Automated notifications SHOULD also be considered for certain types of processing operations (e.g. access to particularly sensitive data)

- Req 6.75: 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 6.76: Outsourcing – reliance upon other entities for personal data handling: Where members/participants of the TAS³ network decide to pass any personal data to entities outside their own organisation for them to process it on their behalf, they MUST ensure that such recipients 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 (e.g. with regards to storage duration, finality etc.)

6.10.4 Complaint handling

- Req 6.77: Complaint capture system: Potential abuses to the system or concerns of either users or organizations MUST be captured.
  - Req 6.77.1: 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 6.77.1: Appropriate levels of proof are required to justify the consequences listed in Req 6.77.2 and complaints should therefore be corroborated on the basis of logs and other relevant documentation

- Req 6.78: Redress/oversight Processes: Once a compliant 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.

6.11 Notification & prior checking

- Req 6.79: 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 on 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 error.

- 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 favors interoperability and provides support for possible automated validation (e.g., by CNR's TAXI [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 [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 Specified 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-CentricRequirements 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

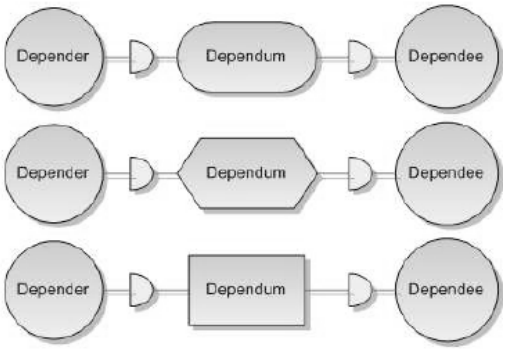
10.1 Modelling with Secure Tropos

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.

Actor and its specializations

Goal, plan and resource



Dependency

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.

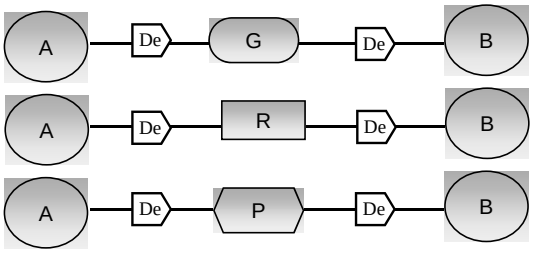
Ownership, which indicates that the actor is the legitimate owner of some goal, some plan, or some resource. The owner has full authority concerning to achieve his goal, execute his plan, or use his resource, and he can also delegate this authority to other actors.

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

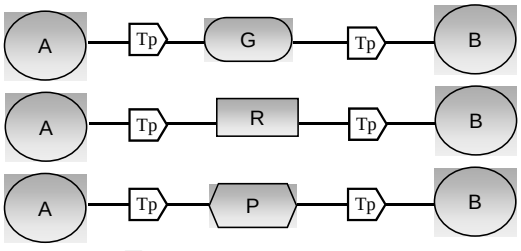
Request, which indicated that the actor intends to achieve a goal, execute a task, or requires a resource.

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 be- comes 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 centers 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.



Delegation on execution



Trust on permission

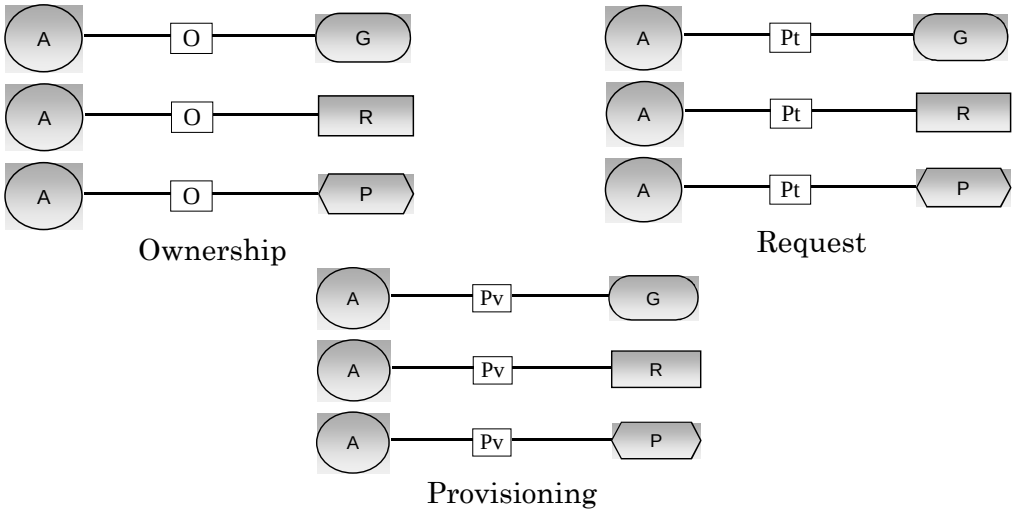


Figure 10 – Graphical Notations of the Secure Tropos Concepts for Delegation, Provisioning, Request, Trust and Ownership

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 stake- holders 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.

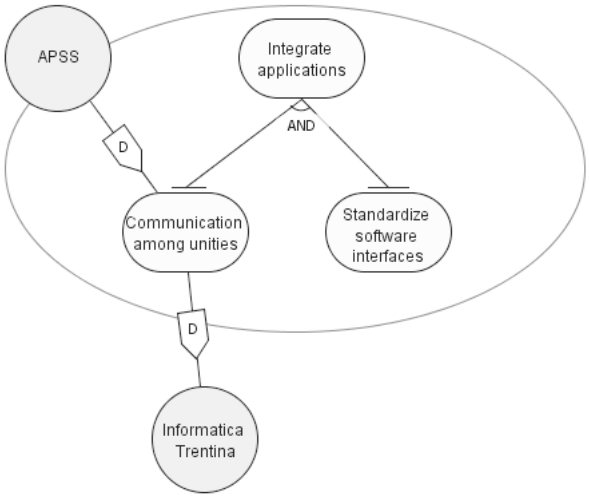


Figure 11 – Actor Diagram

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.

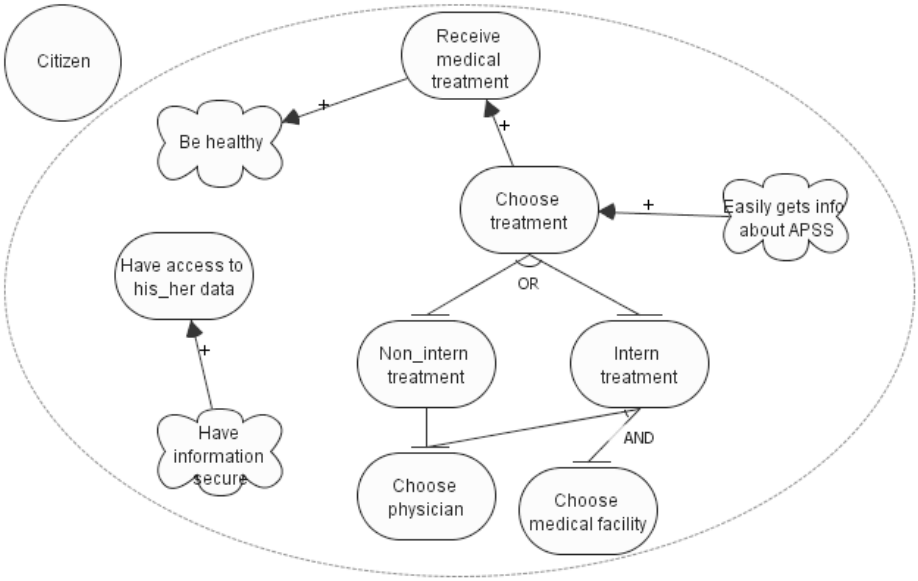


Figure 12 – Goal Diagram

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.

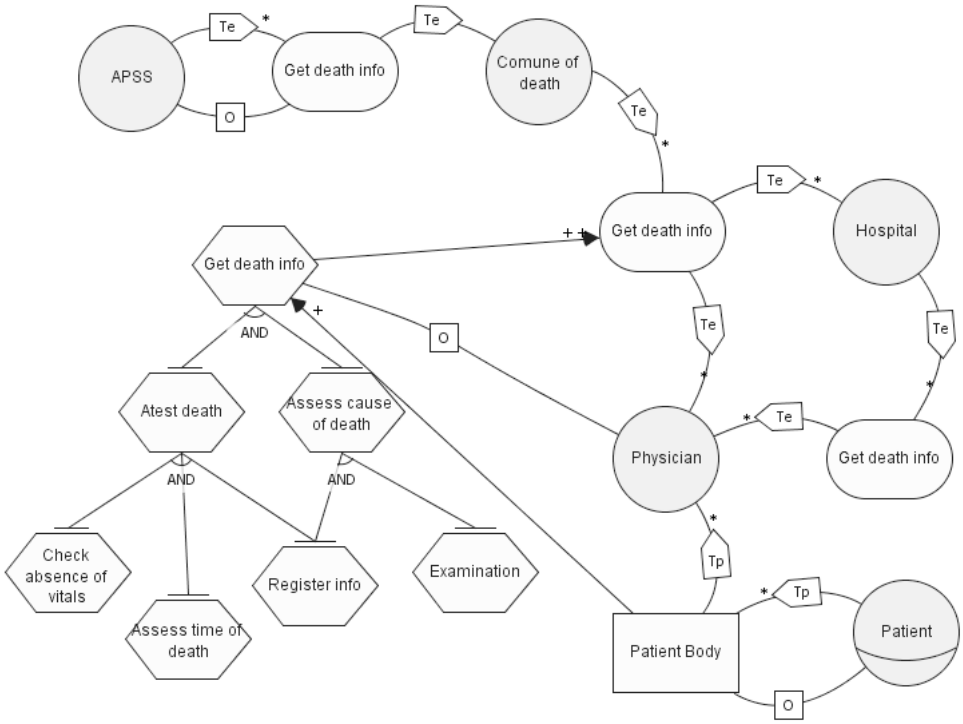


Figure 13 – Trust model