SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document Type: Deliverable

Title: **Self-Evaluation Report**

Work Package: WP1

Deliverable Nr: D1.3

Dissemination: Final

Preparation Date: December, 18th 2009

Version: 1.0

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

The TAS³ Consortium

	Beneficiary Name	Country	Short	Role
1	KU Leuven	BE	KUL	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 Coord.
12	EIfEL	FR	EIF	Partner
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 (editor),Gilles Montagnon	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 Technology.
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	Kenteq

Contents

1 Executive Summary

The purpose of this document is to state the evaluation criteria that are going to be used to assess the degree of achievement of TAS³ main goals. Such criteria are both strategic indicators to unambiguously evaluate the final outcomes of the project, and important guidelines to ensure an on-going self-evaluation process that every participant must implement throughout the whole duration of the project.

The Trusted Architecture for Securely Shared Services (TAS³) project's objective is to develop a trusted infrastructure to support the responsible security and privacy management of information in a world of ever increasing mobility of persons and information. The project is organized in a user-centric manner that is designed to foster user trust and acceptance while allowing for more robust and beneficial use of the information in a controlled and accountable manner.

TAS³ will thus provide a next generation trust & security architecture that is ready to meet the requirements of complex and highly versatile business processes; that enabling the dynamic user-centric management of policies; that ensure end-to-end secure transmission of personal information and user-controlled attributes between heterogeneous, context dependent and continuously changing systems. This includes a trust and data protection infrastructure for managing & assessing the risks associated with identity authentication (level of assurance) and the trustworthiness of actors.

Improved usability of information enables new information economy related services that reflect evolving business, governmental and societal needs. These needs are addressed in a new cross-functional and dynamic trust infrastructure based on legal and policy frameworks supported by technological implementations of authentication, validation, identity management, policy mediation / interpretation, accountability, audit and oversight.

The **TAS³** proposal aims to have a European-wide impact on services based upon personal information, that is to say information which is (co-)owned by the individual, being the 'data owner' who has either full rights or rights shared with the 'data controller', typically an educational, corporate, governmental, or service organization. Personal information is typically generated over a human lifetime, and therefore is collected and stored at distributed locations and used in a multitude of business processes. The **TAS³** architecture can be instantiated in different contexts because the nature of this personal information is not specific to **TAS³**.

In order to tackle the complexity of this wide range goal, TAS³ project has been broken down into several activities, each coping with specific issues of each layer and providing suitable solutions for them. As a natural consequence of this approach, tools and solutions that will be the outcomes of each activity can be significantly different. Therefore, each activity contributes to this document by defining the evaluation criteria that should be

applied to assess the degree of achievement of TAS³ 's general goals within the activity itself.

This document "Self-evaluation" report is the last deliverable of WP01.
To summarize, the "State of the Art" (D1.1) describes the current standards, technologies and methodologies for security, privacy and trust. The document "Requirements Assessment Report" (D1.2) gathers together in one place the full set of requirements for security, privacy and trust in service-oriented open and distributed environments. The "Design Requirements" (D1.4) takes as input the "State of the Art" and the "Requirements Assessment Report" to ensure that the future design is achievable and consistent with TAS³ 's expectations.

2 Introduction

2.1 Scope and objectives

In order to evaluate the overall project, it is important to go through the evaluation of each activity and then each work package. This decomposition is essential to tackle the intrinsic complexity and pervasiveness of the project.

TAS³ project is composed of 13 Work Packages (WP's). To ensure the coordination and consistency across all the work packages within the project, Work packages are grouped into 6 Activities, lead by experienced researchers of the consortium.
The WP's are grouped in Activities to facilitate the coordination of integration work to be done within this project. This clustering is dynamical, and, according to the different phases of the project, a single WP or single Task can be mapped onto one or more Activities. In other words, the Activity structure is flexible and brings together whatever partners/tasks need to work on a particular topic at a particular point in time.

The following Activities have been identified:

- Activity 1, **Requirements, Risk & Compliance**, comprises WP1 and WP6. This Activity is responsible for coordinating all the Requirements, Risk and Compliance contributions, which are spread through the various work packages (mainly, WPs 1 and 6, but relevant contributions come from WP2, WP10 and WP12, too). It gathers together technical, application-scenarios driven and legal requirements and, it ensures the consistency of the risk analysis, and of the compliance testing. It is led by SAP
- Activity 2, **Architecture and Integration**. This high-level Activity monitors and directs the complete architectural process from requirements analysis to delivery of the reference implementation. The activity leads to a commonly endorsed TAS³ achitecture, commonly endorsed interface specifications at the appropriate level of detail, (possibly parallel) implementations of the interface and architectural specifications, and the

integration, verification, and validation of the implementations. It s core includes WP2, WP12 and WP10, and it is led by KUL

- Activity 3. **Trust providers and Protocols** This Activity is responsible for coordinating all the trust, security and privacy related work that is spread through the various work packages (specifically, WPs 3,4,5,7) and partners, to ensure consistency and completeness throughout the project. In particular, it addresses the need to ensure that no important security, trust or privacy feature falls through the gaps between individual work packages and ends up not being implemented, thereby potentially threatening the security of the entire TAS³ infrastructure. Just as importantly, however, we need to ensure that no resources are wasted by replicating some security, trust or privacy mechanism by implementing it multiple times in different work packages, or by re-implementing a feature in one work package that is already being used in another work package. Finally, it ensures that the protocols that are being specified for communicating between the services being developed in each of the work packages are fit for purpose and conform to the overall TAS³ architecture. It is led by KENT
- Activity 4, **Pilots**, focuses on testing the innovative features of the TAS³ infrastructure in realistic use cases. The main contributions to this activity are from WP8 and WP9. It is led by CUS.
- Activity 5, **Dissemination and exploitation**. This activity is responsible for coordinating all the dissemination, training and e**xploitation work which is main**ly supported by WP11 together with all other work packages. It addresses contact with standardisation bodies and the outside community to help to grow the TAS³ Best Practice Network, community and associated partners networks. It also includes all training work between partners coordinated by WP11 training part as well as helping to build the project exploitation plan. It is led by EIFEL.
- Activity 6, **Management,** WP13, is led by KUL. This activity will not be concerned by the evaluation process.

The approach we adopt to address the project evaluation stands on the work package-based evaluation criteria.
Within the Activities, work package leaders have been requested to define the evaluation criteria for the WP they are responsible for.

2.2 Document Structure

The rest of this document is divided in 2 main sections:

- **General evaluation criteria:** it introduces general evaluation criteria and some general evaluation actors (actors responsible of the project evaluation).
- **WP-based evaluation criteria:** more accurate and specific evaluation criteria are provided in order to evaluate separately each WP. For each WP, we provide the success

indicators extracted from the Dow, and the measurement methodologies with a description of the criteria. In order to facilitate the reading we separate the criteria according to each task assigned to the WP. For each task, the criteria are presented in table format. These criteria will be useful in the further iteration of the deliverable when the project will have to be assessed.

3 General Evaluation Criteria

3.1 Different measurement methodologies

More than considering only numerical target, it is needed a more complete assessment, including analysis of users behaviour and satisfaction or the analysis of documentation produced. Three different ways of measure will be used to control the progression and outcome of project, which are listed in the following table:

Code	Typology	Description	Example
Q	Quantitative	This refers to clear quantitative indicators with a numerical target.	Number of accesses
R	Report	This measurement typology indicates that the success indicators are in part quantitative, but also qualitative. In order to have a better evaluation, such indicators require a more detail analysis. This detail analysis may require several lines of description (it won't be a separate document).	Capacity to attract investment
I	Interviews and user Interaction analysis	For all indicators including the user interaction and satisfaction it is impossible to evaluate the success status without an analysis of real user behaviour in managing the system. For this reason this class of indicators will be used where user interaction is needed.	User interface satisfaction

3.2 General Success Factor Indicators

Outcomes from research, prototyping and implementation scenarios will be measured according to the criteria defined below and when the results are not positive, an alternative solution will be considered and implemented. The vision underlying this approach is that

the success indicators will be used in TAS³ as a fundamental management tool. The general indicators are grouped under the four main categories of Research, Technology, and Exploitation in the following table.

Indicator		Type	Threshold value/assessment method
R	**Research**		
R1	Monitoring evolution of the existing approaches (projects, papers, references taken into consideration)	Q,R	The ones foreseen by DoW
R2	Numbers of International and national papers published, conferences, journal, expositions and joint events	Q,R	At least 10 published papers in relevant journals or conferences
R3	Transfer of TAS³ results in universities educational activities (e.g. theses, course materials, etc.)	Q,R	Equal greater than five (5)
R4	Invitations and contributions to working groups by standardization / specification bodies	Q,R	Equal greater than five (5)

Indicator		Type	Threshold value/assessment method
T	**Technology**		
T1	Technical documentation produced	Q	At least the documentation foreseen by the DoW
T3	Number of TAS³ framework prototypes	Q	The prototypes foreseen by the DoW
T4	Security and privacy requirements captured	Q, I	- Security Experts should be interviewed - 70 % of Security and Privacy requirements should

			be captured
T5	User centricity	R, I, Q	I : analysis on user satisfaction : a successful result would be to obtain an score of over 70% in the satisfaction measure at the end of the project R : a short report based on these analysis as well as information related to support of the Manifesto which will focus on user centricity (in T11.5) Q: number of Manifesto Signatories

Indicator		Type	Threshold value/assessment method
E	**Exploitation**		
E1	Press echoes (articles, references, etc)	R,Q	Three (3)
E2	Reference to TAS³ project	Q	At least 300 references to TAS³ and its deliverables within 18 months
E3	Co-operation with other projects (European and world-wide)	Q,R	At least two (2)
E4	Public website statistics report	Q	300 unique visitors per month and at least 3,000 web downloads of project public deliverables within 18 months
E5	Public workshop	Q	Minimum of 8 public workshops held with project partners and external participants, providing review and assessment of project deliverables – as independent events or as part of larger events
E6	Track in an international conference	Q	At least 200 delegates attending the track organized by TAS³ partners in an international conference
E7	Publication of the web site news	Q	Regular publication of news on the web site aggregated as a newsletter and number of readers over 3000
E8	Policy papers	Q	Policy papers taken into account or referred to by at least 3 countries or 3 leading organizations beyond the current consortium
E9	Dimension of the TAS³ community	Q	Establishment of a network of at least 100 European experts, professionals, policy makers

			supporting the outcomes of TAS³
E10	Trainings	R	All partners have a unified and deeper understanding of the TAS³ philosophy, architecture, modules, workflow and integration issues involved. The project will measure the efficiency and outcome of the training using surveys and progress testing. In the later stage the project will also do the same for the demonstrators and end-users.
E11	Number of software prototype downloads	Q	Hundred (100)

3.3 General Evaluation actors

Considering that we have to perform the evaluation of the technical platform, the actors that have been identified as the ones to be involved in TAS³ evaluation framework are the following (the evaluation shall be both internal and external) :

TAS³ Developers are involved in the internal evaluation, which is based on the exploitation of the specific competences of the partners who can provide a competent and as much as possible unbiased opinion on the considered targets. The internal validation can be considered as a first level of evaluation. The involved internal actors, selected on the basis of their competences, market position etc., can be considered as a mean to be prepared for Post Implementation review. Project researchers, Technology providers and Industrial partners are the main TAS³ developers.

External validation involves **TAS³ Users** according different perspectives. In fact TAS³ users can be intended as end users of TAS³. The test bed end-users represented in the Consortium (Employability in the Netherlands and the United Kingdom, eHealth in the Netherlands and Belgium) have in fact driven the TAS³ approach. These business environments are currently all disillusioned by the barely networked personal information they need on a daily basis. Currently there is no flexible, adapted but mutually trusted "knowledge on demand" supporting business processes that require personal information. TAS³ intends to make a real impact in this area throughout Europe.

4 WP-based evaluation criteria

4.1 WP1 Requirement Analysis

As mentioned in the DoW, the Requirements Analysis WP1 led by SAP constitutes the real start of the project. It is the place where all participants gather to meet and discuss the requirements both from a (1) research, (2) technical, (3) architectural and (4) user perspective and a dual compliance (both for (5) legal compliance and for (6) the NESSI reference architecture compliance). Finally WP1 will also provide in a solid (7) overall risk analysis.

4.1.1 Success Indicators

As mentioned in the DoW, This activity will be successful if:

- The functional and technical system specification has timely input of its work package partners and can build on the results thereof;
- Technical partners timely contribute their state of the art analysis and requirements;
- Pilot Partners see their requirements being fulfilled and described in quality.

4.1.2 Measurement methodologies

T1.1 State of the art and technology assessment (SAP)

WP/N	Indicator	Type	Threshold value/assessment method
1.1	Deliverables	R	Evaluation of quality and consistency of the provided deliverables

T1.2 Requirements Assessments (KUL)

WP/N	Indicator	Type	Threshold value/assessment method
1.2.	Requirements documentation produced	R	Assessment is based on a report that evaluates the following: • if all requirements provided by the partners are properly documented • if they are organized and categorized in a readable manner • if there are helpers and pointers provided for the partners/readers to find relevant information

1.3	Security and Privacy requirements analysis	R	Assessment is based on a report that evaluates the following: • appropriate methods are used to capture and analyze quality requirements (for each quality concern document if and which method has been used). • requirements that appeared after initial iteration are integrated. • methods to detect and address conflicts and to make the requirements consistent are used.
1.4	Validation activities for requirements that demand new research or development of new components	R	Report: document if the work packages have forgotten to provide validation activity plans for any requirements.
1.5	Validation of the requirements with the architecture	Q, R	Quantitative: Contains a quantitative count of requirements that are mapped to the architecture after the first iteration of the mapping. >=50-% is expected. After the second iteration, we will count again to see if improvement has been made (if the number of requirements that are not mapped are significantly decreased). Report: The report will include detailed analysis of what is missing and which inconsistencies have been successfully addressed.
1.6	Number of international and national publications based on or related to the deliverable	Q	Count the number of publications. We expect to have at least 2 publications related to this deliverable.

NB. Since D1.2 will not be iterated again at the end of the project, we have chosen to provide evaluation criteria that can be executed after the final iteration of the Deliverable. Specifically, we have criteria to evaluate that all security and privacy requirements are addresses as best as possible, inconsistencies among the requirements are addressed, validation activities are planned by all work packages, and the requirements map to the architecture consistently.

T1.4 Design requirements of and adjusted, process driven trust and security environment (SAP)

WP/N	Indicator	Type	Threshold value/assessment method
1.7	Number of fulfilled requirements	Q	>= 50% of proposed requirements. It contains a quantitative count of requirements that are mapped to the architecture.
1.8	Use of a formal framework to design security & trust high level requirements	R	Evaluation of the tool that has been used
1.9	Use of a coherent language to express requirements	R	Evaluation if a methodology for expressing requirements has been used
1.10	Collaboration with pilot partners	I	Description of involvement of industrial partners in the activity work, with interview of some of them. Pilot partners give their opinion if their requirements have been fulfilled in a correct way.

4.2 WP2 Framework, Architecture and Semantics

The main objective of this work package is to specify the global picture of the **TAS³** system, which means that it closely interacts with the following seven work packages: the requirements (WP1), securely adaptable business processes (WP3), information protection (WP4), trust policy management (WP5), legal, privacy & ethics (WP6), IDM authentication and authorization (WP7) and trusted application infrastructure (WP8). VUB and Symlabs will ensure the embedding of the semantic/ontology layer into the architecture which includes the anchoring, updating processes, defining and enforcement of responsibilities.

4.2.1 Success Indicators

This activity will be successful if:

- The different stake holders agree to commit on the **TAS³** upper common ontology;
- A security officer is able to confirm that the architecture corresponds with the ontology and vice-versa;
- A security officer is able to deactivate parts of the **TAS³** stake holders or their components, e.g., if they should behave in a manner that is inconsistent with the

ontology, or if their trustworthiness should be deprecated, and this without dramatically decreasing the reliability of the **TAS³** system.

- The integration scheme of the ontology into the **TAS³** architecture, performed by VUB, covers all architectural conceptual modules and architectural roles, and all relevant partners have agreed on it.
- Two releases of the architectural embedding of the semantics are foreseen, with as a major milestone the consortium-wide acceptance of the architecture.
- TAS³ partners are able to place their research in context of the reused prior art in identity management, authorization, and web services as well as in context of the other TAS³ components and research contributions.
- No serious interoperation problem, attributable to design flaw or omission, is detected between TAS³ developed components during the project.
- No serious security breach, attributable to a design flaw or omission, is revealed during the project or two years following it.

4.2.2 Measurement methodologies

T2.1 Service Ontology and Lower Common Ontology Specification (VUB)

The lower common ontology will be further developed based on the input from tasks T2.5, T4.4, T5.5 and T6.3.

WP/N	Indicator	Type	Threshold value/assessment method
2.1	Service Ontology	Q	The service ontology will draw on concepts defined from the upper layers. These ontologies will contain at least 150 lexons related to the pilots in WP9.
2.2	Service Ontology	R	The pilot partners will check that the ontology represents the concepts and the relations among them, and that no refinement is required.
2.3	Lower Common Ontology	Q	The common lower ontology will draw on concepts defined in the upper layers. This layer will contain 250 lexons.
2.4	Lower Common Ontology	R	The technical partners will check that the ontology covers the concepts central to security policies, and that no refinement is required.

T2.3 Upper Ontology Specification (VUB)

WP/N	Indicator	Type	Threshold value/assessment method
2.5	Upper Common Ontology	Q	The common upper ontology will draw on concepts defined in the descriptive upper ontology and will cover general concepts in the field of security and privacy. This layer will contain at least 200 lexons.

T2.4, T2.6, T2.9, T2.10 Architecture (SYM)

WP/N	Indicator	Type	Threshold value/assessment method
2.6	Validity of the architecture	R	• No argument has been brought demonstrating an architectural principle to be invalid, insecure, untrustworthy, or detrimental to privacy • No argument has been brought demonstrating an architectural omission leading to lack of security, trustworthiness, or privacy • No law suit has breached an architecturally guaranteed privacy,confidentiality, or nonrepudiation property
2.7	Trust Security and Privacy achievements	R	• No architecture level trust flaw has been reported • No architecture level security flaw has been reported • No architecture level privacy flaw has been reported
2.8	Performance of the architecture	R	• No exponential time, or worse, behaviour has been demonstrated, imputable to the architecture, except for public key crypto operation • No positive feedback loop has been demonstrated • No successful denial of service attack has been mounted on the architecture, as opposed to inadequate or buggy implementation. • In particular, a DoS attack qualifies if it succeeds due to cost of computing or network traffic imputable to the architecture itself rather than the implementation
2.9	Maturity of the architecture	R	• At least two independent implementations of each core security modules are mature, including internal and

			external implementations; mature beyond beta test • There are at least 100 reported bugs, but less than 20 unresolved bugs
2.10	API	R	• There is an undisputed acceptance of the official wire protocol • There is an undisputed acceptance of the official API • The API is bound to at least on 5 programming languages, necessarily including Java and C#

T2.7 Glossary Maintenance (VUB)

WP/N	Indicator	Type	Threshold value/assessment method
2.11	Glossary	R	The partners have checked the content and it includes all core terms used in the different deliverables.

T2.12 Refine use cases and user experience produce internal document (UNIZAR)

WP/N	Indicator	Type	Threshold value/assessment method
2.12	Tangibilization of services	R	Assessment is based on a report that evaluates the following: • Problems associated with lack of tangibilization of services. • The impact of lack of tangibilization on users' behavior and perceptions. • Ways of tangibilization of services.

4.3 WP3 Securely Adaptable Business Process

The main objectives of this work package led by KARL are to:

- provide security mechanisms to handle authorization and access control of workflows and their contexts, e.g., human participants involved and underlying application data
- provide security mechanisms to support adaptations of live processes
- support the security requirements of adaptive workflow management in trusted distributed personal information processing and eHealth scenarios.

- have all relevant business process descriptions annotated to a common, agreed upon semantic knowledge structure in line with partners.

4.3.1 Success Indicators

This work package will have been successful if it delivers:

- a design document that describes a comprehensive secure adaptable process infrastructure which fulfils all the objectives set for this work package;
- open source software that has the functionality described in the design document, satisfying the requirements of the application demonstrators described in WP9.
- all relevant elements of the general **TAS³** business process description being annotated towards the ontology, including acceptance of the Upper Common Ontology by the consortium, commitment to the BPMN annotations by the partners.

4.3.2 Measurement methodologies

The design of a business process management platform, offering security features for business processes, security related process adaptation, underpinned by semantics is reported in D3.1. The conception is an iterative process and is planned with three milestones resulting in three iterations of the deliverable D3.1.

The implementation of the conceptual design to support security and trust as well as adaptability of business processes is reported in D3.2. The development follows the conceptual design, i.e. there also exist three iterations of implementations and of the deliverable D3.2.

The third kind of results of WP3 is the outcome of the conceptual design and the respective implementation of secure adaptable business processes into the overall project framework and validating it in the trust applications of employment and eHealth. The results will be described in deliverable D3.3. We will achieve it in three iterations based on the corresponding results of the iteration of the conceptual design and the components implemented.

T3.1.1 Business process-related ontology of trust and security for business process models (VUB)

WP/N	Indicator	Type	Threshold value/assessment method
3.1	Service Ontology	Q	This service ontology will represent concepts related to business process models. This ontology will contain at least 50 lexons.
3.2	Annotation Tool	R	The tool will be accessed via BPMN tools and will enable the annotation of business process models with concepts

			defined in the ontologies.

T3.1.2 Developing Security mechanisms for business processes (KARL)

WP/N	Indicator	Type	Threshold value/assessment method
3.3	Adapting and defining security mechanisms for business processes	R, Q	>= 70% of the requirements of business-process specific security and trust mechanisms (see D1.2 and D1.4) supported by new or adapted components and functionality.
3.4	Formal specification of the process-specific mechanisms	R	Report with the formal specifications
3.5	Integration into the TAS³ framework	Q	>= 70% of the components integrated into the TAS³ architecture
3.6	Number of related publications	Q	>= 1 paper

T3.1.3 Implement features for specifying security at the business process design level (KARL)

WP/N	Indicator	Type	Threshold value/assessment method
3.7	Specification of security and trust properties at the business process modelling level	Q	Description of the extension of modelling concepts for business processes with security properties and transformation of the security modelling to the security enforcement level. Supporting more than 50% of the security and trust specifications of the pilot applications for business processes..
3.8	Transformation to the enforcement level	Q	>= 50 % of the security and trust annotations will be semi-automatically transformed to concepts of the enforcement framework
3.9	Number of related	Q	>= 1 paper

	publications		

T3.1.4 Enforcement of security and trust specifications for business processes (KARL)

WP/N	Indicator	Type	Threshold value/assessment method
3.10	Implemented components of security mechanisms for business processes, and interaction/integration with a business process management engine	Q Q	>= 70% of the security components for business processes (following the iterations in T3.1.2) implemented. All implemented components tested with applications of the pilots.
3.11	Number of related publications	Q	>= 1 paper

T3.2.1 Define and implement concepts for process adaptation (KARL)

WP/N	Indicator	Type	Threshold value/assessment method
3.12	Mechanisms to structurally adapt business processes	Q	support adaptation at least on two levels: on a (basic) task-based level and on subprocess level. >= 50% of the test cases from the pilot applications for process adaptation are supported.
3.13	Guide process adaptations using security rules and obligations	R Q	Description of rules for process adaptations resulting from the security mechanisms of the TAS³ framework. > = 70% of the rules supported
3.14	Supporting users at semi-automatical adaptations	I	Interview with application partners on adequateness of the support to facilitate adaptation
3.15	Number of related	Q	>= 1 paper

	publications		

T3.3.1 Integrating the business process platform with the TAS³ framework and use cases (KARL)

WP/N	Indicator	Type	Threshold value/assessment method
3.16	Documentation of the integration of the concepts of adaptable secure business processes into the TAS³ security framework	R Q	The integration will result in refined or new security components and the interactions with the other components of the TAS³ security framework >= 70% of the most relevant security components checked for business process specific properties
3.17	Applying business processes in the scenarios to show how the security-aware business processes support the use cases of the project	Q I	At least 50% of the scenarios should be supported by the business process platform Interview of some industrial partners on support by security-aware business processes

4.4 WP4 Information Protection

The goal of this work package led by KUL is to analyze the data and information specific requirements of the work packages WP5, WP6 and WP7, and of the employability and healthcare use cases.

Given these requirements, this work package will research the necessary components for the TAS³ architecture, and propose the information containers and integrated secure repositories in which these containers will be stored to form a privacy-preserving repository

from which it is impossible to extract information without being able to present the necessary credentials.

4.4.1 Success Indicators

This activity will be successful if this work package:

- produces the specification of a generic information container that is consistent with the requirements specified by the requirements work package;
- outputs an implementation of integrated secure repositories implementation supporting context specific identifiers and sticky policies, and that allows access to privileged information in case of exceptional situations, e.g., if the break the glass condition was triggered.
- the service ontologies corresponding with the work result in useful material to derive the lower common ontologies from.

4.4.2 Measurement methodologies

T4.1 Specification of an identifiers and token issuance services (SYM)

WP/N	Indicator	Type	Threshold value/assessment method
4.1	Pseudonymity	R	Identifier assignment and passing does not leak a correlation handle.
4.2	Logistics	R	Identifier management allows any required identifier, for architecturally foreseen operation, to be discovered with maximum of 4 over the net transactions and maximum of 6 public key cryptography operations. Authorization and trust and privacy negotiation steps are excluded from these quotas. The public key crypto quota is increased by number of input and output credentials that need to be verified and issued.

T4.2 Specification of secure data repositories and authoritative repositories (KENT)

WP/N	Indicator	Type	Threshold value/assessment method
4.3	Information container	Q	The information container specified in this WP is able to seamlessly cope with at least 90% of the requirements specified in the requirements WP

T4.3 Providing an implementation of Integrated Secure Repositories (KUL)

WP/N	Indicator	Type	Threshold value/assessment method
4.4	Software compotents available	Q	All (100% of the) software components produced by this WP and that are required by other WPs are freely available to all project partners
4.5	Secure Audit Mechanism	R	The secure audit mechanism is functional and can be used by other TAS3-enabled components with minimum development effort
4.6	Policy Evaluation works	R	The policy evaluation components produced by this WP are correctly evaluating incoming requests against specified policies.
4.7	Privacy-preserving trust negotiation	Q, R	The trust negotiation subsystem produces by this WP allows a client to determine, in a privacy-preserving manner, whether or not it possesses the required credentials/attributes for a service.

N.B : for T4.4 see T2.1.

4.5 WP 5 Trust Policy Management

The overall objective of this work package led by TU/E is to create an expressive, flexible Trust Management (TM) framework, which leads to the following concrete objectives:

- Define a flexible TM architecture.
- Create an efficient TM policy evaluation engine.
- Provide Trust feedback mechanisms based on the evaluation of behavior, policy compliance and key performance indicators.

4.5.1 Success Indicators

This work package will have been successful if:

- Pilot partners are able to express the trust policies they identify for the use cases.
- The implementation is able to handle the policies extracted from the use cases.
- The trust management system interoperates with the other TAS³ components.
- The different components interoperate within the TM architecture, allowing evaluation of trust policies based on multiple trust metrics.

- The component responsible for making trust decisions, called Trust Policy Decision Point (Trust PDP), is able to
  - accept trust evaluation requests expressed in XACML request context.
  - determine the applicable trust policies expressed in combined TAS³ trust policy language and determine the trust metrics to be evaluated.
  - call trust services to evaluate trust metrics and combine their results.
  - support the integration of new trust services.
- The reputation based trust service (RTM service) is able to
  - provide a trust metric language which can be embedded in a combined trust policy language.
  - collect trust feedback information, i.e. ratings of behaviour and performance, through a trust information collection point.
  - accept reputation metric evaluation requests and compute corresponding reputation based on the collected feedback.
  - scale well with large number of participants and large volumes of feedback.
- The Key Performance Indicator service (KPITM service) is able to
  - provide a trust metric language which can be embedded in a combined trust policy language.
  - collect KPI feature information from different sources, capturing different aspects of any quantifiable performance parameter.
  - accept KPI metric evaluation requests and compute corresponding performance scores based on the different factors.
  - provide a flexible trust evaluation model that can be adapted to the user preferences through the use and prioritization of different existing and novel performance factors.
- The Credential based trust service (CTM service) is able to
  - provide a trust metric language which can be embedded in a combined trust policy language.
  - collect credentials chains relevant to a the trust query.
  - accept CTM metric evaluation requests and derive trusted parties based on the credential chains discovered.
  - support nested policies which embed other trust services in the credential issuing and combining rules themselves.

4.5.2 Measurement methodologies

T5.1, T5.4, T5.6 Trust Architecture, its implementation and its usability (TU/E, UNIZAR)

Related documents: D5.1, D5.4, D.5.1 and D2.2

WP/N	Indicator	Type	Threshold value/assessment method
5.1	Expressiveness of the trust policy language	Q	The trust policy language is able to express at least 75% of the use case trust requirements identified by the pilot partners.
5.2	Trust policy usability	R, (Q, I)	Analysis of focus group usability tests. The analysis test a service games covering: - a quantitative analysis of questionnaires identifying different player profiles, trust policy effectiveness and influence of anonymity on policy selection. - focus group interviews determining the perceived usability and other player opinions.
5.3	Effectiveness of the trust policy management system	Q	The trust policy system passes 90% of the test cases provided by project partners.
2.4,5.4	Documentation of the TAS3 Architecture	R	Description of the overall TAS3 architecture and its use of the trust management framework
5.5	Documentation of Trust PDP	R	Description of the design, implementation and interface of the Trust PDP
5.6	Number of Trust PDP test cases passed	Q	Trust PDP passes >= 90% of test cases provided by project partners
5.7	Integrated and extendable Trust PDP	R	Description of the Trust PDP and its interaction with trust services

T5.2 Behavioural (i.e. Reputation based) trust engine - RTM service (KARL)

Related documents: D5.1, D5.2

WP/N	Indicator	Type	Threshold value/assessment method
5.8	Documentation of RTM service	R	Description of the design, implementation and interface of the RTM engine
5.9	Number of RTM service test cases passed	Q	RTM engine passes >= 90% of test cases provided by project partners
5.10	Integration of the RTM service in the Trust Management Architecture	R	Description of the deployment and usage of the RTM service within the Trust Management Architecture
5.11	Use a stress test to evaluate RTM service scalability	Q	The RTM engine is able to handle >= 50 concurrent users and 150 requests per second

T5.3 Novel trust metrics (SAP)

Related documents: D5.1, D5.3

WP/N	Indicator	Type	Threshold value/assessment method
5.12	Documentation of KPITM engine	R	Description of the design, implementation and interface of the KPITM engine
5.13	Number of KPITM service test cases passed	Q	KPITM engine passes >= 90% of test cases provided by project partners
5.14	Integration of the KPITM service in the Trust Management Architecture	R	Description of the deployment and usage of the KPITM service within the Trust Management Architecture
5.15	Scalability of the KPITM service	Q	The KPITM service supports >= 20 different performance factors.

T5.4 Trust tool set (TU/E)

Related documents: D5.1, D5.4

WP/N	Indicator	Type	Threshold value/assessment method
5.16	Documentation of CTM service	R	Description of the design, implementation and interface of the CTM engine
5.17	Number of CTM service test cases passed	Q	CTM engine passes >= 90% of test cases provided by project partners
5.18	Integration of the CTM service in the Trust Management Architecture	R	Description of the deployment and usage of the CTM service within the Trust Management Architecture
5.19	Nested policies test cases passed	Q	CTM supports nested policies with 2 levels of trust, passing at least 90% of test cases with such policies

N.B : for T5.5 see T2.1.

4.6 WP6 Legal, Privacy and Ethics

The main objectives for this work package led by Oracle are:

- To define the privacy requirements and to develop the privacy policy architectures and contractual frameworks that create the information governance structure of the **TAS³** model.
- To ensure the correct interpretation and implementation of data protection, sharing, access and use of information are essential elements of trust required for various stakeholders, especially individuals – such as patients and employees, to participate in these system implementations.

- To ensure that minimum legal requirements are met providing a foundation for the more sophisticated services allowing an individual to access and control their personal information. Meeting these stakeholder requirements will play an important part in assuring user acceptance of the system.
- To take into account, *wherever appropriate for any task in the project*, the relevant EU legislation, the Council of Europe's Recommendations, the OECD guidelines, the WHO and WMA declarations and codes of good practices in the health sector, the ILO conventions relating to employees' privacy and confidentiality of personal data, as well as relevant national legislation.

4.6.1 Success Indicators

While improvements and changes will be made on an ongoing basis, testing of both deliverables will be prepared for use with each major phase completion of the project; it is only at these inflection points and testing iterations that effectiveness of the ongoing enhancements can be properly evaluated after which new needs analysis and mapping of functionality will determine further work that needs to be undertaken.

Therefore success of the project will be determined in three main ways:

- The ability of the generated policies and policy statements to functionally represent the needed controls in system operation.
- System testing and operation to assure that the contractual framework is flexible enough to adapt to needed future changes and complete enough to cover current obligations and limitations.
- The conviction and belief of subject matter experts in DPAs and related agencies that **TAS³** is complete and useful.

4.6.2 Measurement methodologies

T6.1 Identify legal requirements

WP/N	Indicator	Type	Threshold value/assessment method
6.1	Documentation of legal data protection requirements produced	R	The relevant deliverables must provide a comprehensive list of data protection requirements as they relate to the actors, components and services of the TAS³ network. We will also be updating these requirements through the course of the project to assure that they not only capture existing requirements, but reflect the emerging state of the art. Assessment as to completeness and granularity of these

			requirements.

T6.2 Validation of requirements

WP/N	Indicator	Type	Threshold value/assessment method
6.2	Feedback on identified requirements	I	The use of contract framework elements by the pilots as well as consultations with experts both within and outside of TAS³ as to ability of the framework to support business needs in a trust-enabled, user-centric way that, meets or exceeds the legal requirements of data protection. Value assessment of the contract infrastructure will need to progress with the development and deployability of the infrastructure as they are linked. We will do use relevant stakeholders/experts to assess value and functionality in the process of development. We have developed an internal TAS3 functional group to provide input to contract development to assure that the contract framework is closely linked to technology development.

N.B : for T6.3 see T2.1.

T6.4 Controlled natural language policies (KENT)

WP/N	Indicator	Type	Threshold value/assessment method
6 .3	Documentation of controlled natural language policy creation software	R	The documentation should describe to users how they can create policies in controlled natural language
6.4	Controlled Natural Language policy creation software	Q	There is open source software that allows security officers to create authorisation policies in controlled natural language, and the policies are then automatically converted into XML for feeding into a PDP.
6.5	User trials	R,Q	Users will be given a sample policy to create and their performance will be measured quantitatively (% of correctly generated policies) and qualitatively (via a questionnaire)

T6.5 Development of a contractual framework

WP/N	Indicator	Type	Threshold value/assessment method
6.6	Documentation of contractual framework	R	The contractual framework must be sufficiently comprehensive to ensure contractual binding of all the principal actors in TAS³, as well as the potential legal consequences of the ordinary or extra-ordinary functioning of major TAS³ components.

T6.6 Validation of the contractual framework

WP/N	Indicator	Type	Threshold value/assessment method
6 .7	Further iterations of contractual framework	R	Incorporation of references to the components and actors developed or described by other partners in the legal deliverables where appropriate.

T6.7 Provide assistance to other work packages

WP/N	Indicator	Type	Threshold value/assessment method
6.8	Incorporation of legal requirements by other work packages	R	Collaboration with project partners. Partners have integrated or at least cross-referenced those requirements relevant to their area of work in their deliverables.

T6.8 Dissemination towards standardization bodies

WP/N	Indicator	Type	Threshold value/assessment method
6.9	Documentation of dissemination efforts towards standardization bodies	Q, R	Formal liaison or membership status with at least two standardization bodies active in the field of identity management, security and/or trust. At least a total 60 pages of comments or contributions to standardization bodies with which a formal relationship has been established on work items that are related to TAS³ research.

4.7 WP7 Identity Management, Authentication and Authorization

The overall objectives are the following :

- build a fully dynamic authorization infrastructure that allows credentials to be dynamically created and delegated between users and administrators, and policies to be dynamically managed and updated
- incorporate sophisticated real-life authorization requirements such as Break the Glass policies, dynamic separation of duties, state based decision making and adaptive audit controls
- contribute to international standards development in the area of IdM and authorization protocols and profiles and authorization ontology

4.7.1 Success Indicators

This work package led by KENT will have been successful if:

- it delivers a design document that describes a comprehensive IdM, authentication and authorization infrastructure which fulfils all the objectives set for this work package;
- it delivers open source software modules that have the functionality described in a design document;
- the open source software satisfies the requirements of the application demonstrators described in WP9;
- the **TAS³** partners formally agree to the designed ontology and a majority of the protocol specifications that are produced have been accepted by standards bodies for publication.
- a formal agreement of relevant **TAS³** partners on the ontology part has been obtained.

4.7.2 Measurement methodologies

T7.1. Protocol and ontology standardisation

WP/N	Indicator	Type	Threshold value/assessment method
7.1	Design Documentation	R	The design document (Deliverable D7.1) captures 100% of the high level requirements as specified in the DoW

7.27	Contribution to international standardisation efforts	Q	WP7 will have produced at least 8 inputs to various standards bodies

T7.1.2 Authorization Ontology (VUB)

WP/N	Indicator	Type	Threshold value/assessment method
7.2	Authorization Ontology	Q	This ontology will represent standard concepts related to authorization. This ontology will contain at least 50 lexons and will have been formally accepted by the project partners

T7.2 Design & implement an application independent Break the Glass Identity Management infrastructure using an Application Independent PEP (AIPEP) and Obligations

WP/N	Indicator	Type	Threshold value/assessment method
7.3	Break the Glass (BTG) software module	Q	There is an open source software module that implements the BTG functionality
7.4	The BTG documentation adequately describes the functionality, interfaces and configuration of the BTG software module	R	Partners in the project have taken the BTG software module and have successfully installed it on their sites
7.5	Obligations Service	Q	There is an open source software module that implements an Obligations Service
7.6	The Obligations Service documentation adequately describes the functionality, interfaces and configuration	R	Partners in the project have taken the Obligations Service software module and have successfully installed it on their sites

	of the Obligations Service software module		

T7.3 Design & implement a multiple policy evaluating authorization infrastructure

WP/N	Indicator	Type	Threshold value/assessment method
7.7	A Master PDP that supports multiple policies in multiple languages	Q	There is an open source Master PDP software module that implements the multiple policy combining functionality
7.8	The Master PDP documentation adequately describes the functionality, interfaces and configuration of the Master PDP software module	R	Partners in the project have taken the Master PDP software module and have successfully installed it on their sites

T7.4. Design and implement a delegation service to meet the requirements of the use-cases and Deliverable D1.2. e.g. role based delegation rules, task based delegation, invitation based delegation

WP/N	Indicator	Type	Threshold value/assessment method
7.9	Credential creation software module	Q	There is an open source software module that creates user credentials
7.10	The credential creation documentation adequately	R	Partners in the project have taken the credential creation software module and have successfully installed it on their sites

	describes the functionality, interfaces and configuration of the credential creation software module		
7.11	Delegation of Authority (DoA) software module	Q	There is an open source software module that implements the DoA functionality
7.12	The DoA documentation adequately describes the functionality, interfaces and configuration of the DoA software module	R	Partners in the project have taken the DoA software module and have successfully installed it on their sites

T7.5. Design, implementation and testing of the attribute aggregation functionality using an account linking service, taking into consideration the Level of Assurance (LoA)

WP/N	Indicator	Type	Threshold value/assessment method
7.13	Attribute aggregation software module	Q	There is an open source software module that implements the attribute aggregation functionality
7.14	The attribute aggregation documentation adequately describes the functionality, interfaces and configuration of the attribute aggregation	R	Partners in the project have taken the attribute aggregation software module and have successfully installed it on their sites

	software module		

T7.6 Design, implementation & testing of a dynamic policy management infrastructure, in which different policy authorities can update their policies and distribute them to the PDPs

WP/N	Indicator	Type	Threshold value/assessment method
7.15	Dynamic management of policies	Q	There is an open source software module that allows policies to be dynamically updated
7.16	The policy management documentation adequately describes the functionality, interfaces and configuration of this software module	R	Partners in the project have taken the policy management software module and have successfully installed it on their sites

T7.7 Design, implementation & testing of system for static and dynamic Separation of Duties policies

WP/N	Indicator	Type	Threshold value/assessment method
7.17	Separation of Duties (SoD)	Q	There is an open source software module that implements the SoD functionality
7.18	The SoD documentation adequately describes the functionality, interfaces and configuration of the SoD software module	R	Partners in the project have taken the SoD software module and have successfully installed it on their sites

T7.8 Design, implement and test an Enhanced Credential Validation Service (CVS)

7.19	Credential validation service (CVS)	Q	There is an open source software module that provides a credential validation service and will validate credentials in different standard formats
7.20	The CVS documentation adequately describes the functionality, interfaces and configuration of the CVS	R	Partners in the project have taken the CVS software module and have successfully installed it on their sites

T7.9 Design and Implement Trust and Policy Negotiation Service

WP/N	Indicator	Type	Threshold value/assessment method
7.21	Trust negotiation	Q	There is an open source software module that implements trust negotiation
722	The trust negotiation documentation adequately describes the functionality, interfaces and configuration of the trust negotiation software module	R	Partners in the project have taken the trust negotiation software module and have successfully installed it on their sites

T7.10 Design & implementation of adaptive auditing of authorization decisions

WP/N	Indicator	Type	Threshold value/assessment method
7.23	Adaptive	Q	There is an open source software module that implements

	audit controls		adaptive auditing

WP/N	Indicator	Type	Threshold value/assessment method
7.24	The adaptive auditing documentation adequately describes the functionality, interfaces and configuration of the adaptive audting software module	R	Partners in the project have taken the adaptive auditing software module and have successfully installed it on their sites

Other relevant criteria for this WP

WP/N	Indicator	Type	Threshold value/assessment method
7.25	Scientific papers	Q	WP7 will have either published or had accepted at least 8 scientific papers to international journals and conferences
7.26	Requirements implemented	Q	The software delivered by WP7 will have implemented >75% of the specified requirements
7.27	Integration of components	R? Q?	The delivered open source modules can be successfully integrated into the application demonstrators and also with modules from the other WPs

4.8 WP 8 Trusted Application

This work package led by UNIKOLD will implement all components that are needed in addition to the core security and trust related components, which will be provided by WPs2-

7, in order to assemble a trusted infrastructure that is needed to create working systems which can cover the key processes of the envisaged pilot use cases. This infrastructure will be assembled in work package 12. Fitting together application independent security and trust related components with application specific components to be developed in the work package, the following will be obtained

4.8.1 Success Indicators

The individual tasks are successful if : their products adhere to the specifications set out in WP2 and pass the integration tests developed in WP10. The WP is successful if the components provided have been successfully integrated by WP12 into an environment that is capable to execute the envisaged pilot use case processes and meets the specified trust and security requirements.

4.8.2 Measurement methodologies

T8.1 Secure and trustworthy repository service (UNIKOLD, KENT)

WP/N	Indicator	Type	Threshold value/assessment method
8.1	Security layer for Fedora repository	R	The Fedora repository will be able to communicate to other TAS³ components according to their security requirements.
8.2	Security and privacy requirements captured	R	The Security Experts in TAS³ from University of Kent will cooperate and contribute their knowledge so that the security and privacy requirements will be fulfilled.
8.3	Co-operation with organizations (European and world-wide)	R	Introducing new Fedora features to the Fedora community.

T8.2 Client implementation (UNIKOLD)

WP/N	Indicator	Type	Threshold value/assessment method
8.4	Generic Client, Audit Viewer (Dashboard)	R	The generic client will be able to process the TAS³ Generic Data Format in combination with a TAS³ Fedora repository. The Audit Viewer will be able to visualize the audit data fetched from different Audit Services.

8.5	Security and privacy requirements captured	R	The Security Experts in TAS³ from University of Kent will cooperate and contribute their knowledge so that the security and privacy requirements will be fulfilled.

T8.3 Auxiliary services implementation (UNIKOLD, NOTTINGHAM)

WP/N	Indicator	Type	Threshold value/assessment method
8.6	Transformation Services	R	The transformation service will be able to transform from EuropassCV to the TAS³ Generic Data Format et vice versa.
8.7	Audit Bus	R	All relevant TAS³ services will be attached or registered to the TAS³ Audit Bus.

T8.4 Semantically Enriched Search services implementation (VUB)

WP/N	Indicator	Type	Threshold value/assessment method
8.8	Service Ontology	Q	This ontology will represent concepts related to auditing. This ontology will contain at least 50 lexons.
8.9	Search Engine	R	The tool will be integrated within the TAS³ architecture, and the information retrieval will have high precision and recall.

T8.5 Development of Gateways (RIS)

WP/N	Indicator	Type	Threshold value/assessment method
8.10	TAS³ SOA Gateway	R	Risaris' SOA Gateway will be able to function as an application dependent PEP in front of a legacy database.

4.9 WP 9 Employability and Healthcare Demonstrators

The objectives of this work package led by CUS are:

- To Prove the **generic applicability** of the **TAS³** trust infrastructure for exchanging personal information in different domains, more specifically demonstrate the trust,

security and privacy services required for ICT to support employability, vocational education and lifelong skills development through partnerships of education/training providers and employers, and patient–centric eHealth services.

- To Assure **end-user acceptance** during the design and demonstrator period.
- To Progressively implement the **TAS³** infrastructure to demonstrate the implementation of a generic end2end Trust infrastructure:

4.9.1 Success Indicators

This activity will be successful if:

- A baseline against which progress can be assessed and a developing set of generic requirements are agreed with key stakeholders as supporting national needs within the developing single market for education, employment and eHealth within Europe
- A set of expressions of specific requirements tailored to the needs of particular
- groups in particular contexts are developed
- A working example of a service flow requiring **TAS³** trust and security services is created
- Buy-in is achieved from users and strategic stakeholders for the trialling of **TAS³** services
- A simple working example of **TAS³** services can be assessed against the baseline within a partnership with limited links to resources and services
- A more advanced working demonstration incorporates stakeholder feedback and access to a wider range of resources and service providers
- A final version of the demonstrator works within a realistic ecosystem of service providers and users, including international exchange of personal information if this proves legally and practically feasible.

4.9.2 Measurement methodologies

T9.1 Establish a baseline and position of regional partnerships (1) within UK national strategic architecture, (2) within the Benelux employability market and (3) with a Dutch patient organisation and related care providers. The output of this task consists of Deliverable D9.1 – Pilots Specifications and Use Case Scenarios.

WP/N	Indicator	Type	Threshold value/assessment method

9.1	Number of identified requirements	Q	At least 4 requirements identified for each domain. Requirements are fed back to WP01 activities (D1.2)
9.2	Baseline established	R	Understanding of current systems and environments (State of the Art report D1.1)
9.3	Security and privacy issues identified and addressed	R	Requirements are documented in the context of the scenarios; results are fed back to WP01 activities
9.4	Partnership/ networks established	Q, R	Q: At least one working partnership system deploying the TAS³ framework established by each demonstrator partner R: stakeholder engagement with partnerships/networks, results fed into D9.1

T9.2 TAS³ infrastructure progressively implemented. This task results in deliverable D9.2 – Pilot Evaluation report.

WP/N	Indicator	Type	Threshold value/assessment method
9.5	First integrated demonstrator works: D9.2 evaluation report v1	Q, R	Demonstrator components interact with mock-ups of pilot partner systems; at least one business processes is executed end-to-end; system doesn't crash; data integrity is preserved
9.6	Second demonstrator works using actual systems: D9.2 evaluation report v2	Q, R	Demonstrator interacts with at least 2 real-life systems; at least 2 business processes are fully executed; at least 15 test users are engaged with the system
9.7	Final demonstrator works using larger number of users	Q, R	Demonstrator interacts with at least 3 real-life systems; more than 2 business processes are fully executed; at least 50 test users are engaged with the system

T9.3 Expressions of services submitted to the respective national & European frameworks such as the UK e-Framework, the Benelux employability initiatives, and national/European eHealth authorities. This task contributes to the requirements specified in deliverable D1.4.

WP/N	Indicator	Type	Threshold value/assessment method
9.8	Number of service flows submitted	Q	Documented service flows accepted for serious consideration by framework managers; at least one service flow incorporated into a national/international framework

T9.4 Relate to Ministries and sector organizations responsible for education & employment and eHealth to engage them in the use of TAS³ deliverables. This task contributes to deliverable D11.5.

WP/N	Indicator	Type	Threshold value/assessment method
9.9	Number of agencies engaged with	Q	At least 2 major organisations in each pilot country familiarised with the project

T9.5 Analysis of perceived usability, perceived quality and trust of initial demonstrators and final demonstrators. The results of this task are included in Pilot Evaluation Report D9.2. As well, an internal document H9.1 will be developed explaining the key aspects of Usability and the methodology to be applied in the analyses. (UNIZAR)

WP/N	Indicator	Type	Threshold value/assessment method
9.10	Users perceive system as trustworthy and usable	I, Q, R	I: Interviews with end users and system actors; focus groups to determine the opinions of potential end-users. Q: statistical analysis of questionnaire results, first results used as baseline for comparison; Development of valid scales to measure end-user perceptions (usability, quality, trust, satisfaction, intention to use, etc.). To be successful, these measures need to satisfy steps recommended in scientific literature (content and face validity, exploratory analysis of reliability and dimensionality, confirmatory factor analysis, convergent and discriminant validity) Evaluation of perceived usability, perceived quality and trust of initial demonstrators and final demonstrators. Success will be achieved if statistical evaluation of final demonstrators shows at least 10% improvement over the

			previous baseline result R: explanation of methodologies used to evaluate end-user perceptions, including measurement of end-user perceptions in initial and final demonstrators, and proposal of guidelines based on end-user perceptions
9.11	Methodology chosen matches results to be obtained	Q,R	Q: statistical analysis of questionnaire results with users shows level of trust in the system as greater than 70% R: report summarising findings of usability study shows that users trust the system and the level of trust and usability increases demonstrably with each stage of the demonstrator
9.12	Users are happy with level of performance	Q,R	Q: statistical analysis of questionnaire results with users; users give an average satisfaction rating of 70% R: report summarising findings of usability study

T9.6 Business process modeling of use cases for the different demonstrators according to the possibilities of the TAS³ infrastructure (UNIKOLD)

WP/N	Indicator	Type	Threshold value/assessment method
9.13	Models match use cases	R	Pilot partners are able to verify that models are an accurate representation of use case scenarios
9.14	Models integrate requirements	Q	>50% of requirements covered

T9.7 Interface application specific components, in particular executable business process models, data aggregators (UNIKOLD)

WP/N	Indicator	Type	Threshold value/assessment method
9.14	Integration test	R	Evaluation of component integration and how the integrated system works as a whole
9.15	Efficiency and performance	Q	Testing shows that the system runs reliably and gives a response time of less than 5 seconds
9.16	Reliability	Q, R	Testing shows that data is able to move effectively across interfaces from component to component R: report on system testing

T9.8 Provide graphical user interfaces to allow user interaction for executing the business **processes (UNIKOLD)**

WP/N	Indicator	Type	Threshold value/assessment method
9.17	User satisfaction and understanding	Q, I, R	I: interviews with users demonstrate high level of satisfaction and that the interface is intuitive to use; users give an average satisfaction rating of 70% Q: questionnaires show high level of user satisfaction R: usability report summarising feedback from users
9.18	Interface allows successful interaction with business processes	Q, R	At least two business processes per pilot are accessible to users via the interface and can be monitored successfully R: evaluation report in D9.2

4.10 WP10 Quality Measures and Trustworthiness

The goal of WP10 led by CNR is thus to develop and implement a comprehensive validation methodology of the TAS³ platform and its offered services. In particular, WP10 will work towards the implementation of an innovative on-line testing approach, to be embedded within the TAS³ architecture. To realize such a vision, we need to address two orthogonal objectives:

- We need to develop a testing infrastructure within the TAS³ architecture that will permit to launch and monitor/control the on-line testing session
- We need to identify a strategy for derivation of the test cases to be executed
-

4.10.1 Success Indicators

The level of success of WP10 can be measured against the application of the produced validation methodologies to the demonstrators of WP9. Considering the WP10 with respect to the following tasks:

- **T10.1** (Automatic XML Instances Generation) is successful if the TAXI methodology has been successfully applied to generate a set of instances for black-box testing of some benchmark **TAS³** application
- **T10.2** (On-line Compliance Testing) is successful if the on-line compliance testing approach has been integrated within **TAS³**, after selection of a basic set of test cases to be checked (selection could be manual or automated)

4.10.2 Measurement methodologies

T10.1 Automatic XML Instances Generation

WP/N	Indicator	Type	Threshold value/assessment method
10.1	Scientific papers produced, Number of national/inter national papers	Q,R	Quantitative : 3 Report : The Scientific articles produced
10.2	Technical documentation produced	Q	1 Technical Report
10.3	Number of TAS³ prototypes	Q	The assessment is based on the proof of concept released in D10.2 and D10.4
10.4	Integration with the other TAS³ activities	R	The assessment is based on a technical report that describes the test case generation starting from policy documentation available within TAS³

T10.2 On-line Compliance Testing

WP/N	Indicator	Type	Threshold value/assessment method
10.5	Scientific papers produced, Number of national/inter national papers	Q,R	Quantitative : 3 Report : The Scientific articles produced
10.6	Technical documentation produced	Q	The deliverable D10.3
10.7	Number of TAS³ prototypes	Q	The assessment is based on the prototypes released in D10.2 and D10.4
10.8	User manual and	R	The assessment is based on a Technical Report that can be referred as user manual.

	documentation		
10.9	Integration with the other TAS³ activities	R	The assessment is based on a technical report that describes the specific results from the integration of the On-line Compliance Testing with the other TAS³ activities.

WP 11 Dissemination, Exploitation and Training

The overall objectives of this work package led by EIF are:

- Organize the dissemination, training and exploitation of TAS³
- Raise the level of awareness and understanding of key stakeholders in the European Community on the issues of privacy and security and the benefits to be gained through trusted infrastructures
- Manage efficiently and exploit the knowledge produced by the TAS³ consortium
- Set out the development and exploitation for launching commercial services at the end of the project.

4.10.3 Success Indicators

As mentioned in the DoW, this activity will be successful if. This following number are described in section General Evaluation Factor Indicator since it is concerning the overall project.

- Public website statistics report at least 300 unique visitors per month and at least 3,000 web downloads of project public deliverables within 18 months
- Minimum of 8 public workshops held with project partners and external participants, providing review and assessment of project deliverables – as independent events or as part of larger events
- At least 200 delegates attending the track organized by **TAS³** partners in an international conference
- At least 10 published papers in relevant journals
- Regular publication of the newsletter (bimonthly) and number of readers over 3,000

- At least 300 external references to **TAS³** and its deliverables within 18 months
- Invitations and contributions to working groups by standardization / specification bodies
- Policy papers taken into account / referred to by at least 3 countries / leading organizations beyond the current consortium
- Establishment of a network of at least 100 European experts, professionals, policy makers supporting the outcomes of **TAS³**
- All partners have a unified and deeper understanding of the **TAS³** philosophy, architecture, modules, workflow and integration issues involved. The project will measure the efficiency and outcome of the training using surveys and progress testing. In the later stage the project will also do the same for the demonstrators and end-users.

4.10.4 Measurement methodologies

In the section 11, some dissemination indicators are already used to evaluate globally the project, they are anyway duplicated here as they are providing the assessment related to several dissemination tasks.

T11.1 Design and implementation of the dissemination plan (EIF)

This task evaluation would be successful if the designed and implemented dissemination plan as an impact on the other related dissemination tasks and deliverables. So it will be evaluated in terms of three main categories:

- Webpresence : all aspects related to the website, all related online publications mentioning or related to TAS³ , external references and deliverables downloads.Related deliverable: D11.2
- Publication / events : all aspects related to events, publications and support by external community (press releases, policy papers, standardization bodies). Related deliverables : D11.3, D11.4
- Community : all aspects related to the associate partners, the best practice network (BPN) and the related online communities.Related deliverable: D11.5

WP/N	Indicator	Type	Threshold value/assessment method
11.1	Deliverable D11.1 (Dissemination plan and Communication Handbook)	R	R: evaluation of quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.

11.2	Webpresence (related to D11.2)	Q	Q: public website statistics report an annual increase of: unique visitors public deliverables external references
11.3	Publication (related to D11.3, D11.4)	Q	Q: annual increase of participation in events or publications
11.4	Community (related to D11.5)	Q	Q: annual increase of Manifesto signatories, members of related online communities and/or project associate members

T11.2 Raising public awareness and participation (EIF)

WP/N	Indicator	Type	Threshold value/assessment method
11.5	Deliverables D11.3 and D11.4	R	R: evaluation of quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.
11.6	Workshops	Q	Q: minimum of 8 public workshops held with project partners and external participants, providing review and assessment of project deliverables – as independent events or as part of larger events Q: number of participants to these events
11.7	Conferences	Q	Q: at least 200 delegates attending the track organized by TAS³ partners in an international conference
11.8	Events participation and publication	Q	Q: at least 10 published papers/publications in relevant events / journals
11.9	Website	Q	Q: public website statistics report at least 300 unique visitors per month and at least 3,000 web downloads of project public deliverables within 18 months
11.10	Web reference, web presence	Q	At least 300 external references to TAS³ and its deliverables within 18 months

T11.3 Management of knowledge and intellectual property (SYN)

WP/N	Indicator	Type	Threshold value/assessment method
11.11	Deliverable	R	Evaluation of Quality and consistency of the provided deliverable
11.12	Project portal	Q	One project portal should be provided
11.13	IPR	I	Interviews should be conducted
11.14	Distribute Source Code	R	Assess he distribution of the source code

T11.4 Creation of a public identity for the TAS³ project (EIF)

WP/N	Indicator	Type	Threshold value/assessment method
11.15	Deliverable D11.2	R	R: evaluation of quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.
11.16	Public website, Project brochure, leaflet, videos	Q	Public website statistics report at least 300 unique visitors per month and at least 3,000 web downloads of project public deliverables within 18 months
11.17	Newsletter, news	Q	Regular publication of the online news and news feed aggregation newsletter (bimonthly) and number of readers over 3,000
11.18	Press Release	Q, R	Q: number of published press releases R: evaluation of the impact/community covered
11.19	Trials / Test beds	Q, R	Q: number of demos, trials, test beds available R: evaluation of the project technical results covered by these trials

T11.5 Creation of a Best Practice Network (BPN) for Trust and Identity Access Management (EIF)

WP/N	Indicator	Type	Threshold value/assessment method

11.20	Deliverable D11.5 and Manifesto	R	R: evaluation of quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.
11.21	BPN Size and support of Manifesto	Q	Q: establishment of a network of at least 100 European experts, professionals, policy makers supporting the outcomes of TAS³ This will composed by: Number of Manifesto signatories Number of members of the related online Community
11.22	TAS³ stakeholders opinion(Deliverable H11.1)	R	R: evaluation of BPN consistency

T11.6 TAS³ Associated Partner program (SAP)

WP/N	Indicator	Type	Threshold value/assessment method
11.23	Deliverable D11.5 (Associate Partner Charter part) (Lead : SAP)	Q, R	Q: number of associate partners (signatories of the charter) R: evaluation of quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.
11.24	Events / Participations (Lead : EIF)	Q	Q: number of events (meetings, plugfests, workshops) organised with Associate Partners Q: number of associate partners involved in these events Q: number of external participants

T11.7 Improved technical standards and reference models (EIF)

WP/N	Indicator	Type	Threshold value/assessment method
11.25	Deliverable D11.4 and (standardisation efforts actions plan)	R	R: evaluation of Quality and consistency of the provided deliverable. Reviewers issues raised correctly in new iteration.
11.26	Standardisati-	R	R: invitations and contributions to working groups by

	-on effort		standardization / specification bodies
11.27	Support of Policy papers	R	Policy papers taken into account / referred to by at least 3 countries / leading organizations beyond the current consortium

T11.8 Post-Project Exploitation Plan (SAP)

WP/N	Indicator	Type	Threshold value/assessment method
11.28	Deliverable (D11.6, two iterations)	Q, R	Q: number of Associate partners R: report on level of engagement and outcomes of TAS³ associate partners.
11.29	Stakeholder opinion	R, I	R: conclusions derived from interviews with stakeholders I: focus groups and in-depth personal interviews with different stakeholders to discover their opinions.
11.30	Launching a new service	R	Report on the key aspects to be considered when launching a new service into the market

T11.9 Training requirements for technical partners following first results (NOT)

WP/N	Indicator	Type	Threshold value/assessment method
11.31	Deliverable	Q, R	Q: every partner has identified at least one training requirement and one area for training offering R: evaluation of quality and consistency of the provided deliverable

T11.10 Developing training material and presentations in collaboration with subject matter experts from within the project team (NOT)

WP/N	Indicator	Type	Threshold value/assessment method
11 .32	Project training environment	Q, R	Q: at least two resources on each of 10 major topic areas available to internal partners; each resource accessed a minimum of 10 times R: report on status and usage of environment and incorporation of feedback from participants; evaluation of levels of improved understanding resulting from engagement

T11.11 Video recording of internal face-to-face training sessions (NOT)

WP/N	Indicator	Type	Threshold value/assessment method
11. 33	Session recording	Q	At least one public training session recorded and published via the website as training material

T11.12 Using an LCMS platform for storing and re-using learning objects and delivering training via multiple channels (NOT)

WP/N	Indicator	Type	Threshold value/assessment method
11.34	Project training environment	Q, R	Q: a minimum of two resources available to internal partners on each of 10 major topic areas; each accessed a minimum of 10 times R: report on status and usage of environment and incorporation of feedback from participants; evaluation of levels of improved understanding resulting from engagement
11.35	External use of project training environment and resources	I, Q, R	Q: at least 100 external people accessing and engaging with materials I: interviews to assess outcomes of training in terms of understanding of the project and technology R: report on level of engagement and outcomes

T11.13 Organising face-to-face training sessions and workshops at key points in the project, including before pilot phases (NOT)

WP/N	Indicator	Type	Threshold value/assessment method
11.36	Face-to-face training for external parties	I, Q, R	I: interviews with external partners engaging with formal and informal training Q: at least 10 training events held and a mimimum of 100 individuals engaging with formal project training R: report on level of engagement and outcomes of training
11.37	Report on face-to-face training	R	R: evaluation of quality and fitness for purpose of event; analysis of results of evaluation by participants, including improved awareness/facility/ understanding

T11.14 Produce a TAS³ training manual for all 3 pilots (NOT)

WP/N	Indicator	Type	Threshold value/assessment method

11.38	TAS• training manual	R, I	R: evaluation of quality, consistency and fitness for purpose of the manual I, R: evaluation of accessibility and fitness for purpose by pilot partners and incorporation of feedback into further iterations

4.11 WP12 Overall Integration

WP12 led by KUL, integrates the results of both research and development, maintains test beds, and keeps an overview, without content contributions to the supplying work packages. Of course, this happens in close cooperation with especially WP2 Architecture and all developing work packages.

4.11.1 Success Indicators

This activity will be successful if the integrated system:

- meets the requirements specified in WP1
- demonstrates conformance with the WP2 defined **TAS³** open architecture
- sufficiently passes both the module tests (carried on within WP3-WP8) and integration system testing
- satisfies WP9 pilots users

4.11.2 Measurement methodologies

We make a distinction between local development processes and the project-wide main integration process.
The variety of organisations participating inTAS³, ranging from research institutions to commercial software development companies, leads to a wide spectrum of processes and associated quality assessments and metrics. Few „development metrics“ can be obtained which are available and comparable across all project partners. In order to have at least some indications of development process quality, project partners have been asked to provide a description of their internal quality assurance process. These processes are available in D12.3.1 (End-to-end System Testing). Where possible and relevant, metrics obtained from these internal quality assurance processes will be used to assess the development processes. However there is no underlying methodology, as there is no common ground.

In D12.3.1 we describe how we will establish a "lowest common denominator" base line of

quality assessment processes and metrics that all developing partners can and must adhere to. During project year 3 (2010) this common baseline will be gradually enforced. We expect some teething problems in what will become an organisational change process.

For the main integration process, we follow the methodology outlined in D12.1.1. It is a specialisation of the general TAS³ Quality Assurance process, tuned towards software engineering. The methodology is based on the acquisition of several key performance indicators that come out of the integration process as a by-product. Typical examples are: number of issue reports, number of open issues, etc.

As the integration process is not routinely followed yet, we have no reliable null measurements of most performance indicators (see D12.3.1). Without null measurements it makes little sense to provide target figures for metrics. These targets will be established during project year three, in a conservative manner. Observing the metrics change during the project is the main purpose of the exercise, not meeting targets, as industrial quality software is no TAS³ project goal.

T12.1 Monitoring adherence to the Architecture

WP/N	Indicator	Type	Threshold value/assessment method
12.1	D12.2 Tr&App Integration	R	Expert assessment
12.2	Component Inspection	R	Expert assessment, certification: Req 12.7

T12.2 Central Server Base

WP/N	Indicator	Type	Threshold value/assessment method
12.3	Nagios uptime records	Q	99%
12.4	Tickets on “Central Servers”	Q	Reasonable activity as usage indication
12.5	Tickets on “Portal”	Q	Reasonable activity as usage indication

T12.3 Central Development Resources

WP/N	Indicator	Type	Threshold value/assessment method
12.6	Tickets on “Component	Q	Reasonable activity as usage indication

	Pool"		
12.7	Trac Activity Records	Q	Timeline events per month
12.8	Tickets on "Certificate Authority"	Q	Reasonable activity as usage indication

T12.4 Create and Monitor Development Schedule

WP/N	Indicator	Type	Threshold value/assessment method
12.9	% milestone components in the Pool	Q	Component Matrix inspection
12.10	% milestone completed	Q	Matrix and Wiki inspection

T12.5 Facilitate continuous development

WP/N	Indicator	Type	Threshold value/assessment method
12.11	Tickets between developers	Q	Trac inspection per component
12.12	Components entering "Testing" phase after maturisation	Q	Observation

T12.6 Deliver the demonstrator system

WP/N	Indicator	Type	Threshold value/assessment method
12.13	Demo releases by project management	Q	Observation
12.14	Formal releases by project management	Q	Observation

4.12.3 Availability of Resources and Procedures

As described in D1.2, several resources and procedures must be in place in order to support the integration process. The following list summarizes the availability as of November 13, 2009.

Resource	Provider	Status
Central Interface Documentation Repository	WP12	Available
Short List of Implementation Platforms	WP12	--
Short List of Interface Frameworks	WP12	--
Service Wrapper	WP8	--
Standard Deployment Process	WP12	Available
Quality Assurance and Configuration Management System	WP12	Available
Fault Tolerance in all Components and Interfaces	all devs	--
Escalation Procedure	WP12	Available
Hierarchical Error Reporting	all devs	--
Early Test Equipment Integration	WP10	--
Relevant Interfaces to Real-world Applications	all devs	Some
Stub Applications	all devs	Some
Relevant Demonstrator Applications	WP9	Available
Release Process	WP12	Available
Rollback Process	WP12	Available
Integrated Environment Monitor and Hotline	WP12	Available

Many of the still missing items will be available after the individual developers have completed their documentation, which is all scheduled for PM24. Several items may be canceled as more insight in issues has been gained since the initial requirements were drafted.