SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document type: Deliverable

Title:	Common Ontologies

Work Package: 2

Deliverable Number: D2.2

Editor: Vrije Universiteit Brussel

Dissemination Level: PU

Preparation Date: 31 December 2008

Version: 1.0

The TAS3 Consortium

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

Contributors

	Name	**Organisation**
1	Dr. Gang Zhao, Quentin Reul	VUB
2	Dongya Wu	VUB/CESI

Table of Contents

1 EXECUTIVE SUMMARY 5

2 INTRODUCTION 6

2.1 Document Scope and Objective 6
2.2 Document Structure 6

3 APPROACH 7

3.1 Assumptions 7
3.2 Ontology Engineering Methodology 8
3.3 Knowledge Resources 9
3.3.1 SUMO 9
3.3.2 ISO/IEC Standards on Information Security Systems 10
3.3.3 Privacy Issues 12

4 REQUIREMENTS 13

4.1 Scope of the Ontology 13
4.1.1 Themes 13
4.1.2 Domain of Application 14
4.2 Application of Ontologies 14
4.2.1 Information Retrieval 14
4.2.2 Interoperability 14
4.2.3 Constraint-based Decision Support 15
4.3 Semantics within TAS^3 System Architecture 15
4.4 In and Out 18

5 ONTOLOGY ARCHITECTURE 19

5.1 Building Blocks 19
5.2 Upper Ontology 20
5.2.1 Entity 20
5.2.2 Predicate 21
5.2.3 Descriptor 21
5.3 Rationale behind the Architecture 21

6 TOPICS 22

6.1 Stakeholders 22
6.2 Protected Assets 22
6.2.1 Sensitive Personal Data 22
6.2.2 Physical and Environmental Security 23
6.3 Security Activity 23
6.3.1 Security Actions 23
6.3.2 Information Security Event 23
6.3.3 Information Security Incident 24
6.4 Compliance 24
6.5 Trust 24
6.6 Security Technique 24
6.6.1 Cryptography 24

7 CONCEPTS AND RELATIONS 25

7.1 Security Activity 25
7.1.1 Risk Assessment 26
7.1.2 Risk Treatment 26

7.2 USER DATA PROTECTION 30
7.2.1 Data Controller 30
7.2.2 Personal Data 31
7.2.3 Other Concepts 31

8 CONCLUSION 32

9 REFERENCES 33

10 DOCUMENT CONTROL 34

Table of Figures

Figure 1: The ontological building blocks. 5
Figure 2: Agile ontology engineering methodology. 8
Figure 3: The SUMO Upper level. 9
Figure 4: Security concepts and their relationships. 10
Figure 5: PDCA model applied to ISMS processes. 11
Figure 6: Guaranteeing Cross-Context Semantic Interoperability. 16
Figure 7: A Typical TAS³ Process Flow. 17
Figure 8: TAS³ Architecture/Protocol Stack View. 17
Figure 9: The ontological building blocks. 19
Figure 10: The Upper Ontology. 20
Figure 11: The TAS³ Building Blocks. 22

1 Executive Summary

An ontology is commonly defined as: "*a [formal,] explicit specification of a [shared] conceptualization*" [1]. More specifically, an ontology explicitly defines a set of entities (e.g. classes, relations and individuals) imposing a structure on the domain that is readable by both humans and machines. An ontology must obey certain constraints. Firstly, the ontology should include a strict hierarchy. In other words, a class should be considered as a subclass of another if and only if the former has the same attributes as the superclass plus one or more attributes. Note that meronymy should not be included as part of this hierarchy. Secondly, the schema of the ontology (i.e. its terminology) must be separated from the actual data. Note the difference between classes and individuals is that the latter are explicit realisation of a class.

TAS3 Ontology consists of five building blocks of specification (Figure 1). Each block targets particular essential tasks of semantic modelling.

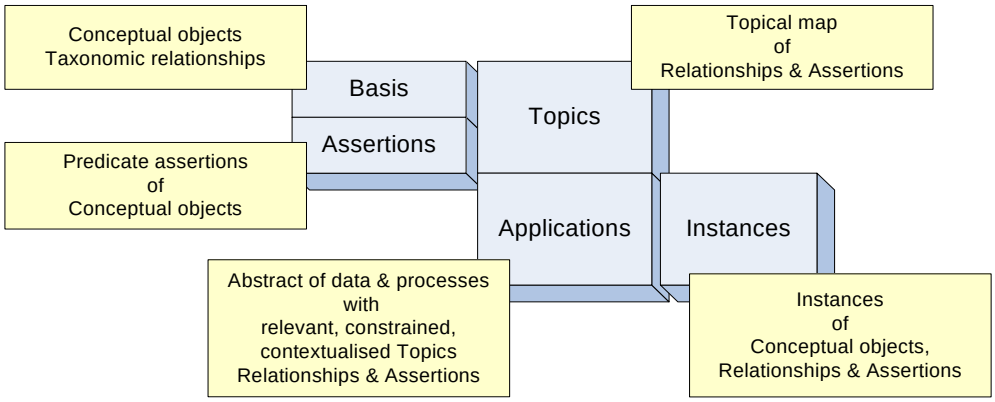

Figure 1: The ontological building blocks.

The *Basis* identifies conceptual objects and their typological relationship. The *Assertions* asserts about how the conceptual objects interact with each other. The *Topics* groups the relationships and assertions into a topical map of larger reusable units. The *Applications* selects, constrains and contextualises the topics, relationships and assertions to formulate abstracts about business data and processes in view of specific application semantics. The Instances lists concrete references or values about the conceptual objects, relationships and assertions.

2 Introduction

2.1 Document Scope and Objective

As part of this document, we describe the approach developed by STARLab to develop ontologies. Furthermore, we highlight the specific requirements for the TAS^3 project. We also demonstrate how our approach has been used to develop an Upper Ontology that would enhance reuse across different domain of application. Finally, we describe how this Upper Ontology can be used to define lexons relevant to different security standards.

2.2 Document Structure

The rest document is structured as follow:

- Section3 describes the approach taken to develop the ontology as part of the TAS^3 project. Furthermore, it provides a description of the different sources used.
- Section 4 presents the requirements of TAS3.
- Section 5 presents the Upper Ontology developed by STARLab.
- Section 6 describes the different topics.
- Section 7 lists the assertion extracted from different documents.
- Section 8 provides a conclusion of the current ontology.

3 Approach

This section presents the assumptions behind the approach used by STARLab. Furthermore, we introduce the methodology to develop ontologies proposed by STARLab. Finally, we describe the different knowledge sources used as part of this document.

3.1 Assumptions

STARLab's DOGMA (Developing Ontology-Grounded Methods and Applications) ontology framework is based on database semantics and model theory [2]. Its *double articulation* principle and grounding in *natural language representation of knowledge* makes DOGMA particularly fit for representing business-level as well as technical terminology and semantics typically found in business process models and their web service implementations respectively.

A DOGMA inspired ontology decomposes the ontology into a *lexon base* and a layer of reified ontological *commitments* [3]. The lexon base layer stores uninterpreted, extensive and reusable pool of elementary building blocks, called lexons, for constructing an ontology. A lexon represents a plausible binary fact-type and is formally described as a 5-tuple <*V, term1, role, co-role, term2*>, where *V* is an abstract context identifier (e.g. a piece of text or an image), which describes the context of the lexon and groups lexons that are logically related in the conceptualisation of the domain. Intuitively, a lexon within the context *V* can be read as: *term1* (also denoted as the *header term*) may have a relation with *term2* (also denoted as the *tail term*) in which it plays a *role*, and conversely, in which *term2* plays a corresponding *co-role*. Each (context, term)-pair then lexically identifies a unique concept. Although ontologies can differ in syntax, semantics, and pragmatics, they all are built on the shared vocabularies in the lexon base.

The commitment layer mediates between the lexon base and its applications. Each ontological commitment corresponds to an explicit instance of a (intentional) first order interpretation of a task in terms of the lexon base. It consists of a finite set of axioms that specify which lexons of the lexon base are interpreted and how they are visible in the committing application, and (domain) rules that semantically constrain this interpretation. An important difference with the underlying lexon base is that commitments are internally unambiguous and semantically consistent. Once elicited, ontological commitments (i.e. ontologies) are used by various applications such as information integration and mediation of heterogeneous sources.

The double articulation allows a distinct separation between the elicitation and the application of an ontology, which can be effectively exploited by an ontology engineer. The rationale is that experience shows that agreement on the domain rules is much harder to reach than on the conceptualization [4]. E.g., the rule stating that each car has exactly one license plate number may hold in the Universe of Discourse (UoD) of some application, but may be too strong in the UoD of another application.

Another fundamental DOGMA characteristic is its grounding in the linguistic representation of knowledge. This is exemplified most clearly in the linguistic nature of the lexons, with terms and role strings chosen from a given (natural) language, and that constitute the basis for all interfaces to the ontology. Linguistic "grounding" is achieved through elicitation contexts, which in DOGMA are just mappings from identifiers to source documents such as generalized glosses, often in natural language. A full formalisation of DOGMA can be found in De Leenheer, Meersman, and de Moor [5].

3.2 Ontology Engineering Methodology

DOGMA-MESS (Meaning Evolution Support System) is STARLab's methodology (and tool) to support inter-organizational ontology engineering [6]. The main focus in DOGMA-MESS is how to capture relevant inter-organizational commonalities and differences in meaning. It provides a community grounded methodology to address the issues of relevance and efficiency.

DOGMA-MESS is composed of two main steps: *semantic reconciliation* and *semantic application* (see Figure 2). The semantic reconciliation is composed of five phases. The user (or knowledge engineer) first elicitates the scope of the ontology by collecting abstract facts (e.g. logical schemas and natural language sentences). These facts are created and then formalized into lexons. Finally, redundant elements are removed. This first step results in a number of reusable language-neutral patterns for constructing semantics that are grounded in informal meaning descriptions.

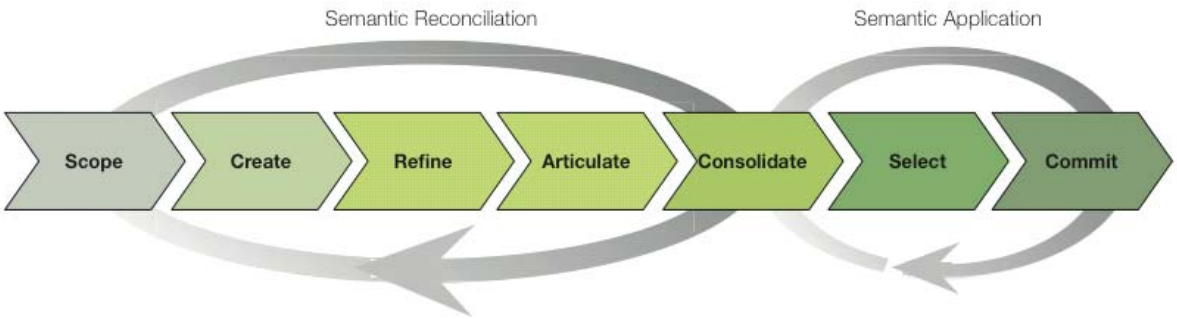

Figure 2: Agile ontology engineering methodology.

During the semantic application, existing information sources and services are committed to a selection of semantic patterns. This is achieved by selecting the appropriate patterns, constraining their interpretation and finally mapping (or committing) the selection on the existing data sources. In other words, a commitment creates a bidirectional link between the existing data sources and services and the business semantics that describe the information assets of an organization. The existing data itself is not moved.

In DOGMA-MESS, there are three user roles; (1) Knowledge Engineer, (2) Core Domain Expert and (3) Domain Expert. The task of the Knowledge Engineer is to assist the (Core) Domain Experts in their tasks. The major chunk of knowledge is captured by the Domain Experts themselves. The Core Domain Expert builds high-level templates in the so-called Upper Common Ontology. The Domain Experts specialize these templates to reflect the perspective of their organization in their Organizational Ontologies. The Domain Experts are shielded from complexity issues by assigning specific tasks in the elicitation process. In every version of the process, common semantics are captured in the Lower Common Ontology whilst organizational differences are kept in the Organizational Ontologies. Information in the Lower Common Ontology is distilled from both the Upper Common Ontology and the Organizational Ontologies using meaning negotiation between (Core) Domain Experts. The Lower Common Ontology is then used as input for future versions in the process. Initial user tests of DOGMA-MESS showed promising results in the first version of the methodology and the tool [7].

The importance of DOGMA-MESS is that (1) it allows the domain experts themselves to capture meaning, (2) relevant commonalities and differences are identified and (3) every version in the process results in a useable and accepted ontology.

3.3 Knowledge Resources

3.3.1 SUMO

The Suggested Upper Merged Ontology (SUMO) [8] is an upper level ontology developed by the Standard Upper Ontology Working Group, which covers fields such as engineering, philosophy, and information science. SUMO provides a terminology that acts as foundation for more specific domain ontologies (e.g. communication and people). Currently, it contains over 20,000 terms associated to definitional statements. SUMO was created by merging several publicly available ontologies into a comprehensive, and cohesive structure. This content included the ontologies available on the Ontolingua server, John Sowa's upper level ontology, the ontologies developed by ITBM-CNR, and various mereotopological theories, among other sources.

The diagram in Figure 3 represents the highest level concepts in SUMO and the relation between them. The root node is, as in many other ontologies (e.g. DOLCE[1]), ***Entity***, and this concept subsumes ***Physical*** and ***Abstract***. The former category includes everything that has a position in space/time, and the latter category includes everything else.

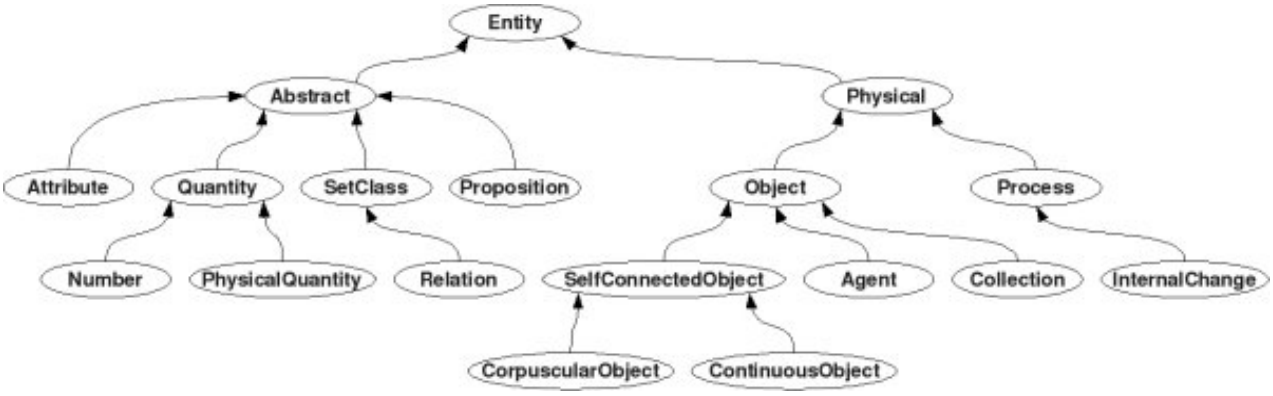

Figure 3: The SUMO Upper level.

Under the concept of ***Physical***, we have the disjoint concepts of ***Object*** and ***Process***. The existence and nature of the distinction between these two notions was subject to much debate. Those who adopt a 3D approach to model ontologies consider that objects are present at any moment of their existence, whereas processes do not. However, those who adopt a 4D approach do not make this distinction. SUMO has adopted the 3D approach, as its designer wanted to incorporate process-related related ontologies (e.g. PSL[2]) as well as mereotopologies. Immediately under the concept of ***Object***, there are several disjoints concepts including ***Collection***, ***SelfConnectedObject*** and ***Agent***. ***Collection*** refers to anything containing members that can be added or removed without changing the identity of the collection, while ***SelfConnectedObject*** covers any object that is not constituted of two or more disconnected parts. ***Agent*** represents something or someone that can act on its own and produce changes in the world. Under ***Process***, we find a several sub-concepts. For example, ***InternalChange*** refers to processes that involve the alteration of the internal property of an object. However, processes related to spatial or temporal location are not considered as instances of this class.

The class ***Abstract*** subsumes four concepts; namely ***SetClass***, ***Proposition***, ***Attribute***, and ***Quantity***. ***SetClass*** covers any instances of ***Abstract*** that contains elements or instances. ***Proposition*** refers to the notion of semantic or information content, while ***Attributes*** represents all qualities, properties that are not reified as ***Object***. For example, ***Men*** and ***Women*** are not found as sub-concepts of ***Person***, instead we create two instances (i.e. *Male* and *Female*) of ***BiologicalAttribute***. Finally, ***Quantity*** represents implied or explicit measurement system and is composed of ***Number*** and a particular unit of measure. For

[1] Descriptive Ontology for Linguistic and Cognitive Engineering (url: http://www.loacnr.it/DOLCE.html)
[2] http://www.mel.nist.gov/psl/

example, 1 meter and 39.37 inches are two instances of a same concept under ***PhysicalQuantity***.

3.3.2 ISO/IEC Standards on Information Security Systems

International Standards related to Information Security are developed by JTC1 (Joint Technical Committee 1), which is established by ISO (International Organization for Standardization) and IEC (International Electro-technical Commission). We refer to several ISs in this document.

ISO/IEC 15408 [9] is used as a specification for evaluating the security of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience. In this standard, general security concepts and relationships between them are proposed. Figure 4 shows how assets can be protected from threats by assessing the resulting effect of such abuse. Note that every type of threat should be considered, but in the domain of security the attention is given to those related to malicious or human activities.

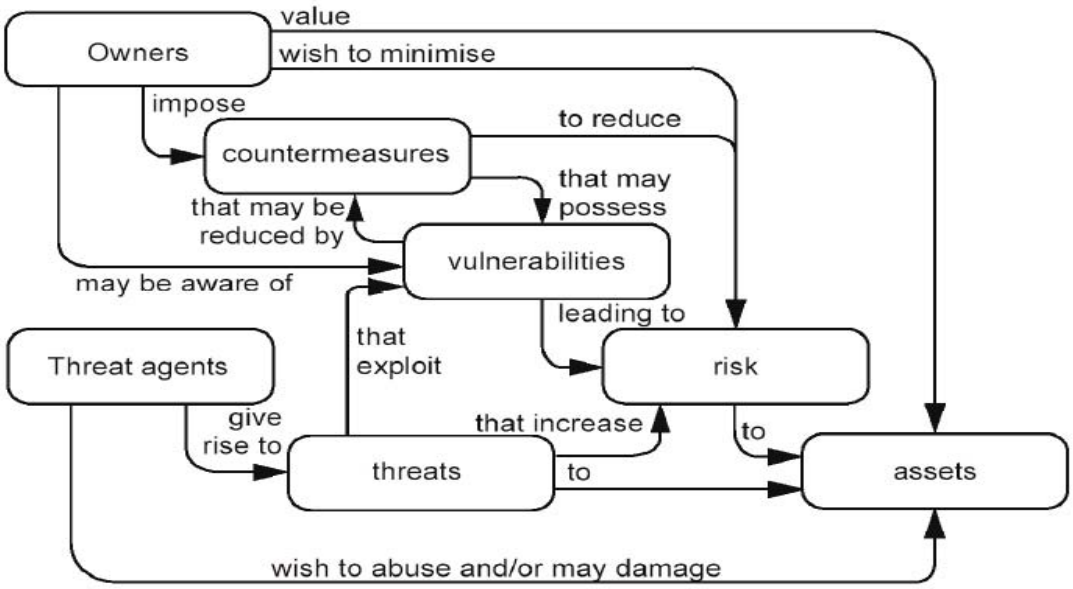

Figure 4: Security concepts and their relationships.

Safeguarding assets is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Owners perceive such threats as damaging with regard to the value of the assets. For example, the value of the asset could be reduced as a result of attacks, such as damaging disclosure of the asset to unauthorized recipients (loss of confidentiality), damage to the asset through unauthorized modification (loss of integrity), or unauthorized deprivation of access to the asset (loss of availability). The owners will analyse the threats applicable to their specific assets and their environment, determining the risks associated with them. This analysis can aid in the selection of countermeasures to counter the risks and reduce it to an acceptable level. Residual vulnerabilities may remain after the imposition of countermeasures. These vulnerabilities may be exploited by threat agents representing residual level of risk to the assets.

The ISO/IEC 17799 [10] establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The ISO/IEC 27001 [11] provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a process approach. The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

a. Understanding an organization's information security requirements and the need to establish policy and objectives for information security;

b. Implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;

c. Monitoring and reviewing the performance and effectiveness of the ISMS; and

d. Continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. Figure 5 illustrates how an ISMS takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

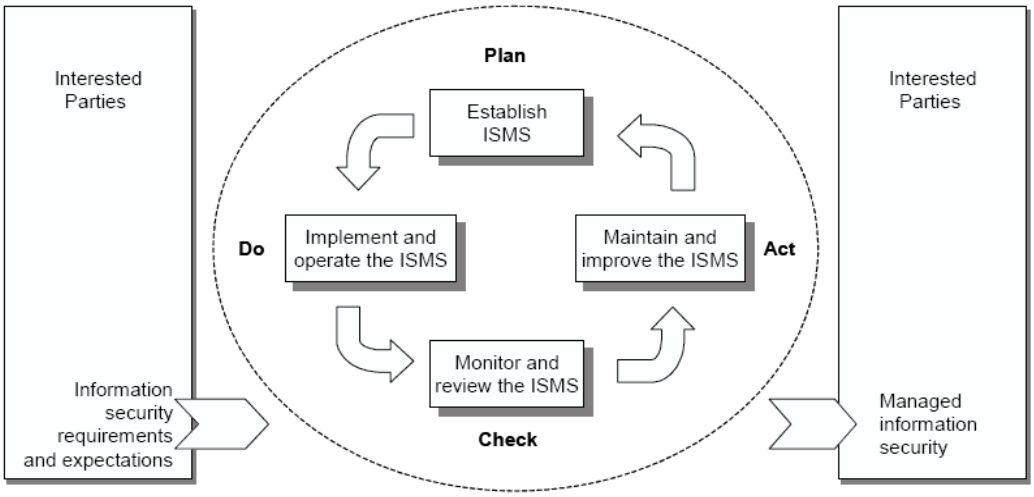

Figure 5: PDCA model applied to ISMS processes.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines [12] governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

3.3.3 Privacy Issues

There are three major documents that create the foundation of privacy in the EU:

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)[3]
- OECD Guidelines for the Security of Information Systems and Networks: TOWARDS A CULTURE OF SECURITY[4]
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.I.1981)[5]
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[6]

The UK and the Netherlands, the Member States focused on in the TAS3 architecture, have both implemented the EU Privacy Directive in national law.

- Data Protection Act 1998 CHAPTER 29[7]
- Personal Data Protection Act (Wet Bescherming Persoonsgegevens) 2001[8]

[3] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[4] http://www.oecd.org/dataoecd/16/22/15582260.pdf
[5] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[6] http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
[7] http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1
[8] http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml?refer=true&theme=purple

4 Requirements

4.1 Scope of the Ontology

The TAS3 project involves the regular collection, processing and exchange of large amount of data across organisations. In addition, the operations need to be carried with high levels of reliability and security.

This section seeks to clarify the conceptual of the ontology by answering two questions about its content:

- What are the subjects covered?
- Where are they used?

4.1.1 Themes

4.1.1.1 Policies

The polices under attention are rules and regulations concerning the use of IT resources. They are legislation and organisational policies about IT operations and IT policies about the configuration, development and operation of IT systems

The policies in the project of TAS3 is concerned with

- IT security system (approach, evaluation, auditing, etc.)
- Data security (creation, modification, usage, destruction with respect to the trust and identity of the participants)
- Authentication and identity management
- Authorisation over the use of IT system and data
- Trust (among participants in activities and over data, direct or migrated)
- Privacy

The semantic model of policies is a type of regulatory ontology, describing essential concepts and relationships in the regulation and standards for conformance.

4.1.1.2 Process

Since the security, trust and data protection are to be regulated in view of business processes and services, the semantics about the business process and work flows must be also covered to capture the semantics of input, output, operation and participant of the process, for process flow and dynamic process adoption.

4.1.1.3 Data

The TAS^3 is concerned with security controls on the data flow through the business process. The metadata specification of data consumed and produced in the process or services are necessary for defining business processes and specifying security policies. Since data are application and system specific, the metadata specification will be confined to the data in the use cases of employability and e-health in the project.

4.1.1.4 Overall Semantic Descriptive Framework

The overall semantic descriptive framework describes the approach of top-level conceptualisation of semantics for reference, organisation and methodology. It is detailed in other sections of this deliverable.

4.1.2 Domain of Application

As ontology can be created on different granularity and specifity, it is important to define the context in which the ontology is to be used. The project of TAS[3] involves two domains of use: employability and e-Health. Employability refers to the ability of a person to gain and maintain employement, while eHealth covers health care practices that are supported by electronic processes and communication. The application of ontologies is envisaged in the business process of the two application domains. This means the process ontology and data ontology may need to cover the parts particular to these domains. For example, the elaboration of the concepts of *Record* and *Competence*.

4.2 Application of Ontologies

This section describes the potential use of ontologies in computing science. We first describe how ontologies can enhance the performance of information retrieval. Secondly, we present different types of interoperability issues that can be resolved by them. Finally, we describe how ontologies can be used as part of decision systems.

4.2.1 Information Retrieval

The field of information retrieval [13] deals with the accurate and speedy access of information from large repositories (e.g. the web or the database of a specific organisation). More specifically, the goal of automatic retrieval strategies is to retrieve all documents relevant to the search of user while keeping the number of non-relevant one as low as possible. This is often achieved by indexing the information in such a way that its retrieval will be facilitated. For example, libraries often classify (i.e. index) books according to the Dewey Decimal Classification[9] (DDC). The DDC generally organises knowledge by subject, with extensions for subject relationships, places, etc. For example, 346.94 relates to private law in Europe.

As part of the Semantic Web [14], data (e.g. documents) is enriched by machine understandable annotations. These annotations provide semantics describing the content of information. For example, the concept ***Security*** will enable the retrieval of documents about security such as ISO/IEC 17799 [10] and ISO/IEC 27001 [11].

In TAS3, we envisage to use semantic markups to filter information by comparing the semantic similarity between information request and supply in the context of WP8. For example, given a job profile, retrieve a list of relevant candidates and finding the matching ones. This implies the semantic comparison of the job profile and candidate profiles based on an ontology of skills.

4.2.2 Interoperability

The IEEE [15] defined interoperability as: "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*." In other words, interoperability allows different organisations (both private and public) to exchange information and knowledge to reach a common goal. The European Union has founded the IDABC programme[10], which developed the European Interoperability Framework[11] (EIF). This framework describes policies and standards to be agreed by all organisations involved to promote interoperability. EIF proposes four types of interoperability; namely *semantic*, *technical*, *organisational*, and *legal* interoperability.

Semantic interoperability enables different systems to understand the intended meaning of the data being exchanged. Suppose two systems are exchanging data about a common user, then these systems should be able to recognise the user even if their internal representation is different. For example, a system could refer to the user by its name (e.g. Barak Hussein Obama), while another divide the name into first name (e.g. Barak), middle name (e.g. Hussein), and last name (e.g. Obama). Without an agreed semantic, the task of exchanging data in different format would require labour-intensive and time consuming manipulations to process the data.

---

[9] http://www.oclc.org/dewey/
[10] http://ec.europa.eu/idabc/en/home
[11] EIF, European Interoperability Framework for Pan-European eGovernment Services, 2004. http://europa.eu.int/idabc/en/document/3761

Technical interoperability considers technical issues related to linking computer systems and services. It includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services. For example, in TAS^3, we could augment a set of preconditions (i.e. input parameters) and a set of effect (i.e. output parameters) related to a web service with semantic markups (i.e. concepts in an ontology) to facilitate web service composition. This type of interoperability results in more reliable exchange and reduces the amount of maintenance compared to ad-hoc solutions.

Organisational interoperability is concerned with defining business goals and modelling business processes for the interaction between organisations. Furthermore, this type of interoperability aims at addressing the requirements of the user community by making services available, easily identifiable, accessible and user-oriented. Semantic markups can describe the relationships between activities and the role of their participants (e.g. actors, data) in a meaningful manner. As a result, processes and activities that would normally not be able to take place can be carried to reach a certain objective.

Finally, *legal (and political) interoperability* addresses the legal and political constraints on how the information is exchanged and used by the different organisations. These constraints include laws related to copyright, privacy, freedom of information, telecommunication regulation, and trade policies. For example, an activity (e.g. accessing data about someone health) might be legal in a certain context (e.g. a clinician requests the information) but not in another (e.g. a sale person requests the information).

4.2.3 Constraint-based Decision Support

The ontology can provide the common vocabulary for specifying/interpreting security constraints in the guard and policy enforcement points in the TAS3 architecture. At each security decision point, constraints expressed in semantic terms can be compared, overridden or rejected in generic terms.

4.3 Semantics within TAS^3 System Architecture

TAS^3 aims at producing an open and interoperable service oriented architecture, which provides an open source BPMS/SOA that allows adaptive processes while being able to maintain the needed trust and security. Thus, TAS^3 will provide a trust & security architecture that is ready to meet the requirements of complex and highly versatile business processes, the requirement of ensuring end-to-end secure transmission of personal information, the requirement of the transparent information transmission across the heterogeneous information systems. An essential element of this architecture is a community-managed ontology, which allows for unambiguous, but flexible, meaning agreement at all times. This ontology will bring together the elements of security, trust and semantics.

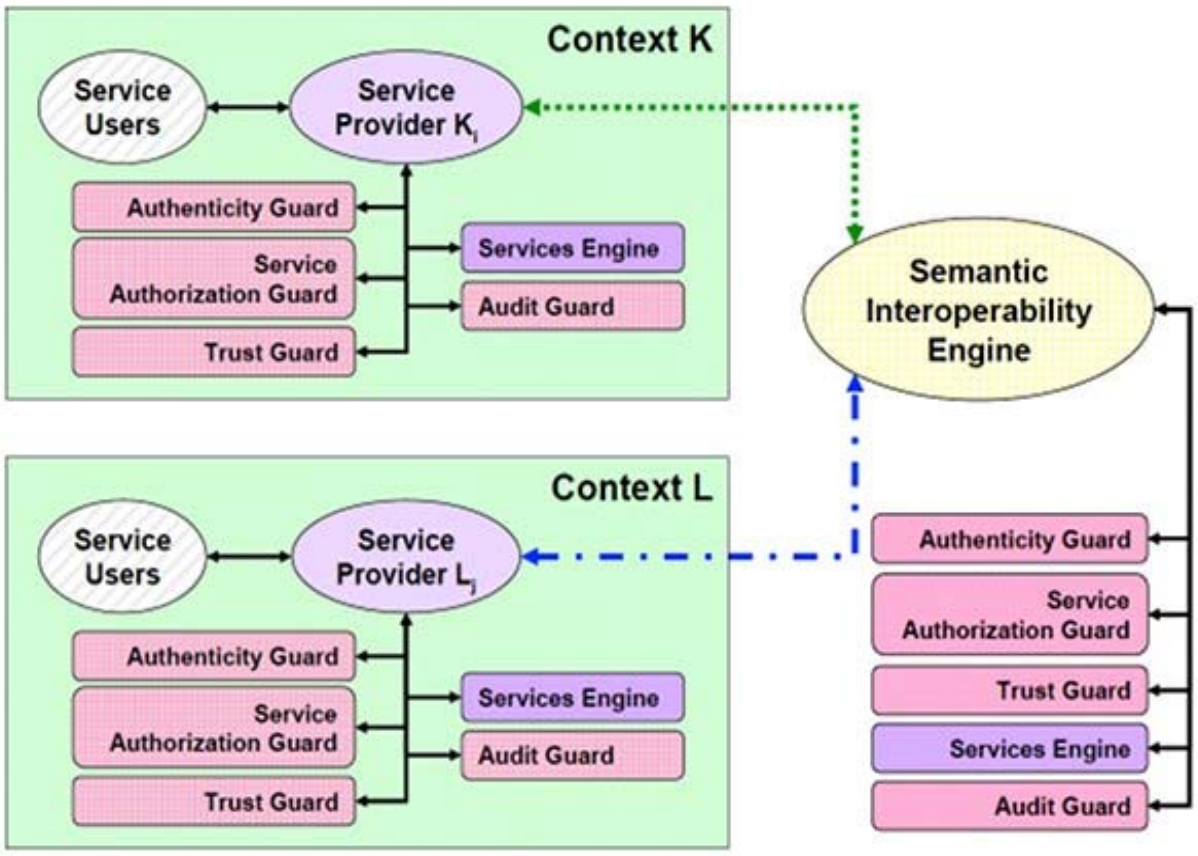

Figure 6: Guaranteeing Cross-Context Semantic Interoperability.

TAS[3] will maintain a consistent and integrated semantic approach while describing the features of the trust architecture. This description both functions as a machine-readable documentation of the architecture, and as the primary formal vehicle to exchange explicit semantic agreements (i.e. commitments) between partners and, eventually, systems. The integrated, co-evolved ontology will assure that relevant parts of the system commit to the same interpretation of possibly ambiguous elements to allow for meaning alignment, certification and early conflict discovery. This ontology will enable improved understanding; common methods of expressing terms enabling people and organisations to better trust each other in these application environments. TAS3 will integrate these architecture elements into a fully embedded trust framework to automate business processes managing personal information, which will result in considerable societal benefits.

Figure 7 is a typical TAS[3] process flow from the Business view. This figure describes the process by which a service requester requests a service from a service provider. The actual nature of the service and how they find one another does not really matter.

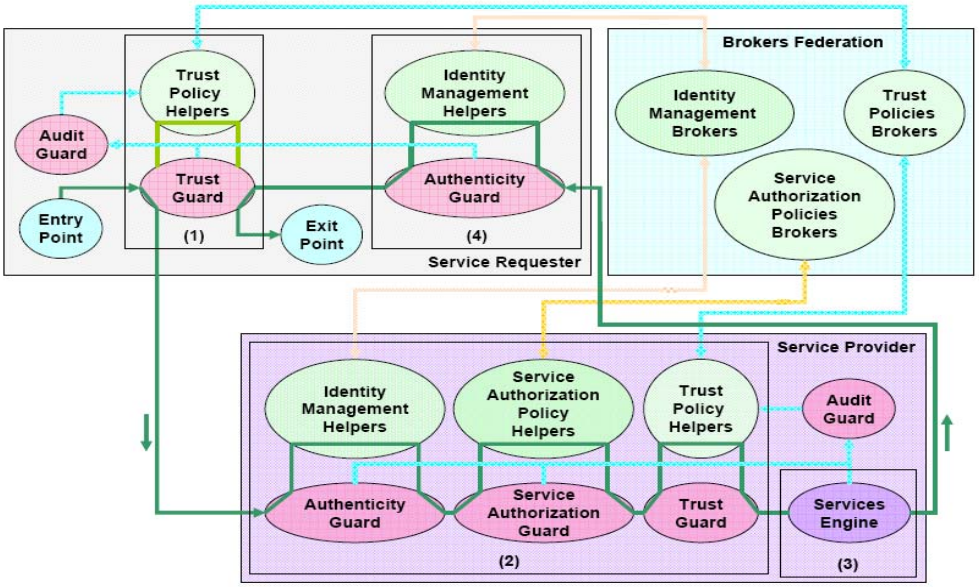

Figure 7: A Typical TAS³ Process Flow.

From the view of information security, a general security concepts and relationships can be described in Figure 4, Security is concerned with the protection of assets from threats, where threats are categorized as the potential for abuse of protected assets. All categories of threats should be considered; but in the domain of security greater attention is given to those threats that are related to malicious or other human activities.

From the view of information system, TAS3 should be an information infrastructure, which enables to acquire, describe, process, storage, and transport personal data in a secure way. Figure 8 describes an abstract TAS3 protocol stack, which ensures to transport personal data securely.

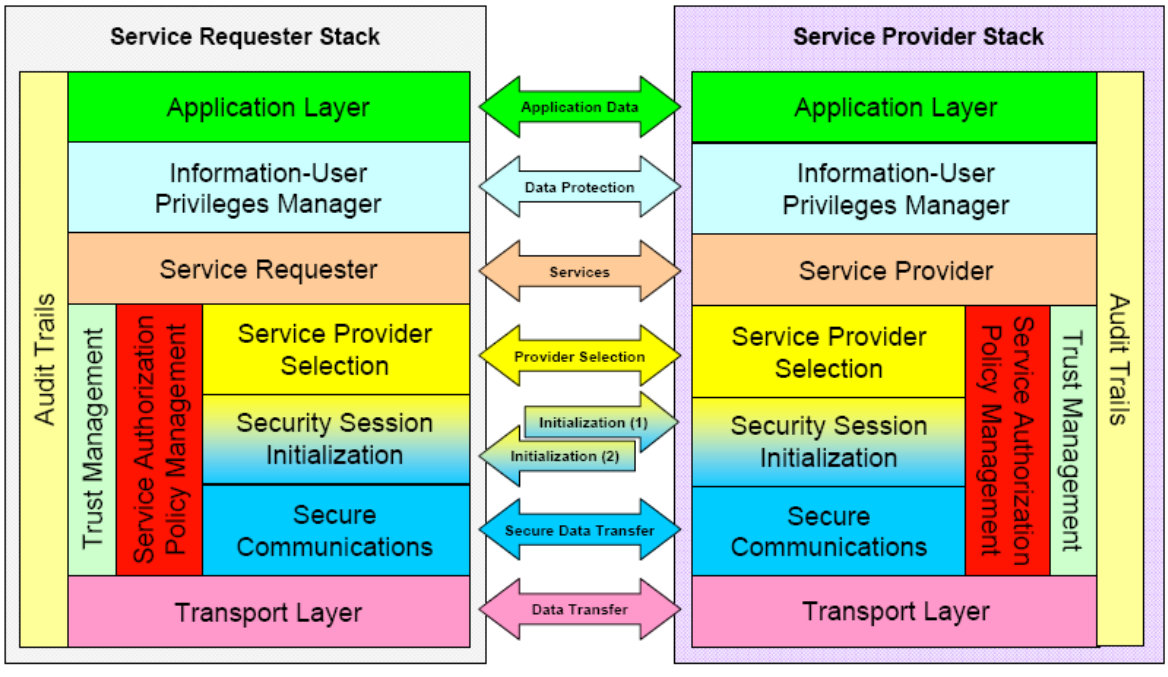

Figure 8: TAS³ Architecture/Protocol Stack View.

4.4 In and Out

Description	In	Out
1. Security		
2. Trust		
3. Policies		

5 Ontology Architecture

The Semantic Web has been envisioned to allow people and machine to share the meaning of data and ultimately of applications. The main goal is to capture data and application semantics in ontologies and map these ontologies via related concepts. As part of this section, we describe the ontology architecture developed by STARLab for the TAS[3] project.

5.1 Building Blocks

The architecture of TAS3 Ontology consists of five building blocks of semantic specification (Figure 9). The Ontological Basis and Ontological Assertions consist of conceptual *objects* and relations in the form of lexons. The Basis consists of objects related to each other in a hierarchical manner, such sub classes, compositions. The Assertions links these objects by factual predicates, for example, *overtake, produce*. They are layered on each other, with the latter uses objects defined in the former.

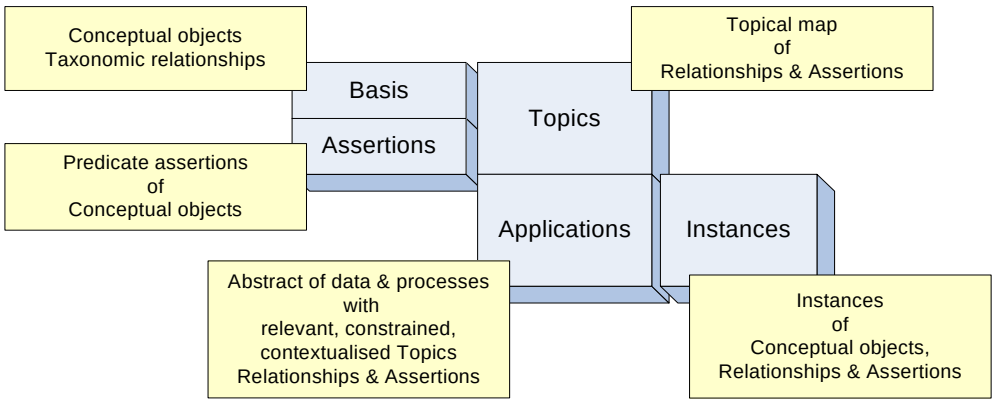

Figure 9: The ontological building blocks.

The Ontological Topics block defines *groups* of lexons from the Basis and Assertions by a particular topic or theme. The topic is the mechanism to identify a unit of lexons for regular or common semantic patterns or frameworks for rapid semantic modelling and reuse. If lexons are grouped by subject matters, ontologies of economics, stock exchanges are examples.

The Ontological Application block describes application-specific semantic entities and statements in terms of the Basis and Assertions grouped by topics. Here the generic ontological terms and relations are *constrained* in application-specific considerations. The denotation of terms and relations of one topic are *refined* by the terms and relations from another topic. For example, competences in the Workplace Individual Competence Ontology are set in the context of the business process ontology.

The Ontological Instances block is a dictionary of instances or *instantiations* of the concepts (business objects, domain topics, ontological assertions) with reference to specific reality. It substantiates or defines the reference of a semantic term.

The Basis, Assertions and Topics are the layer of semantic resources generic and reusable over different applications. The Applications and Instances pertain to application specific semantics, with instantiated and contextualised terms and relations from the Basis, Assertions and Topics.

5.2 Upper Ontology

One approach for mapping disparate ontologies is to use a standard upper ontology. An upper ontology is defined as a high-level, domain-independent ontology providing a framework to describe common sense concepts and from which more domain-specific ontologies can be derived [16]. Many upper ontologies (e.g. SUMO, DOLCE) have been proposed over the last decade. However, these have often been criticised as they couldn't be used in every domain. Nevertheless, we thought that SUMO could be a good basis. Figure 10 describes the upper ontology developed by STARLab representing our basic understanding of the world. In TAS3, the upper ontology will enable the interoperability between the two domains of application (i.e. employability and eHealth) by creating specific ontologies "under" this upper ontology.

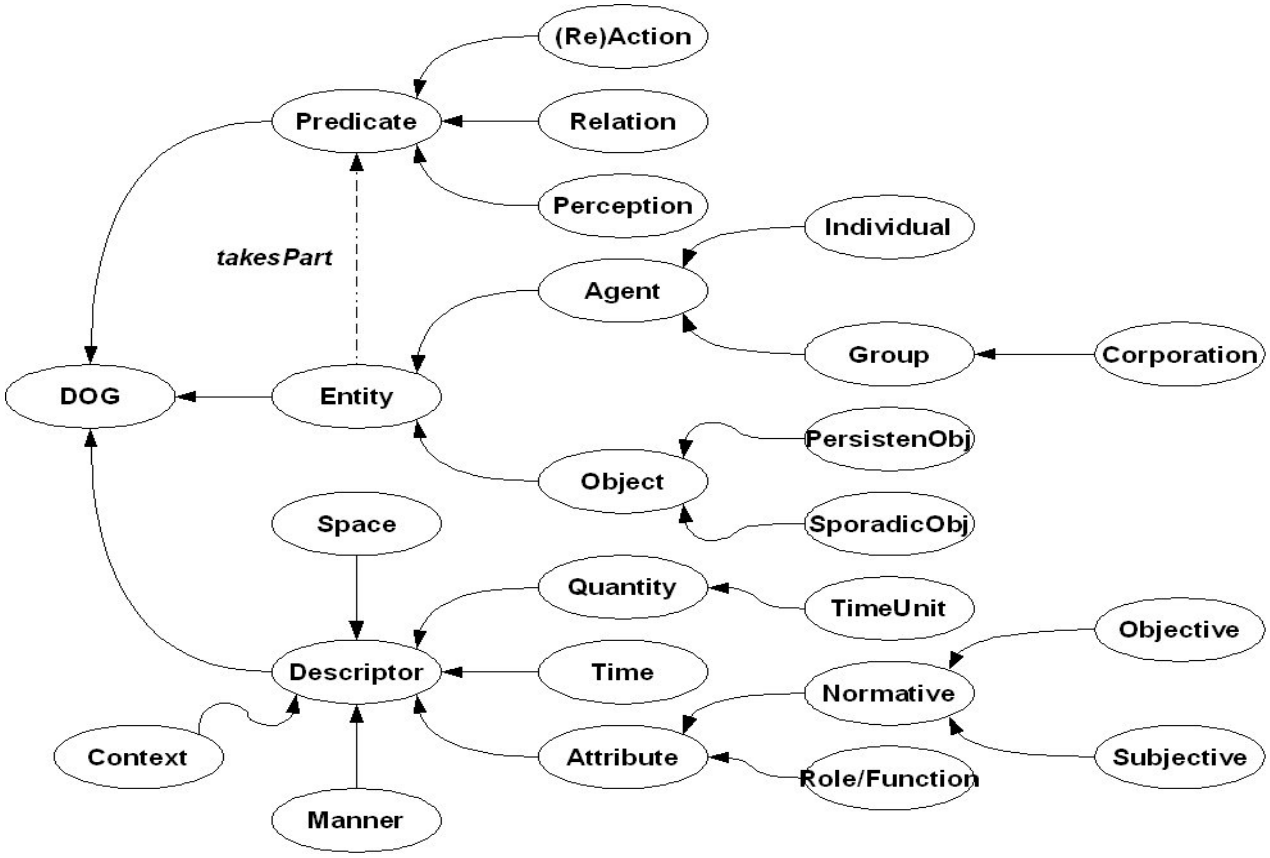

Figure 10: The Upper Ontology.

Our main assumption is that the world (or ***DOG***) contains three main concepts, namely ***Entity, Predicate***, and ***Descriptor***, whereas SUMO suggests that the main concept (i.e. ***Entity***) subsumes ***Physical*** and ***Abstract*** concepts. In our upper ontology, an ***Entity*** represents anything that can take part into an action or that can be acted upon. A ***Predicate*** denotes a verb which affirms or denies information about the subject, while a ***Descriptor*** categorises or describes either an ***Entity*** or a ***Predicate***. It is important to note that ***Descriptor*** encompasses a lot of the elements described under ***Abstract*** in SUMO (Figure 3). Similarly, ***Entity*** (Figure 10) represents concepts listed under ***Object*** in SUMO. The following sections describe the lower level of the ontology in more details.

5.2.1 Entity

An ***Entity*** is a thing with distinct and independent existence. An ***Agent*** is a person or thing that takes an active role or produces a specified effect. An ***Individual*** is a person, while a ***Group*** is a number of people or things located, gathered, or classed together. A more specific type of ***Group*** is a ***Corporation***, which is a large company or group of companies authorized to act as a single entity and recognized as such in law. An ***Object*** is a thing to which an action or feeling is directed. A ***PersistentObject*** is a continuing or recurring; prolonged object, while a ***SporadicObject*** is an object that occurs at irregular intervals or only in a few places.

5.2.2 Predicate

An ***Predicate*** represents anything that is happening or being done in time. We have also identified three types of activity; namely *(re)action*, *relation* and *perception*. ***Action*** is the process of doing something to achieve an objective, while ***Reaction*** is an instance of reacting to or against something. For example, a transaction is a type of ***Action***, where an exchange is taking place between two entities. ***Relation*** is the way in which two or more entities are connected or related. ***Perception*** is the ability to see, hear, or become aware of something through the senses.

5.2.3 Descriptor

A ***Descriptor*** is something that is used to identify an object or an agent. ***Quantity*** is a descriptor that is measurable in number, amount, size, or weight. ***Time*** is the measure associated with time (e.g. minute, hour). ***Context*** is the circumstances that form the setting for an event, statement, or idea. ***Temporal*** is a portion of time characterized by particular events or circumstances. ***Spatial*** is a context pertaining to or involving or having the nature of space. ***Manner*** is the way in which something is done or happens. ***Attribute*** is a characteristic or inherent quality or feature. ***Role*** is a person's or thing's function in a particular situation. ***Function*** is an activity that is natural to or the purpose of a person or thing.

5.3 Rationale behind the Architecture

Upper ontologies are intended to define foundational concepts used in both mid-level and domain ontologies. In theory, the mapping between domain ontologies becomes easier if the ontologies to be mapped are derived from a standard upper ontology. Two approaches exist for the use of upper ontologies: top-down and bottom-up. In a top-down approach one uses the upper ontology as the foundation for deriving concepts in the domain ontology. In this way, the domain ontology designer takes advantage of the knowledge and experience already built into the upper ontology. Furthermore, use of the upper ontology provides a theoretical framework on which to build. In a bottom-up approach, the ontology designer maps new or existing domain ontology to the upper ontology. This approach also capitalizes on the knowledge built into the upper ontology but one would expect the mapping to be more challenging, as inconsistencies may exist between the domain and upper ontology.

6 Topics

The concept of *Topics* is used to architect ontologies by particular themes or applications. It serves a mechanism to define components of ontology by their reference and usage [2]. Each topic consists of a subset of lexons from the Basis and Assertion building blocks of the ontology. We identify key topics of the TAS^3 ontology through ISO/IEC standards on information system security, OECD and EU data protection guidelines. The idea is another ontological layer of refinement from the upper ontology. It is devoted to the themes of security, data protection and trust in general without but subsumes the specifics of the TAS^3 architecture and test cases.

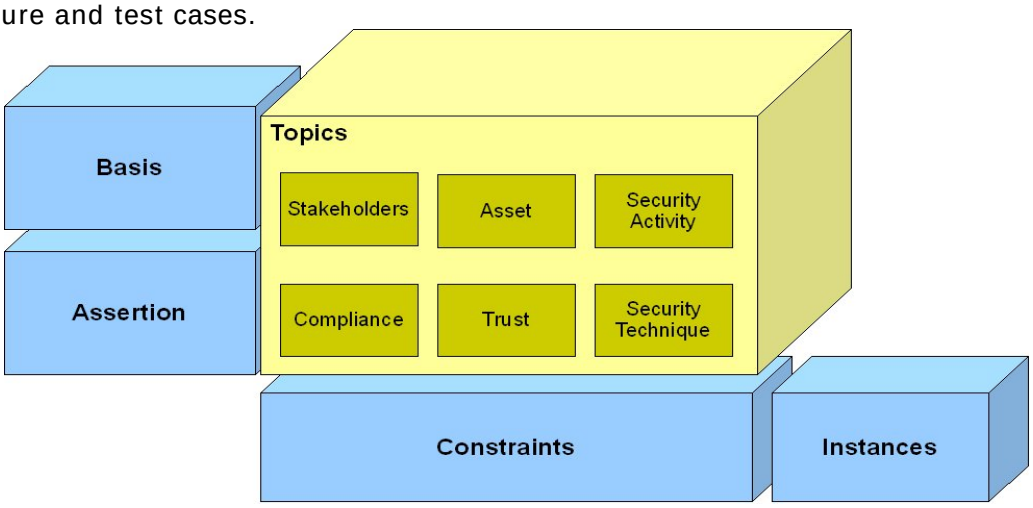

Figure 11: The TAS^3 Building Blocks.

This section describes a map of topics to capture the semantic terrain of security, data protection and trust issues.

6.1 Stakeholders

Stakeholders are actors in the security scenarios, impacting or impacted on the security state or conditions. They are Data Owner, DataSubject, ThreatAgent, RiskAssessor, AssetController. They are subtype of Agent in the upper ontology.

6.2 Protected Assets

Asset means anything that has value to the organization [17]. The term "*owner*" identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term owner does not mean that the person actually has any property rights to the asset [11].

6.2.1 Sensitive Personal Data

Personal Data is the information that relates to a living and identifiable individual [18]. Private data is information, called *sensitive personal data*, about a specific individual that this individual does not want to be revealed. Sensitive personal data includes information about racial or ethnic origin, physical or mental health or conditions, sexual preference, political opinions, religious or similar belief, alleged commission of any offence or proceedings relating to offences.

In the employability domain, sensitive personal data covers any type of information such as religion, sexual orientation, political affiliation that could lead to a prospective employer discriminating an individual.

In eHealth, a person may not wish to have their medical records to be available. This may be because they would not wish for others to know about medical or psychological conditions or treatments which would be embarrassing. Revealing medical data could also reveal other details about one's personal life (such as about one's sexual activity for example).

6.2.2 Physical and Environmental Security

6.2.2.1 Secure Area

The objective of secure area is to prevent unauthorized physical access, damage and interference to the organization's premises and information [11].

6.2.2.2 Equipment Security

The objective of equipment security is to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities [11].

6.3 Security Activity

6.3.1 Security Actions

Security activity describes the action related to security issues of information system. It is concerned with how to establish, implement, operate, monitor, review and improve a Security Information System. Its description is largely based on ISO/IEC 15408.

6.3.1.1 Security Audit

Security audit includes information about security alarm, audit analysis, audit review and audit storage.

6.3.1.2 Risk Assessment

Risk assessment is the overall process of risk analysis and risk evaluation [17], while risk analysis seeks to identify potential risks involved in an IT operation. Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of the risk [18, 11].

6.3.1.3 Risk Treatment

Risk treatment is the process of selection and implementation of measures to modify risk [17].

6.3.1.4 Data Protection

IT systems need to implement several mechanisms to avoid any breach of sensitive personal data. Furthermore, these systems need to store the information in such as way that this information is available at an individual's request.

6.3.1.5 Access Control

The objective of the user access management is to ensure authorized user access and to prevent unauthorized access to information systems [11].

The objective of controlling network access is to prevent unauthorized access to networked services such as user authentication, equipment identification, port protection, network segregation, network connection control.

The objective of operating system access control is to prevent unauthorized access to operating systems such as secure log-on procedures, user identification and authentication, password management, use of system utilities, session time-out, and limitation of connection time.

The objective of application and information access control is to prevent unauthorized access to information held in application systems [11], such as access restriction, sensitive system isolation.

6.3.2 Information Security Event

Information security event means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [19].

6.3.3 Information Security Incident

Information security incident means a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [19].

6.4 Compliance

The objective of ensuring compliance with legal requirements is to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements [11], while the objective of security policies and standards, and technical compliance is to ensure compliance of systems with organizational security policies and standards.

6.5 Trust

In the service-oriented environment, business entities or agents can require or inquire information about a third party. As these communication can be (semi)anonymous, the quality of the information received is a huge consideration. Therefore, trust is an essential element in making sure that the services are used by people. Trust enablers are means to inspire or create trust, for example, proof origin and receipt on the issue of communication proof. In order to measure this notion of trust, trustworthiness must be calculated and provided to the user. Although trustworthiness can be transmitted through trusted paths, trusting an agent does not necessarily mean the opposite.

6.6 Security Technique

6.6.1 Cryptography

Cryptography is the practice and study of hiding information.

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others.

A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The *public key* is typically used for encryption, while the *private* or *secret key* is used for decryption.

7 Concepts and Relations

7.1 Security Activity

Security activity describes the action related to security issues of information system. It is concerned with how to establish, implement, operate, monitor, review and improve a Security Information System. It is largely based on ISO/IEC 15408 [9], ISO/IEC27001 [11] and ISO/IEC 17799 [10].

Context	Term1	Role	Co-role	Term2
	Action	subsume	subtypeOf	SecurityActivity
ISO/IEC 27001 Clause 4.2.1	SecurityActivity	subsume	subtypeOf	EstablishSecuritySystem
ISO/IEC 27001 Clause 4.2.2	SecurityActivity	subsume	subtypeOf	ImplementSecuritySystem
ISO/IEC 27001 Clause 4.2.2	SecurityActivity	subsume	subtypeOf	OperateSecuritySystem
ISO/IEC 27001 Clause 4.2.3	SecurityActivity	subsume	subtypeOf	MonitorSecuritySystem
ISO/IEC 27001 Clause 4.2.3	SecurityActivity	subsume	subtypeOf	ReviewSecuritySystem
ISO/IEC 27001 Clause 4.3	SecurityActivity	subsume	subtypeOf	MaintainSecuritySystem
ISO/IEC 27001 Clause 4.3	SecurityActivity	subsume	subtypeOf	ImprovementSecuritySystem
	SecurityActivity	subsume	subtypeOf	ThreatSecuritySystem
	ReviewSecuritySystem	subsume	subtypeOf	SecurityAudit
ISO/IEC 27001 Clause 4.3 d),e)	EstablishSecuritySystem	subsume	subtypeOf	RiskAssessment
ISO/IEC 27001 Clause 4.3 f),g)	EstablishSecuritySystem	subsume	subtypeOf	RiskTreatment
	ThreatSecuritySystem	subsume	subtypeOf	SecurityEvent
	ThreatSecuritySystem	subsume	subtypeOf	SecurityIncident
	ImplementSecuritySystem	subsume	subtypeOf	EstablishSecurityPolicy
	SecurityActivity	comprise	isComprised	Function
	Function	follow	precede	Function
	Agent	perform		Function
	Agent	assignedBy		Organization

7.1.1 Risk Assessment

Context	Term1	Role	Co-role	Term2
ISO/IEC 27001 Clause 4.3 d)	RiskAssessment	comprise	isComprised	RiskIdentification
ISO/IEC 27001 Clause 4.3 d),e)	RiskAssessment	comprise	isComprised	RiskAnalysis
ISO/IEC 27001 Clause 4.3 d),e)	RiskAssessment	comprise	isComprised	RiskEvaluation
	Agent	subsume	subtypeOf	RiskAssessor
ISO/IEC 27001 Clause 4.3 d)	RiskAssessor	identify		Asset
ISO/IEC 27001 Clause 4.3 d)	RiskAssessor	identify		Owner
ISO/IEC 27001 Clause 4.3 d)	RiskAssessor	identify		Vulnerability
		subsume	subtypeOf	Threat
ISO/IEC 27001 Clause 4.3 d)	Threat	impact		Confidentiality
ISO/IEC 27001 Clause 4.3 d)	Threat	impact		Integrity
ISO/IEC 27001 Clause 4.3 d)	Threat	impact		Availability
ISO/IEC 27001 Clause 4.3 e)	RiskAssessor	estimate		RiskLevel
ISO/IEC 27001 Clause 4.3 e)	RiskAssessor	compareTo		RiskCriteria
ISO/IEC 27001 Clause 4.3 e)	RiskAssessor	determine		RiskTreatment
	RiskAssessor	assess		Risk

7.1.2 Risk Treatment

Context	Term1	Role	Co-role	Term2
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	comprise	isComprised	IdentifyTreatment
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	comprise	isComprised	AcceptRisk
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	comprise	isComprised	AvoidRisk
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	comprise	isComprised	TransferRisk
ISO/IEC 27001 Clause 4.3 g)	RiskTreatment	comprise	isComprised	SelectControlObjective
ISO/IEC 27001 Clause 4.3 g)	RiskTreatment	subsume	subtypeOf	SelectCtrl
ISO/IEC 27001 Clause 4.3 f)	Agent	identify		Treatment
ISO/IEC 27001 Clause 4.3 f)	Agent	accept		Risk
ISO/IEC 27001 Clause 4.3 f)	Agent	avoid		Risk
ISO/IEC 27001 Clause 4.3 f)	Agent	transfer		Risk
ISO/IEC 27001 Clause 4.3 g)	Agent	select	isSelected	ControlObjective
		subsume	subtypeOf	Control
ISO/IEC 27001 Clause 4.3 g)	Agent	select	isSelected	Control
ISO/IEC 27001 Clause 4.3 g)	Agent	Perform		Control
ISO/IEC 27001 Annex A.5	Control	subsume	subtypeOf	SecurityPolicyCtrl
ISO/IEC 27001 Annex A.5.1.1	SecurityPolicyCtrl	comprise	isComprised	SecurityPolicyDocument
ISO/IEC 27001 Annex A.5.1.2	SecurityPolicyCtrl	comprise	isComprised	SecurityPolicyReview
ISO/IEC 27001 Annex A.5.1.1	Agent	document		SecurityPolicy
ISO/IEC 27001 Annex A.5.1.2	Agent	document		SecurityPolicy
ISO/IEC 27001 Annex A.6	Control	subsume	subtypeOf	OrganizationSecurityCtrl
ISO/IEC 27001 Annex A.6.1	OrganizationSecurityCtrl	subsume	subtypeOf	InternalOrgSecurityCtrl

ISO/IEC 27001 Annex A.6.2	OrganizationSecurityCtrl	subsume	subtypeOf	ExternalPartiesSecurityCtrl
ISO/IEC 27001 Annex A.6.1	Agent	control		InternalOrganizaionSecurity
ISO/IEC 27001 Annex A.6.2	Agent	control		ExternalPartiesSecurity
ISO/IEC 27001 Annex A.7	Control	subsume	subtypeOf	AssetManagement
ISO/IEC 27001 Annex A.7.1	AssetManagement	comprise	isComprised	ResponsibilityAssetMgt
ISO/IEC 27001 Annex A.7.2	AssetManagement	comprise	isComprised	InformationClassification
ISO/IEC 27001 Annex A.7.1	Agent	clarify		ResponsibilityAssess
ISO/IEC 27001 Annex A.7.2	Agent	classify		Information
ISO/IEC 27001 Annex A.8	Control	subsume	subtypeOf	HumanResouceSecurity
ISO/IEC 27001 Annex A.8.1	HumanResouceSecurity	comprise	isComprised	PriorEmploymentSecurity
ISO/IEC 27001 Annex A.8.2	HumanResouceSecurity	comprise	isComprised	DuringEmploymentSecurity
ISO/IEC 27001 Annex A.8.3	HumanResouceSecurity	comprise	isComprised	TerminationEmplSecurity
	ensure	subsume	subtypeOf	ensureSecure
ISO/IEC 27001 Annex A.8.1	Agent	ensureSecure		PriorEmployment
ISO/IEC 27001 Annex A.8.2	Agent	ensureSecure		DuringEmploymen
ISO/IEC 27001 Annex A.8.3	Agent	ensureSecure		TerminationEmployment
ISO/IEC 27001 Annex A.9	Control	subsume	subtypeOf	PhysicalEnvironmentSec
ISO/IEC 27001 Annex A.9.1	PhysicalEnvironmentSec	comprise	isComprised	SecureAreas
ISO/IEC 27001 Annex A.9.2	PhysicalEnvironmentSec	comprise	isComprised	EquipmentSecurity
ISO/IEC 27001 Annex A.9.1	Agent	ensureSecure		Area
ISO/IEC 27001 Annex A.9.2	Agent	ensureSecure		Equipment
ISO/IEC 27001 Annex A.10	Control	subsume	subtypeOf	CommunicationOpMgt
ISO/IEC 27001 Annex A.10.1	CommunicationOpMgt	comprise	isComprised	OperationalProcedureResponsibilityMgt
ISO/IEC 27001 Annex A.10.2	CommunicationOpMgt	comprise	isComprised	ThirdPartyServiceDeliveryMgt
ISO/IEC 27001 Annex A.10.3	CommunicationOpMgt	comprise	isComprised	SystemPlanningAcceptance
ISO/IEC 27001 Annex A.10.4	CommunicationOpMgt	comprise	isComprised	ProtectionAgainstMaliciousMobileCode
ISO/IEC 27001 Annex A.10.5	CommunicationOpMgt	comprise	isComprised	Backup
ISO/IEC 27001 Annex A.10.6	CommunicationOpMgt	comprise	isComprised	NetworkSecurityMgt
ISO/IEC 27001 Annex A.10.7	CommunicationOpMgt	comprise	isComprised	MediaHandlingMgt
ISO/IEC 27001 Annex A.10.8	CommunicationOpMgt	comprise	isComprised	ExchangeInformationMgt
ISO/IEC 27001 Annex A.10.9	CommunicationOpMgt	comprise	isComprised	E_CommerceSecurity
ISO/IEC 27001 Annex A.10.10	CommunicationOpMgt	comprise	isComprised	MonitoringInformation
ISO/IEC 27001 Annex A.10.1	Agent	clarify		OperationProcedureResponsibility
ISO/IEC 27001 Annex A.10.2	Agent	ensureSecure		ThirdPartyServiceDelivery
ISO/IEC 27001 Annex A.10.3	Agent	perform		SystemPlanningAcceptance
ISO/IEC 27001 Annex A.10.4	Agent	against		MaliciousMobileCode
ISO/IEC 27001 Annex A.10.5	Agent	perform		Backup
ISO/IEC 27001 Annex A.10.6	Agent	ensure		NetworkSecurity

ISO/IEC 27001 Annex A.10.7	Agent	ensure		MediaHandling
ISO/IEC 27001 Annex A.10.8	Agent	ensure		ExchangeInformation
ISO/IEC 27001 Annex A.10.9	Agent	ensure		E_Commerce
ISO/IEC 27001 Annex A.10.10	Agent	monitor		Information
ISO/IEC 27001 Annex A.11	Control	subsume	subtypeOf	AccessControl
ISO/IEC 27001 Annex A.11.1	AccessControl	comprise	isComprised	ClarifyAccessControlPolicy
ISO/IEC 27001 Annex A.11.2	AccessControl	comprise		UserAccessMgt
ISO/IEC 27001 Annex A.11.3	AccessControl	comprise	isComprised	ClarifyUserResponsibilities
ISO/IEC 27001 Annex A.11.4	AccessControl	comprise	isComprised	NetworkAccessCtrl
ISO/IEC 27001 Annex A.11.5	AccessControl	comprise	isComprised	OperatingSystemAccessCtrl
ISO/IEC 27001 Annex A.11.6	AccessControl	comprise	isComprised	ApplicationInfoAccessCtrl
ISO/IEC 27001 Annex A.11.7	AccessControl	comprise	isComprised	MobileCompTeleworking
ISO/IEC 27001 Annex A.11.1	Agent	clarify		AccessControlPolicy
ISO/IEC 27001 Annex A.11.2	Agent	manage		UserAccess
ISO/IEC 27001 Annex A.11.3	Agent	clarify		UserResponsibilities
ISO/IEC 27001 Annex A.11.4	Agent	manage		NetworkAccess
ISO/IEC 27001 Annex A.11.5	Agent	manage		OperatingSystemAccess
ISO/IEC 27001 Annex A.11.6	Agent	manage		ApplicationInfoAccess
ISO/IEC 27001 Annex A.11.7	Agent	ensureSecure		MobileCompTeleworking
ISO/IEC 27001 Annex A.12	Control	subsume	subtypeOf	InfoSysAcquistionDvtMain
ISO/IEC 27001 Annex A.12.1	InfoSysAcquistionDvtMain	comprise	isComprised	ClarifyInformationSystemSecurityRequirements
ISO/IEC 27001 Annex A.12.2	InfoSysAcquistionDvtMain	comprise	isComprised	ApplicationCorrectProcess
ISO/IEC 27001 Annex A.12.3	InfoSysAcquistionDvtMain	comprise	isComprised	CryptographicCtrl
ISO/IEC 27001 Annex A.12.4	InfoSysAcquistionDvtMain	comprise	isComprised	SystemFilesSecurity
ISO/IEC 27001 Annex A.12.5	InfoSysAcquistionDvtMain	comprise	isComprised	DvtSupportProcessSecurity
ISO/IEC 27001 Annex A.12.6	InfoSysAcquistionDvtMain	comprise	isComprised	TechnicalVulnerabilityMgt
ISO/IEC 27001 Annex A.12.1	Agent	clarify		InformationSystemSecurityRequirements
ISO/IEC 27001 Annex A.12.2	Agent	ensure		ApplicaionProcess
ISO/IEC 27001 Annex A.12.3	Agent	adopt		Cryptography
ISO/IEC 27001 Annex A.12.4	Agent	ensureSecure		SystemFiles
ISO/IEC 27001 Annex A.12.5	Agent	ensureSecure		DvtSupportProcess
ISO/IEC 27001 Annex A.12.6	Agent	manage		TechnicalVulnerability
ISO/IEC 27001 Annex A.13	Control	subsume	subtypeOf	SecurityIncidentMgt
ISO/IEC 27001 Annex A.13.1	SecurityIncidentMgt	comprise	isComprised	EventWeaknessesReport
ISO/IEC 27001 Annex A.13.2	SecurityIncidentMgt	comprise	isComprised	IncidentImprovementMgt
ISO/IEC 27001 Annex A.13.1	Agent	report		EventWeakness
ISO/IEC 27001 Annex A.13.2	Agent	improve		IncidentManagement
ISO/IEC 27001 Annex A.14	Control	subsume	subtypeOf	BusinessContinuityMgt
ISO/IEC 27001 Annex A.14	Agent	ensureSecure		BusinessContinuity

ISO/IEC 27001 Annex A.15	Control	subsume	subtypeOf	Compliance
ISO/IEC 27001 Annex A.15.1	Compliance	comprise	isComprised	LegalCompliance
ISO/IEC 27001 Annex A.15.2	Compliance	comprise	isComprised	PolicyStandardCompliance
ISO/IEC 27001 Annex A.15.3	Compliance	comprise	isComprised	EnsureAuditEffectiveness
ISO/IEC 27001 Annex A.15.1	Agent	ensure		Legalrequirement
ISO/IEC 27001 Annex A.15.2	Agent	ensure		PolicyStandard
ISO/IEC 27001 Annex A.15.3	Agent	ensure		AuditEffectiveness
ISO/IEC 27001 Annex A.11.4.1	NetworkSecurityMgt	comprise	isComprised	ClarifyNetworkServicesPolicy
ISO/IEC 27001 Annex A.11.4.2	NetworkSecurityMgt	comprise	isComprised	UserAuthentication
ISO/IEC 27001 Annex A.11.4.3	NetworkSecurityMgt	comprise	isComprised	EquipementIdentificaion
ISO/IEC 27001 Annex A.11.4.4	NetworkSecurityMgt	comprise	isComprised	RemoteDiagnosticConfigurationPortProtection
ISO/IEC 27001 Annex A.11.4.5	NetworkSecurityMgt	comprise	isComprised	NetworkSegregation
ISO/IEC 27001 Annex A.11.4.6	NetworkSecurityMgt	comprise	isComprised	NetworkConnectionCtrl
ISO/IEC 27001 Annex A.11.4.7	NetworkSecurityMgt	comprise	isComprised	NetworkRoutingCtrl
ISO/IEC 27001 Annex A.11.4.1	Agent	clarify		NetworkServicesPolicy
ISO/IEC 27001 Annex A.11.4.2	Agent	authenticate		User
ISO/IEC 27001 Annex A.11.4.3	Agent	identificate		Equipement
ISO/IEC 27001 Annex A.11.4.4	Agent	perform		RemoteDiagnosticConfigurationPortProtection
ISO/IEC 27001 Annex A.11.4.5	Agent	seperate		Network
ISO/IEC 27001 Annex A.11.4.6	Agent	manage		NetworkConnection
ISO/IEC 27001 Annex A.11.4.7	Agent	manage		NetworkRouting
ISO/IEC 27001 Annex A.11.5.1	OperatingSystemAccessCtrl	comprise	isComprised	LogOnProcedure
ISO/IEC 27001 Annex A.11.5.2	OperatingSystemAccessCtrl	comprise	isComprised	UserIdentificationAuthentication
ISO/IEC 27001 Annex A.11.5.3	OperatingSystemAccessCtrl	comprise	isComprised	PasswordManagement
ISO/IEC 27001 Annex A.11.5.4	OperatingSystemAccessCtrl	comprise	isComprised	SystemUtilitiesUse
ISO/IEC 27001 Annex A.11.5.5	OperatingSystemAccessCtrl	comprise	isComprised	SessionTimeOut
ISO/IEC 27001 Annex A.11.5.6	OperatingSystemAccessCtrl	comprise	isComprised	ConnectionTimeLimitation
ISO/IEC 27001 Annex A.11.5.1	Agent	clarify		LogOnProcedure
ISO/IEC 27001 Annex A.11.5.2	Agent	identify		UserToOS
ISO/IEC 27001 Annex A.11.5.2	Agent	authenticate		UserToOS
ISO/IEC 27001 Annex A.11.5.3	Agent	manage		Password
ISO/IEC 27001 Annex A.11.5.4	Agent	use		SystemUtilities
ISO/IEC 27001 Annex A.11.5.5	Agent	timeOut		Session
ISO/IEC 27001 Annex A.11.5.6	Agent	limit		ConnectionTime

7.2 User Data Protection

The following lexons are ontological readings of OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data. The table below indicates the key entities (DataController, DataSubject, PersonalData) in the principles of:

- **Collection Limitation Principle**: there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality Principle**: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification Principle**: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation Principle**: personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law
- **Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

In the following tables, the first table of lexons are directly read from the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data. The other tables are inferred from the document. The paragraphs are quoted below.

7.2.1 Data Controller

A data controller is a party, who according to domestic law is competent to decide about the components and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent in its behalf.

Context	Term1	Role	Co-role	Term2
		subsume	subtypeOf	DataController
OECD data protection Guideline	DataController	collect		Data
OECD data protection Guideline	DataController	store		Data
OECD data protection Guideline	DataController	process		Data
OECD data protection Guideline	DataController	disseminate		Data
OECD data protection Guideline	DataController	transfer		Data
OECD data protection Guideline	DataController	use		Data
OECD data protection Guideline	DataController	implement		SecuritySafeguard
		subsume	subtypeOf	DataSubject
OECD data protection Guideline	DataSubject	approve		processData
OECD data protection Guideline	DataSubject	know		processData
OECD data protection Guideline	SecuritySafeguard	protect		PersonalData
OECD data protection Guideline	Authority	approve		processData

7.2.2 Personal Data

Personal data means any information relating to an identified or identifiable individual (data subject). The Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

Context	Term1	Role	Co-role	Term2
OECD data protection Guideline	Data	subsume	subtypeOf	PersonalData
OECD data protection Guideline	Data	characterisedBy		Category
OECD data protection Guideline	Data	characterisedBy		Descriptor
OECD data protection Guideline	Agent	access		Data
OECD data protection Guideline	Agent	destory		Data
OECD data protection Guideline	Agent	modify		Data
OECD data protection Guideline	Agent	create		Data
OECD data protection Guideline	Agent	subsume	subtypeOf	DataSubject
OECD data protection Guideline	Agent	subsume	subtypeOf	DataController
OECD data protection Guideline	Organisation	subsume	subtypeOf	Authority

7.2.3 Other Concepts

Context	Term1	Role	Co-role	Term2
OECD data protection Guideline	process	fulfill		Purpose
OECD data protection Guideline	process	characterisedBy		Time
OECD data protection Guideline	process	characterisedBy		Purpose
OECD data protection Guideline	process	characterisedBy		Context
OECD data protection Guideline	process	characterisedBy		Manner
OECD data protection Guideline	process	characterisedBy		Means
OECD data protection Guideline	process	subsume	subtypeOf	collect
OECD data protection Guideline	process	subsume	subtypeOf	store
OECD data protection Guideline	process	subsume	subtypeOf	disseminate
OECD data protection Guideline	process	subsume	subtypeOf	transfer
OECD data protection Guideline	process	subsume	subtypeOf	use
OECD data protection Guideline	process	subsume	subtypeOf	SecuritySafeguard
OECD data protection Guideline	process	endanger		Privacy
OECD data protection Guideline	process	endanger		Liberty
OECD data protection Guideline	Manner	characterisedBy		Attribute
OECD data protection Guideline	Manner	subsume	subtypeOf	Means
OECD data protection Guideline	Attribute	subsume	subtypeOf	Fairness
OECD data protection Guideline	Attribute	subsume	subtypeOf	Lawfulness
OECD data protection Guideline	Attribute	subsume	subtypeOf	Appropriateness
OECD data protection Guideline	Attribute	subsume	subtypeOf	Accuracy
OECD data protection Guideline	Attribute	subsume	subtypeOf	Completeness
OECD data protection Guideline	Attribute	subsume	subtypeOf	Relevence
OECD data protection Guideline	Attribute	subsume	subtypeOf	Necessity

8 Conclusion

As part of this document, we have highlighted the requirement for an ontology as part of TAS^3. Furthermore, we described an upper ontology that would be relevant to many project including this one. The advantage of an upper ontology is to be able to deal with multiple domains within the same applications (e.g. employability and eHealth). Finally, we have shown how this upper ontology could be used to define lexons based on different standards.

9 References

[1] Gruber, T. R. (1993). Towards principles for the design of ontologies used for knowledge sharing. In *Formal Ontology in Conceptual Analysis and Knowledge Representation*, pages 907–928, Deventer, The Netherlands.

[2] P. Spyns, Y. Tang, and R. (2008). Meersman. An Ontology Engineering Methodology for DOGMA. In *Journal of Applied Ontology*, 3:13-39.

[3] Spyns, P., Meersman, R., Jarrar, M. (2002). Data modelling versus ontology engineering. *SIGMOD Record Special Issue on Semantic Web, Database Management and Information Systems* 31(4):12-17.

[4] Meersman, R. (2002). Web and ontologies: Playtime or business at the last frontier in computing? In *Proceedings of the NSF-EU Workshop on Database and Information Systems Research for Semantic Web and Enterprises*, pages 61–67.

[5] De Leenheer, P., de Moor, A., Meersman, R. (2007). Context dependency management in ontology engineering: a formal approach. *Journal on Data Semantics VIII*, LNCS 4380, Springer-Verlag, pages 26-56.

[6] de Moor, A., De Leenheer, P., Meersman, R. (2006). DOGMA-MESS: A meaning evolution support system for interorganizational ontology engineering. In *Proceedings of the 14th International Conference on Conceptual Structures (ICCS 2006)*, Aalborg, Denmark.

[7] Christiaens, S., de Moor, A. (2006). Tool interoperability from the trenches: the case of DOGMA-MESS. In *Proceedings of the First Conceptual Structures Tool Interoperability Workshop (CS-TIW 2006)*, pages 103–118.

[8] Niles, I., and Pease, A. (2001). Towards a Standard Upper Ontology. In *Proceedings of the 2nd International Conference on Formal Ontology in Information Systems (FOIS-2001)*, Ogunquit, Maine.

[9] ISO/IEC 15408-1 (2005): Information technology — Security techniques — Evaluation criteria for IT security —Part 1:Introduction and general model.

[10] ISO/IEC 17799: Information technology — Security techniques — Code of practice for information security management.

[11] ISO/IEC 27001 (2005): Information technology - Security techniques - Information security – management systems – Requirements.

[12] OECD Guidelines for the Security of Information Systems and Networks (2002). Towards a Culture of Security. Paris: OECD, www.oecd.org.

[13] van Rijsbergen, C. (1979). Information Retrieval (2nd ed.). Butterworths, London.

[14] Berners-Lee, T., Hendler, J., and Lassila, O. (2001). The Semantic Web. *Scientific American*, May:34-43.

[15] Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

[16] Phytila, C. (2002) An Analysis of the SUMO and Description in Unified Modeling Language, April.

[17] ISO/IEC Guide 73 (2002): Risk Management –Vocabulary – Guidelines for use in standards.

[18] Morgan, R., and Boardman, R. (2003). Data Protection Strategy: Implementing data protection compliance. Sweet & Maxwell.

[19] ISO/IEC TR 18044 (2004): Information Technology – Security techniques – Information security incident management.

10 Document Control

Amendment History

Version	Baseline	Date	Author	Description/Comments
0.1		17-11-2008	G Zhao	Creation of the document
0.2		01-12-2008	D Wu	Added material from ISO standards
0.3		04-12-2008	Q Reul	Added content to Chapter 3
0.4		09-12-2008	G Zhao	Added the requirements for TAS^3
0.5		10-12-2008	Q Reul	Added content for section 4.2
0.6		12-12-2008	D Wu	Developed lexons in Chapter 7
0.7		12-12-2008	Q Reul	Added content to section 4.3
0.8		19-12-2008	Q Reul	Edited the document
0.9		30-12-2008	Q Reul	Addressed reviewer's comments
1.0		31-12-2008	Q Reul	Formatted the document