SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document Type: Deliverable

Title: **TAS³ Upper Common Ontology**

Work Package: WP2

Deliverable Nr: D2.2

Dissemination: PU

Preparation Date: December 17, 2010.

Version: 3.2

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	Project Mgr
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	Gang Zhao	VUB
2	Ioana Ciuciu	VUB
3	Cristian Vasquez	VUB
4	Quentin Reul	VUB
5	Dongya Wu	VUB, CESI

Contents

List of Figures

1 Executive Summary

The TAS³ (***Trusted Architecture for Securely Shared Services***) project aims to develop an open, secure and trusted architecture for the exchange of personal information across services. As this data is generated over a human lifestyle, it needs to be collected and stored at distributed locations and used by a multitude of services. In the employability domain, for instance, a person is continuously learning new competences not only based on her education history, but also based on her employment experience. As a result, all partners in a Trust Network (TN) need to agree upon a common understanding for the technical underpinning of the services as well as a common vocabulary for the data.

One of the goals of the TAS³ project is to exploit Semantic Web technologies to address this problem. The Semantic Web extends the current World Wide Web (WWW) with resources in machine-readable form. On the one hand, each organisation needs to document their respective services in well documented standards (e.g. SOAP and WSDL). On the other hand, the resources (e.g. personal information) being exchanged need to be given adequate semantics to know which services have to be used. These types of resources are given meaning through the use of *ontologies*. An ontology is a server-stored shared agreement on the semantics of the concepts and the relations between them in a given domain.

This document describes the TAS³ ontology developed by STARLab. We first introduce a Descriptive Upper Ontology (DUO) representing general concepts, which can be applied to any domains. This upper ontology is different from existing ones as (i) it is grounded in natural language, and (ii) provides a descriptive framework to capture real world semantics. As a result, the upper ontology can be re-used in a non-restrictive manner. The UCO is the baseline for the semantic services developed and integrated within the TAS³ architecture:

- The ontology-based interoperability service, which provides authorization policy interoperability, and
- The secure business process models annotator, which enables security by design.

In the employability and the eHealth scenario, the ontology-based interoperability service is used in the authorization phase, ensuring the interoperability between the service requester and the service provider. The annotator is supporting the business modeller into creating security policies, with a recommendation system based on the security constraints ontology and a knowledge base.

Furthermore, we extracted important concepts from IT standards (e.g. ISO/IEC 15008, 17799) to develop the Upper Common Ontology (UCO). A UCO contains the conceptualizations and semantic constraints that are common to and accepted by a domain. As such, we believe that standards provide a vocabulary of terms (agreed upon by domain experts) and that this can provide a starting point for the TAS³ conceptualisation. Annotating (web) services with security concepts would allow the correct semantic interpretation of security paradigms and data protection regulations (addressing privacy) and thus increase the trust in the TN.

2 Introduction

2.1 Document Scope and Objective

The goal of the TAS³ (***Trusted Architecture for Securely Shared Services***) project is to develop a trusted Service-Oriented Architecture (SOA) enabling secure exchange of personal information across (human and non-human) agents. A SOA decomposes complex business processes into manageable and reusable services to respond to changing business environments. Furthermore, it facilitates the collaboration between any numbers of organisations to provide combined services. For instance, a company providing vocational advice (e.g. Kenteq) might require contacting multiple sources (e.g. companies, schools) to aggregate personal information for each customer. To achieve this, all partners participating in the Trust Network (TN) need to agree upon a common understanding for the technical underpinning of the services as well as a common terminology for the data.

Semantic Web technologies provide the means to address this problem. The Semantic Web [1] extends the current World Wide Web (WWW) with resources in machine-understandable format. On the one hand, each organisation needs to document their respective services in well documented standards. For example, WSDL [2] provides a language describing the requirements and capabilities of Web Services, while SOAP [3] provides a basic messaging framework on which Web Services are built. On the other hand, the resources (e.g. personal data) being exchanged need to be given adequate semantics to know which services have to be used. These types of resources are normally given meaning through the use of ontologies. An ontology is commonly defined as: "*a [formal,] explicit specification of a [shared] conceptualization*" [4]. More specifically, an ontology is a server-stored shared agreement on the semantics of the concepts and the relations imposing a structure on the domain that is readable by both humans and machines.

This document describes the TAS³ ontology developed by STARLab to be integrated within the TAS³ architecture [5]. Originally, we were supposed to follow a bottom-up approach to ontology development. However, there were several issues that made this approach difficult to follow in practice. On the one hand, a consensus on the use cases was not reached in the early phase of the project. On the other hand, it became quickly apparent that the project would benefit from capturing key concepts from the security and privacy domain in a high level ontology. This would create a resource that would enhance and add greater support to the latter integration of more specific concepts from the domain as they emerge. Therefore, it was agreed that STARLab would first develop the upper common ontologies. Our top-down approach stresses the architecture of the ontology to facilitate evolution and change management, in the spirits of the best practices of architecture-centred, component-based software engineering.

As part of this approach, we first developed a novel Descriptive Upper Ontology (DUO). This upper ontology is different from existing ones (e.g. SUMO [6], DOLCE [7]) as (i) it is grounded in natural language, and (ii) provides a

descriptive framework allowing the upper ontology to be re-used in a non-restrictive manner.

Secondly, we developed an Upper Common Ontology (UCO) to provide semantics to underpin the trust and privacy negotiation within the TN. As a result, we need to represent the conceptualisation that is common to a domain and accepted by its experts. As part of this development process, we first followed a *top-down* approach to extract key concepts in the domain of security, data protection and privacy. Although several ontologies on security already exist (e.g. [8, 9]), none of these have been developed to represent IT security standards (e.g. ISO standards). Moreover, these ontologies cover the concept of Privacy, which is essential to the success of the TAS³ TN. Looking at the available literature on security and data protection, we identified a series of IT security guidelines (i.e. ISO/IEC 15408 [10], ISO/IEC 17799 [11] and ISO/IEC 27001 [12]) and data protection regulations (i.e. EU Directive95/46/EC) and guidelines (i.e. OECD guideline on the Protection of Privacy and Transborder Flows of Personal Data). For instance, ISO/IEC 17799 describes best practices in the domain of information security management (e.g. asset management). Although these standards and guidelines do not focus solely on SOA, they describe key concepts that hold for any type of systems where security and data protection are indispensable. In addition, these standards provide a vocabulary, which has been agreed upon by domain experts through concertation.

Based on the DOGMA-MESS methodology [13], the conceptualisation in the UCO is revised through consolidation of knowledge defined in the lower layers of the ontologies (i.e. Lower Common Ontology [14] and Service Ontology). The latest iteration of this deliverable includes a revision of the UCO based on the conceptualisation provided in Deliverable D2.3. Although the TAS³ ontology will cover other topics (i.e. web services and business processes), these topics are not the focus of this deliverable and will represented in the Service Ontology associated with each service on the TN. For instance, Deliverable D3.1 [15] provides a conceptualisation of business processes. Annotating business processes with security concepts would allow the correct semantic interpretation of security paradigms and data protection regulations and thus increase the trust in the TN. For example, a placement provider trying to access a student's personal data remotely, needs to pass the authentication and authorization process, to determine if (1) the placement provider dominates the subject in the student's authorization policy, (2) the requested action is dominated by the action in the access control policy and (3) the resource to be accessed is dominated by the resource in the policy. By annotating the authorisation policies with appropriate security concepts, the access control can be done more effectively.

2.2 Reading Guide

The rest document is structured as follow:

- Section 3 describes the background information required to understand this document. It first disambiguates common concepts, such as glossary, thesaurus and ontology. It then presents several general applications of ontologies, before describing the different resources used as part of this deliverable.

- Section 4 describes the scope of the TAS³ ontology and highlights how the semantics will be used within the TAS³ architecture.
- Section 5 introduces the assumptions behind the ontology engineering methodology developed at STARLab.
- Section 6 describes ontology in more detail focusing on the ontology structure and in particular the different topics covered by the ontology; namely stakeholders, protected assets, security activities, compliance, trust, and security techniques.
- Section 7 presents the ontological architecture design adopted as part of TAS³, introduces a novel Descriptive Upper Ontology and describes the implementation of the ontology and its link to standards representing several key concepts related to security and privacy.
- Section 8 describes the integration of the ontology within TAS³, introducing the ontology-based interoperability server (OBIS) and the secure business process annotator.
- Section 9 provides a conclusion on our current work and presents future work.

3 Background

This section introduces the background knowledge required to understand the document. Firstly, we introduce the differences between glossaries, thesauri and ontologies. We then present how ontologies have been used to solve two well-known problems; namely information retrieval and interoperability. Finally, we describe the different knowledge resources (i.e. standards and guidelines) used as part of this document.

3.1 Glossaries, Thesauri and Ontologies

A *glossary* is a list of terms, together with definitions, specific to a given field of knowledge usually presented in alphabetical order [16]. In other words, terms are defined for a specific environment (e.g. TAS³) and rarely include homonyms. Traditionally, a glossary is located at the end of a document referring to terms that have been introduced or were referred to by acronyms. For example in TAS³, a trust network is defined as:" a*n online business environment where parties can interact with each other securely. While the network does not warrant hones behaviour of the members in the network, it does ensure that everybody adheres to some basic principles especially in non-repudiation, data security, communications security, and IT security. Thus a Trust Network promotes trust between its members.*"

A *thesaurus* is a collection of terms arranged in a known order and structured to clearly display various standardized relationships among them [16]. These terms are composed of one or more words designating a concept. Terms in thesauri are defined as either *preferred term* (used for indexing) or *non-preferred term* (known synonyms used for searching). Preferred terms are related to non-preferred terms with *Use For* (UF); USE is the inverse of this relation (Figure 3.1). Note that homonymous terms[1] should be supplemented with a qualifier to distinguish them.

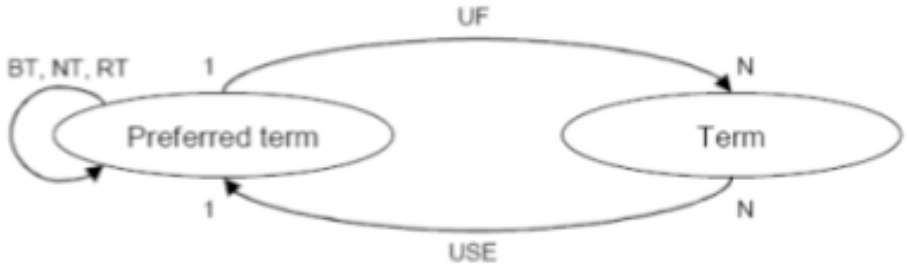

Figure 3.1: Basic thesaurus relations taken from [17].

The structure of the thesaurus is achieved by three types of semantic relations; namely *broader term* (BT), *narrower term* (NT), and *related term* (RT). Although BT and NT can be used to define subsumption, it can also represent many other relations, such as partonomy. RT is used to express the associative relation

[1] A term with more than one distinct meaning.

between terms. eCl@ss[2] is a thesaurus representing products, material and services along an entire supply chain.

An *ontology* provides an agreed semantics of a certain domain (e.g. security) represented in a computer format that enables sharing and interoperation between information systems [18]. More specifically, an ontology is a server-stored shared agreement on the semantics of the concepts and the relations imposing a structure on the domain that is readable by both humans and machines. Note that ontologies provide a much richer set of user-defined relationships (e.g. *instance_of*, *part_of*) than thesauri. The creation of ontologies requires a combination of lexical terms (for naming concepts) and rules to constrain the structure and interrelationships of concepts. Several representational schemas have been proposed to express these rules and constraints (e.g. Ω-RIDL and description logic). For example, OWL provides a syntax based on description logic to publish and share ontologies on the web [19]. However, OWL hinders knowledge elicitation by technical and non-technical domain experts as it requires background in description logic.

3.2 Applications of Ontologies

Ontologies are essential in distributed SOA's to enable applications. The application of ontologies greatly enhances the process of information retrieval making it more efficient and accurate to retrieve data. Moreover, dynamic and composite applications within SOA's are enhanced by this efficiency and improvements on interoperability and design aided by ontologies.

3.2.1 Information Retrieval

The field of information retrieval [20] 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 ones 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[3] (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, 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 [11] and ISO/IEC 27001 [12].

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 find the matching ones. This implies the semantic comparison of the job profile

[2] http://www.eclass-online.com/
[3] http://www.oclc.org/dewey/

and candidate profiles based on an ontology of skills. See Section 4.2 for more examples related to TAS³.

3.2.2 Interoperability

The IEEE [21] 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[4], which developed the European Interoperability Framework[5] (EIF). This framework describes policies and standards to be agreed by all organisations involved to promote interoperability. EIF have identified four types of interoperability enabling the transfer data across systems that have some relevance to TAS³; namely *semantic*, *technical*, *organisational*, and *legal* interoperability. The different types of interoperability are explained below:

- *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. Deliverable D8.2 (section 2.1) provides a solution to handling this problem [22].

- *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 TAS³, 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. In TAS³, two organisations could use the same terminology to represent security, privacy and trust concepts but provide different policies based on this

[4] http://ec.europa.eu/idabc/en/home
[5] EIF, European Interoperability Framework for Pan-European eGovernment Services, 2004. http://europa.eu.int/idabc/en/document/3761

terminology. As such, we need to ensure that access to data is enforced based on their respective policies. For example, a user shouldn't gained access to data (he doesn't have access to) by accessing it through other organisations on the TN.

- *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 organisation (e.g. health centre) attempting to access the medical record of a patient located in another country would have to abide to the regulations in its own country as well as those of the patient's.

3.2.3 Security by Design

Ontologies can serve as tools for design, in domains where the vocabulary needs to be controlled and secured. The security and privacy is such a domain. In TAS³, web services are orchestrated in a lightweight manner, via the implementation of business processes. The security constraints are modelled in a descriptive way, on top of classical business processes, using semantic annotations. The security constraints are then transformed into business rules and enforced.

The semantic annotations of security constraints are a tool intended to support the business modeller into designing secured business processes. In uses an ontology base of security constraints and a knowledge base. We refer to Section 8 for more details.

3.3 Knowledge Resources

In this sub-section, we describe in some details the different resources used for the development of our ontology.

3.3.1 Glossary

As part of the TAS³ project, we have developed a project specific glossary (see Appendix A). A glossary is an alphabetical list of terms in a particular domain of knowledge with the definitions for those terms. However, glossaries do NOT contain semantics and we plan to use this glossary as an input to our ontology development in future iterations of this document.

3.3.2 ISO/IEC Standards on Security in IT Systems

Hafner and Breu [23] define security in SOA as:"... the sum of all techniques, methods, procedures and activities employed to maintain an ideal state specified through a set of rules of what is authorised and what is not in a heterogeneous, decentralized, and inter-connected computing systems." Although SOA are different from typical IT systems, we believe that they share common techniques, methods and procedures to protect assets. As a result, we have used several

international standards developed by ISO (International Organization for Standardization) in collaboration with IEC (International Electro-technical Commission). We believe that these standards provide key security concepts agreed upon by domain experts. Although there exists several other ISO standards (e.g. ISO/IEC 18044 and ISO/IEC 27002), we focused on these three as they are developed and adopted popularly by many countries, especially the countries from Europe, such as UK, Netherland, etc. Furthermore, these standards describe the basic concepts and measures that are accepted widely. This list was not intended to be an exhaustive one but instead describes the standards currently used and their relations to TAS³.

Firstly, ISO/IEC 15408 [10] 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 3.2 describes the relation between the main security concepts, such as assets, risk. For example, it shows that vulnerabilities lead to risk (e.g. loss of integrity) towards an asset (e.g. personal data). The owners will analyse the vulnerabilities applicable to their specific assets and their environment, determining the risks associated with them. This analysis will result in the implementation of countermeasures to counter the risk and reduce it to an acceptable level. For example in TAS³, the integrity of personal data could be in danger when accessed by an unauthorized agent. As a result, the owner will implement adequate authentication mechanisms (e.g. RBAC) to ensure that the data can be accessed by the right user. Note that residual vulnerabilities may remain despite the implementation of countermeasure.

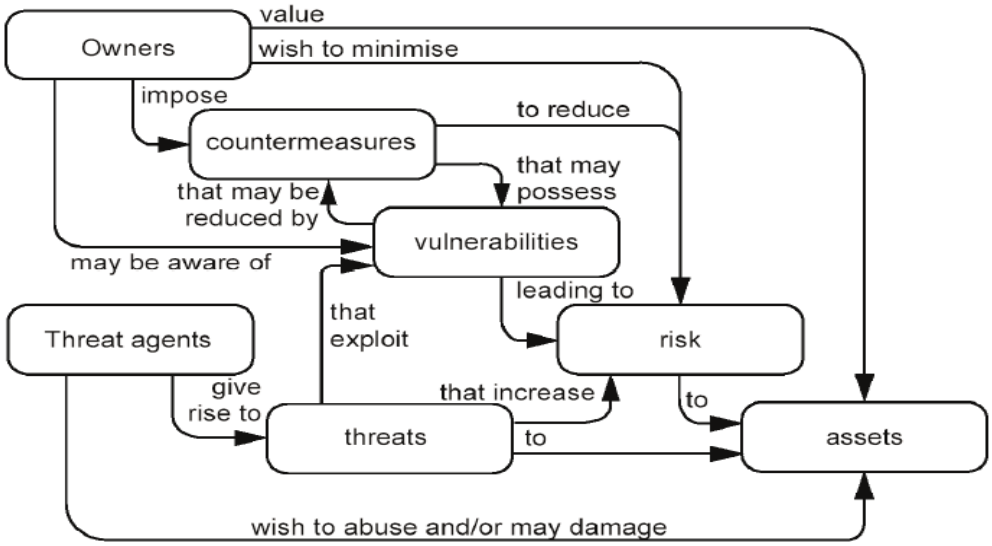

Figure 3.2: Security concepts and their relations in ISO/IEC 15408.

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. For example, an agent might want to intercept data and then make a profit out of its resale. Furthermore, threat agents may exploit residual vulnerabilities (i.e. those that remain despite countermeasure being put into place). For example in TAS³, denial-of-service attacks (DoS) could make personal data unavailable to its

intended users. As a result, the value of an 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).

Secondly, ISO/IEC 17799 [11] establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. This standard provides general guidance on the commonly accepted goals of information security management. It covers aspects such as security policy, asset management and access control that are at the core of the work within TAS³.

Finally, ISO/IEC 27001 [12] describes security vulnerabilities and business risks that an organisation (e.g. commercial enterprises, government agencies) could encounter as part of their IT systems. Furthermore, it provides a list of security controls to protect information assets leading to an increase in trust from third parties. To enable secure exchange of personal information between organisations in TAS³, we first need to investigate the security management processes available within each organisation.

This standard is suitable for a wide range of uses, including the following that are relevant to TAS³:

- define security requirements and objectives within an organisation;
- ensure that these objectives are compliant with current laws and regulations;
- identify and clarify the existing information security management processes;
- implement and operate relevant security controls;
- provide information about the security policies enforced by an organisation;
- internally and/or externally audit the degree of compliance with security policies adopted by a company.

Moreover, ISO/IEC 27001 adopts the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all Information Security Management System (ISMS) processes. Figure 3.3 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.

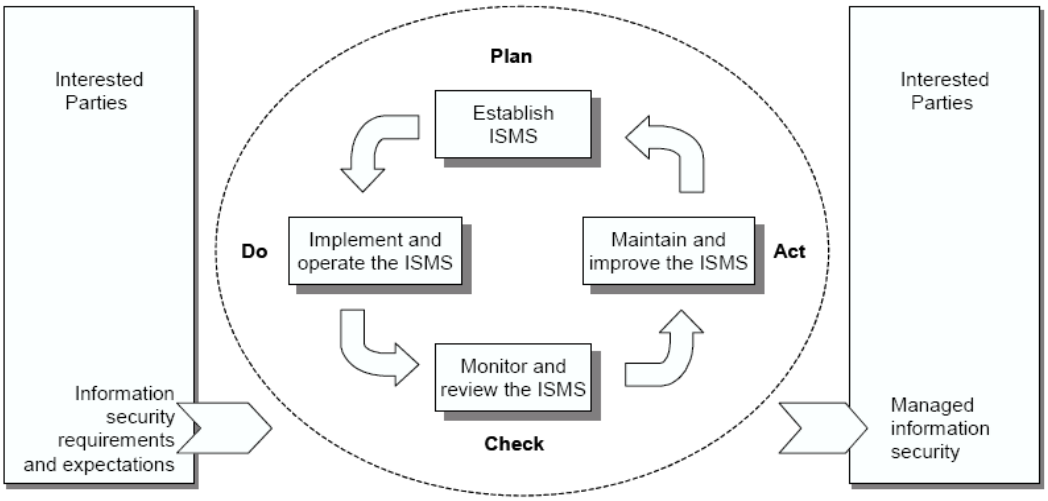

Figure 3.3: PCDA model applied to ISMS processes.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines [24] 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 Data Protection Resources

There are three major documents that create the foundation of privacy in the EU. Firstly, the Organisation for Economic Co-operation and Development (OECD) developed guidelines on the Protection of Privacy and Transborder Flows of Personal Data[6]. This document addresses the problem of privacy protection with regard to the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data. Although many countries have introduced privacy protection laws, the OECD guidelines have been proposed as a way to harmonise national legislations to facilitate the free flow of personal data across frontiers. Secondly, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[7] (Strasbourg, 28.I.1981) describes how personal data should be processed by automatic process to respect of privacy regardless of frontiers. This convention has been agreed by the member state of the Council of Europe. Finally, Directive 95/46/EC[8] on the protection of individuals with regard to the processing of personal data and on the free movement of such data has been developed to remove potential obstacles to such flows and to ensure a high level of protection within the EU, data protection legislation has been harmonised. The Commission also engages in dialogues with non-EU countries in order to insure a high level of protection when exporting personal data to those countries. It also initiates studies on the development on European and international level on the state of data protection.

---

6 http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

7 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

8 http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

In TAS³, we plan to deploy the architecture in several pilots for specific countries (see TAS³ Deliverable D9.1 [25]). To address the privacy legislation in these Member States (i.e. UK and the Netherlands), we need to take account the following national laws:

- Data Protection Act 1998 CHAPTER 29[9]
- Personal Data Protection Act (Wet Bescherming Persoonsgegevens) 2001

[9] http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

4 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 scope of the ontology by answering two questions about its content:

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

4.1 Themes

The themes identify the different universe of discourse to be covered by the TAS³ ontology, namely policy, process and data. The following sections describe each theme in more details.

4.1.1 Policies

The policies considered within the TAS³ TN 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.

Based on the analysis of the TAS³ use-case [24], security standards and data protection policies, we can identify the following policies:

- 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
- Privacy

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

4.1.2 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.

The concept of Process has been further refined into a Lower Common Ontology (see Deliverable D2.3) for secure business processes. This ontology is conceptually representing the security constraints which are at the basis of the security annotations. The role of this ontology is to assist the business process modeller into annotating secured business processes with security annotations, which will further be transformed in security policies.

4.1.3 Data

TAS³ 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 eHealth in the project. However, it will not be a focus as part of this document.

4.2 Semantics within the TAS³ System Architecture

The TAS³ project aims at developing a trusted Service-Oriented Architecture (SOA) enabling secure exchange of personal information across (human and non-human) agents. Thus, TAS³ 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.

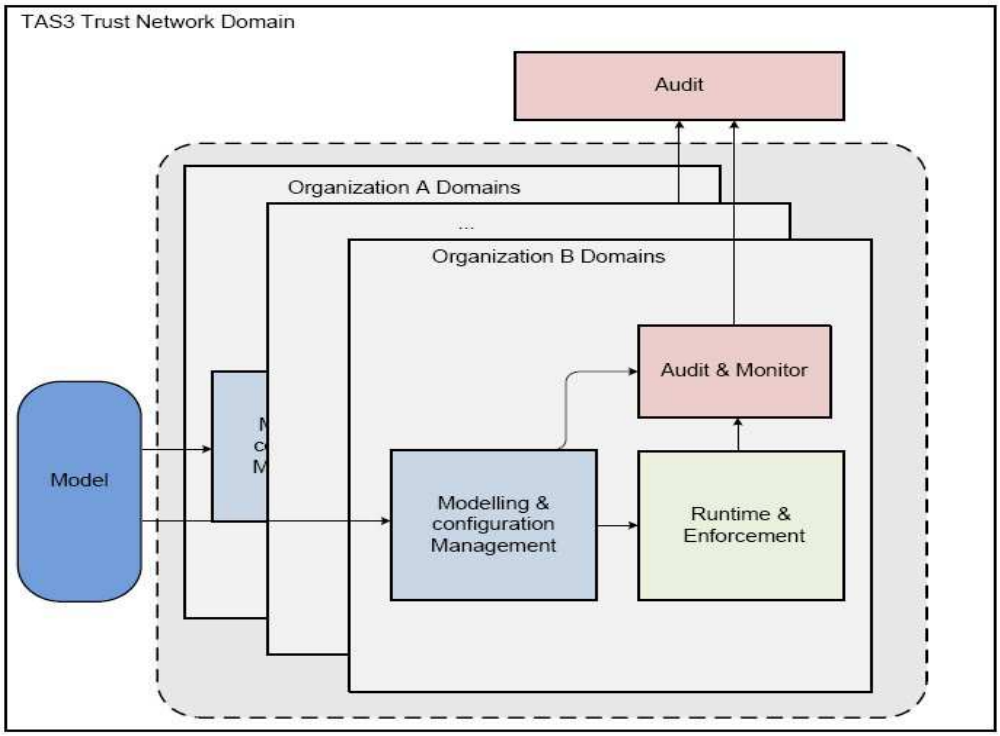

Figure 4.1: TAS³ high-level Trust Network Architecture.

Figure 4.1 describes the high-level Trust Network Architecture [5]. An essential element of this architecture is a community-managed ontology (Model in Figure

4.1), which allows for unambiguous, but flexible, meaning agreement at all times. We can envisage several roles for this ontology. It first provides a machine-understandable documentation of the architecture as well as a formal vehicle to exchange explicit semantic agreements (i.e. commitments) between partners and, eventually, systems. Thus, these commitments will enable the enforcement of (organisational and/or legal) policies within the TAS³ architecture. For example in Role-Based Access Control (RBAC), the role of a subject need to be provided with some semantics (e.g. a list of attributes) to be able to enforce authorisation based on the privileges assigned to that role.

Secondly, the 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.

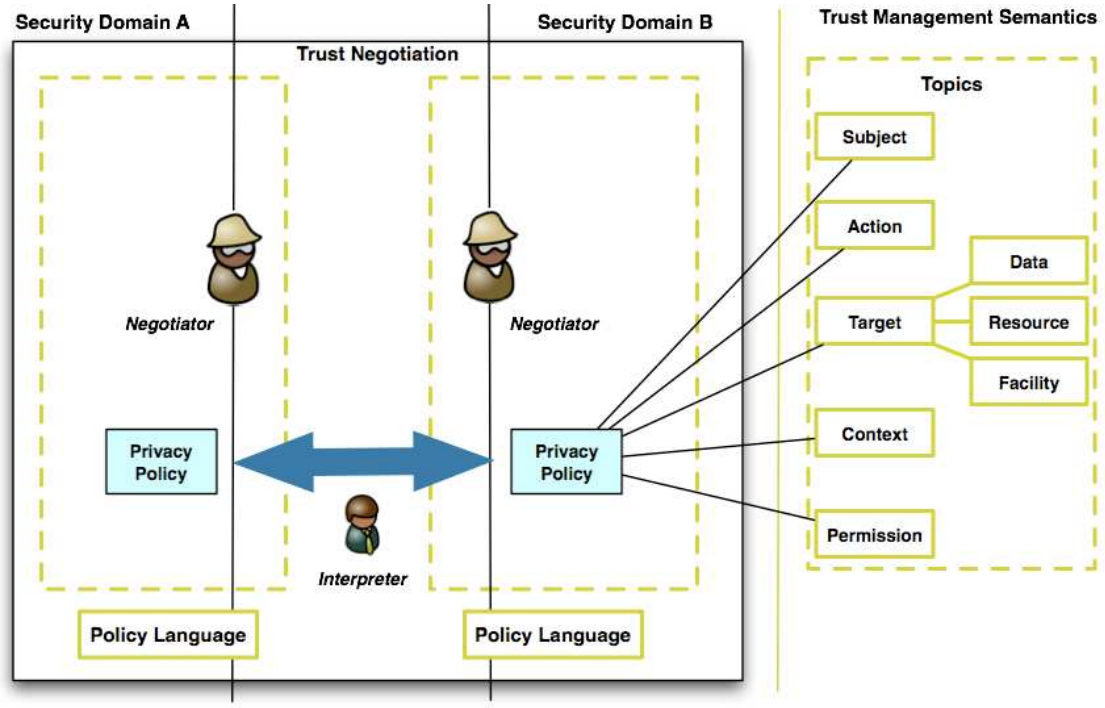

Figure 4.2: Cross-organisation policy interoperability.

In Figure 4.2, the interpreter (see the Ontology-based Interoperation Service in Section 9) translates a privacy policy from Security Domain A to a policy suitable for Security Domain B by focusing on 5 main concepts; namely *Subject*, *Action*, *Target*, *Context* and *Permission*. The Subject of a policy is an agent (e.g. data requestor, data consumer) who wants to perform a specific Action on a Target (e.g. personal data) in a particular Context. The target is any type of object that can be acted upon by an agent. In the eHealth domain, for example, the types of actions allowed on a patient record can be "read", "write", "modify" or "delete" and this can be done either by a doctor or by the patient himself depending on the context. The context covers information about the domain of application of a

policy, such as location and time. It may also cover a history of recent past actions. Finally, Permission is used to describe the rights given to a subject to perform some actions on a target in some context.

The interpreter provides different mechanisms to map ontological entities from heterogeneous entities. Castano et al. [26] identify two main categories of ontology matching techniques; namely linguistic and contextual matching techniques. Linguistic techniques evaluate the similarity among ontological content (i.e. classes, roles and instances) based on their names or labels. The main characteristic of these techniques is that they evaluate the similarity between two strings of characters. For example, the edit distance counts the minimum number of changes, such as insertion, deletion and replacement of characters, required to transform one string into the other string [27]. Although linguistic techniques often provide highly precise mappings, these techniques tend to fail when there is little lexical overlap between the labels of ontological entities. Contextual matching techniques can remediate to this problem by assuming that some of the meaning of an entity is conveyed by its context. For example, Dieng and Hug [28] calculate the similarity between two concepts based on their direct super-classes and/or direct subclasses and/or sibling classes. The semantic interoperability engine will include different algorithm of these types, and thus be able to deal with a wide range of mismatches.

In Section 3.3.2, we presented the relationships between general security concepts. 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. In TAS³, these threats will have to be complemented with potential problems arising in SOA. Furthermore, TAS³ involves two domains of use: employability and eHealth. Employability refers to the ability of a person to gain and maintain employment, while eHealth covers health care practices that are supported by electronic processes and communication. Deliverable D9.1 [24] describes several use cases in these two domains. 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.

5 DOGMA

As part of this deliverable, we used the DOGMA (Developing Ontology-Grounded Methods and Applications) framework to develop ontologies. This framework is based on database semantics and model theory [29]. This section describes the assumptions behind the framework as well as the building blocks of ontology inspired ontologies.

5.1 Assumptions

A DOGMA inspired ontology decomposes the ontology into a *lexon base* and a layer of reified ontological *commitments* [30]. This is called the *double articulation* principle. Its grounding in *natural language* 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.

Definition 1 (Lexon) *A Lexon is formally described as a 5-tuple* ***<γ, head, role, co-role, tail>****, where*

- ***γ*** *is an abstract context identifier,*
- ***head*** *is the subject,*
- ***role*** *is the predicate,*
- ***co-role*** *is the inverse of role, and*
- ***tail*** *is the object*

A lexon base layer stores context-specific binary fact types, called lexons, for constructing an ontology. A lexon (Definition 1) represents a plausible binary fact-type, where the context identifier (i.e. ***γ***) can be described in some natural language, and is used to group lexons that are logically related to each other in the conceptualisation of the domain. Intuitively, a lexon may be read as: within the context ***γ***, ***head*** may have a relation with ***tail*** in which it plays a ***role***, and conversely, in which ***tail*** plays a corresponding ***co-role***. Each (context, term)-pair then lexically identifies a unique concept. A lexon base can hence be described as a set of plausible elementary fact types that are considered as being true. In other words, the lexon base defines the vocabulary of the ontology. For example, *<ISO/IEC15008, Threat, targets, is-targeted, Asset>* is a lexon representing the relation between the concepts of `Threat` and `Asset`. In OWL [19], the context of a concept can only be defined by a Unique Resource Identifier (URI), whereas lexons allows the context to be the document (e.g. ISO.IEC15008) from which the fact was extracted. Furthermore, lexons refine the relation between two concepts by providing a co-role (or inverse role). Note that two roles are the same if and only if they have the same role co-role combination.

The commitment layer mediates between the lexon base and its applications. Each ontological commitment consists of a finite set of axioms that specify which lexons of the lexon base are interpreted. Therefore, it implies the choice of, and/or

adherence to a set of rules, constraints that will depend on the task to be performed. For example, it allows the application owner to define the properties (e.g. transitivity) of subsumption (i.e. is-a/subsumes) within his/her application. Note that rules that hold in one commitment need not to do so in another, but will nevertheless need to be formally *interpreted* in terms of the lexons in the same or related contexts. For example, inheritance of attributes (in subsumption) could be applied to some concepts but not to all. Moreover, commitments provide mappings between the conceptualisation layer and the data layer (in databases). An important difference with the underlying lexon base is that commitments are semantically consistent. For example in TAS³, we can use these ontological commitments (i.e. ontologies) to enable the integration of data (e.g. personal data) from 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 [31]. 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. As a result, the DOGMA methodology enables the domain knowledge to be re-used across multiple applications. This is very different from methodologies based on OWL (e.g. [32]), where the concepts are defined from the start based on the need of the 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 more complete formalisation of DOGMA can be found in [33].

5.2 Building Blocks

The structure of a DOGMA Ontology [13] consists of five building blocks of semantic specification (Figure 5.1). The ontological *Basis* layer defines essential objects (e.g. descriptor, predicate, and agent) and describes how these objects are related to each other through generic relations, such as subtype, supertype, instance, equivalence. The ontological *Assertion* layer states facts in terms of entities, relations and processes. Note that there is no limitation on the type of relationships allowed. For example, *<TAS3, Threat, target, is-targeted, Asset>* is an assertion. Ontological Basis and ontological Assertions consist of conceptual objects and relations in the form of lexons.

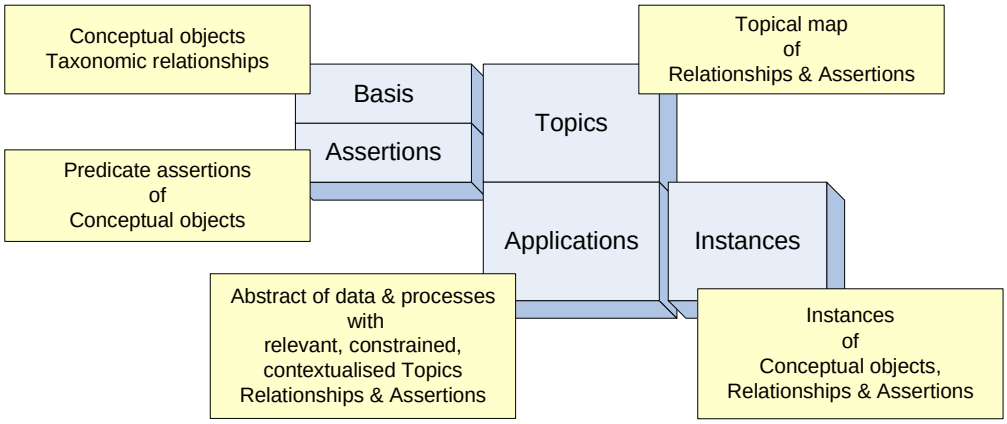

Figure 5.1: The DOGMA building blocks.

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. For example in TAS³, we can group lexons by subject matters, such as risk assessment, privacy, and trust (see Section 8). It is also the layer where the other existing ontological models (e.g. OWL-S [34] or WSMO [35]) are interfaced and incorporated.

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. It serves as a semantic representation with respect to a particular application. It needs further constraining and instantiating. For example in the Dutch Employability Domain [24], the vocational learning (e.g. soft skills, process knowledge) gained while working at a company (e.g. Heineken) will be represented different from those gained in another company. More specifically, each company will use its own vocabulary that need to be set within the context of the APL process.

The Ontological Instances block contains a list of concrete values for specific instantiations of lexons. In other words, it provides mappings between data stored in a specific repository (e.g. database) and its application-specific conceptualization. As a result, an application is able to retrieve data from multiple repositories based on semantic. For example in TAS³, a Kenteq service would be able to retrieve data about on individual from institutions a candidate previously attended, his/her former employer, as well as his/her ePortfolio.

The Basis, Assertions and Topics blocks form a layer of semantic resources that are generic and reusable over different applications. The Applications and Instances blocks pertain to application specific semantics, with instantiated and contextualised terms and relations from the Basis, Assertions and Topics. Together they form a platform on which the TAS³ ontologies will be built.

6 TAS³ Topics

The concept of *Topics* is used to represent the knowledge structure of domain experts (Section 5.2). Thus, it defines domain specific knowledge. Each topic consists of a subset of lexons from the Basis and Assertion building blocks of the ontology. We identify key topics of the TAS³ ontology through ISO/IEC standards on information system security, OECD and EU data protection guidelines (Figure 6.1). 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 but subsumes concepts specific to the TAS³ architecture and test cases.

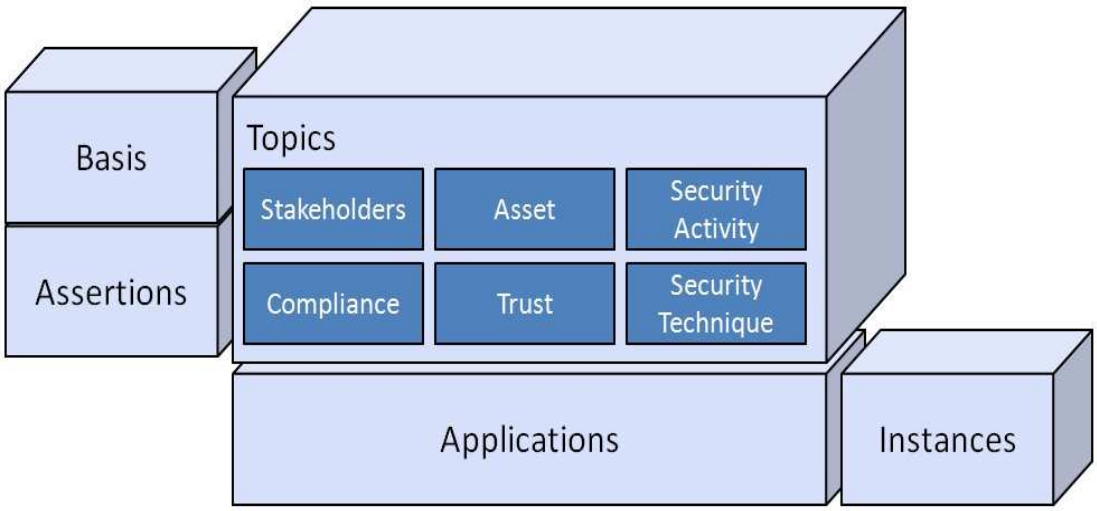

Figure 6.1: TAS3-specific ontology building blocks.

This section describes a map of topics to capture the semantic terrain of security, data protection and trust issues. Note that these topics were extracted from the standards described in Section 3.3.2 and 3.3.3. The following sections describe each box within the Topics block in more details.

6.1 Stakeholders

Stakeholders are agents in the security scenarios (e.g. student, patient), impacting or impacted on the security state or conditions. We can identify several types of stakeholders as sub-types of Agent; namely data owner, data subject, threat agent, risk assessor, and asset controller. A data owner is an agent that can authorize or deny access to certain data, while a data subject is a human to whom personal data relates. A threat agent describes any agent (i.e. human and non-human) seeking to abuse assets in a manner contrary to the interest of the data owner, while a risk assessor analyses the possible impact of an attack on assets. An asset controller ensures the availability of assets by managing the perceived risks. In TAS³, any entity participating in the TN will be a stakeholder.

6.2 Protected Assets

Asset means anything that has value to the organization [35]. 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 [36]. 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

The objective of secure area is to prevent unauthorized physical access, damage and interference to the organization's premises and information [11]. The objective of equipment security is to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

6.3 Security Activity

6.3.1 Security Action

A security action describes any activities 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 [9]. We can highlight several types of actions:

- **Security Audit**: A security audit is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site.
- **Risk Assessment**: Risk assessment is the overall process of risk analysis and risk evaluation [35], 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 [35, 11].

- **Risk Treatment**: Risk treatment is the process of selection and implementation of measures to modify risk [35].
- **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.
- **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, such as access restriction, sensitive system isolation.

In TAS³, the access control is checked by calling the ontology-based interoperability service, for computing the domination relation between two security concepts originating from two different security policies.

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 [37].

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 [37].

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. 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

Chang et al. [38] define Trust as: "a belief of confidence or a feeling of certainty that one person has in another person or thing that is/she is interacting with." In service-oriented network, like the TAS³ TN, trust is used to refer to the subjective notion of trust, i.e. a perceived likelihood that an entity/system (e.g. Service Provider) will behave/perform as required as well as to a formalization of this notion into a measurable quantity. The measurable quantity is called trustworthiness and represents the amount in which an entity is worthy of being trusted. Although trustworthiness can be transmitted through trusted paths, trusting an agent does not necessarily mean the opposite. In other words, if entity **A** trusts entity **B**, it does not necessarily mean that **B** trusts **A**. Trust in a system can be gained by trust enablers, i.e. have a behaviour that inspire trust. For example, a system implementing adequate authentication mechanism and thus protecting the privacy of personal data will inspire trust to its users.

6.6 Security Technique

The objective of security technique includes the protection of information from theft, corruption, while allowing the information and property to remain accessible and productive to its intended users.

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 TAS³ Semantic Architecture

The Semantic Web has been envisioned to allow people and machines to share the meaning of data and ultimately of applications to aid both distributed and dynamic computation over the web. The main efforts to enable this vision are focused on the capture of data and application semantics in ontologies and then map these ontologies via related concepts. As part of this section, we describe the ontology architecture developed by STARLab and its use in the TAS³ project.

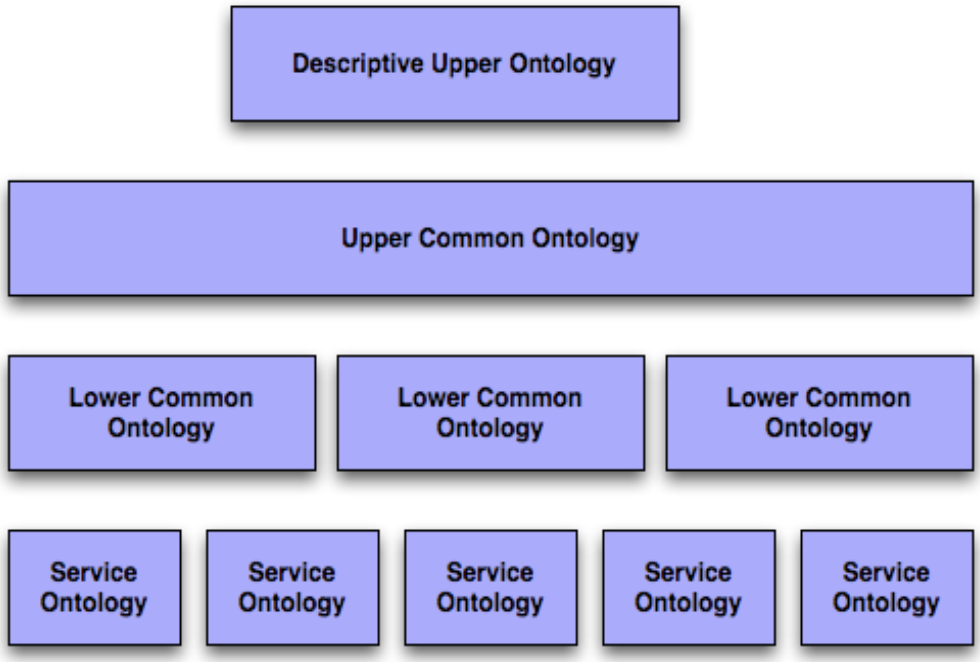

Figure 7.1: Ontology Layers in TAS³.

DOGMA-MESS distinguishes four ontological layers (Figure 7.1), where each lower layer refers to concepts defined in the higher-level ontologies. The Descriptive Upper Ontology (DUO) is a very small theoretical ontology, which defines domain independent concepts and relations (Section 7.1). The Upper Common Ontology (UCO) contains the conceptualizations and semantic constraints that are common to and accepted by a domain. The Lower Common Ontology (LCO) represents the interpretation of the domain from the perspective of an organisation (e.g. Kenteq in TAS³). While the ontology evolves, this layer contains the information that is going to be refined by a core domain expert to be integrated in the UCO. Finally, the lowest layer represents the knowledge specific to a particular application. Note that only DUO and UCO are the focus of this deliverable.

Since ontologies evolve over time, they cannot be produced in one single session, but over multiple sessions each resulting in a more "advanced version". Each version starts from the Upper Common Ontology (UCO), which hold the current insights about a domain of interest. Whenever there is a need to change the current insights, the stakeholders formalize their interpretation in their own Service Ontology (SO), resulting in a divergence of perspectives. In order to

converge these different perspectives, the different common and organizational interests need to be aligned. The alignment is then formalized in a Lower Common Ontology (LCO). The community then decides which parts of the LCO are candidates for a next version of the LCO. An illustration of this process is contained in Figure 7.2.

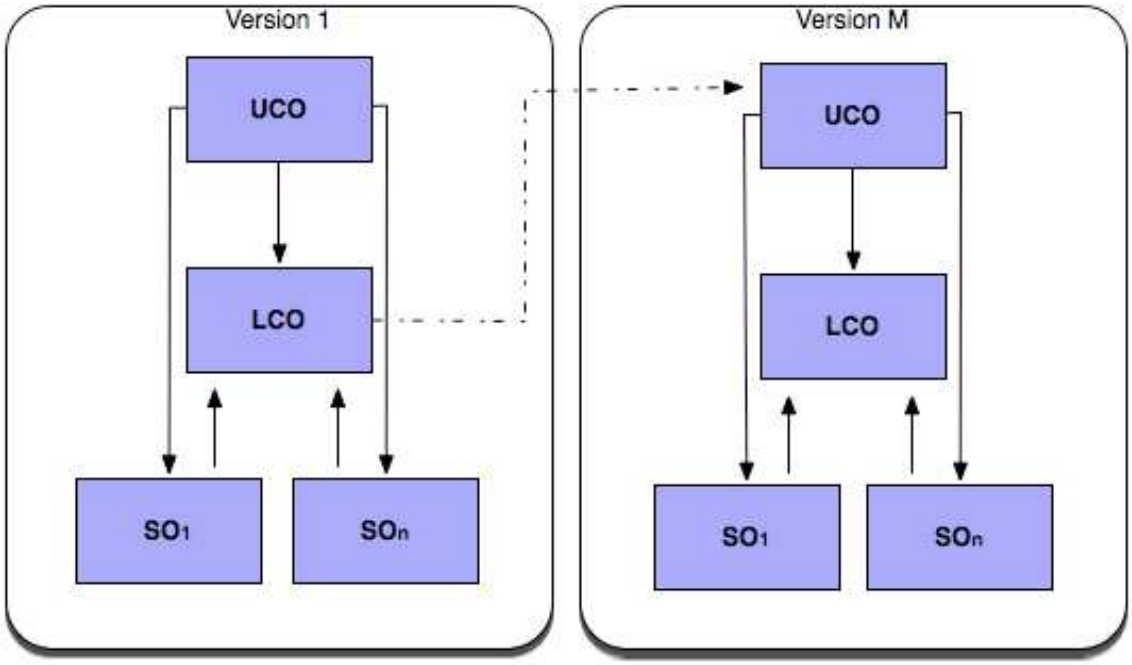

Figure 7.2: Ontology evolution in DOGMA-MESS.

The Upper Common Ontology, the Lower Common Ontology and the Service Ontologies are created using either DOGMA Studio[10*] or Collibra Studio* and stored on the DOGMA Server*. Part of the TAS³ ontologies are available at http://starpc11.vub.ac.be:9999/OBIS/.

7.1 Descriptive 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 [36]. In other words, an upper ontology defines the foundational concepts used in both mid-level and domain ontologies. As a result, mapping between domain ontologies (following the same upper ontology) becomes easier even if they are covering drastically different domains. Many upper ontologies (e.g. SUMO [5], DOLCE [6]) have been proposed over the last decade. However, these have often been criticised as they couldn't be used in every domain.

[10] * Collibra NV/SA has the exclusive right to commercialize this product

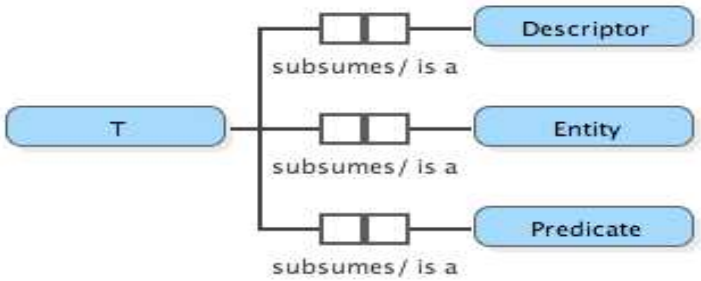

Figure 7.3: DUO Top layer.

Our upper ontology (Figure 7.3) differs from existing upper ontologies in two ways. Firstly, we have grounded the upper ontology in linguistic rather than philosophy. The main advantage of this grounding is that it can easily be understood by domain experts and hence re-used across domains. Secondly, we provide a descriptive framework to capture real world semantics. Thus, the upper ontology can be re-used in a non-restrictive manner. This is possible as the DOGMA ontology framework enables concepts and relationships to be represented within the same hierarchy. In TAS³, the upper ontology will enable the interoperability between the two domains of application (i.e. employability and eHealth) by creating application specific ontologies "under" this upper ontology.

Our main assumption is that the world (or `T`) contains three main concepts, namely `Entity`, `Predicate`, and `Descriptor`. 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`.

7.1.1 Entity

An `Entity` is a thing with distinct and independent existence (Figure 7.4). An `Agent` is a person or thing that takes an active role or produces a specified effect. An `Organism` represents any living thing in the world, while a `System` represents anything (e.g. web services, applications) that can be agent but that is not an organism. 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. For example, a resource (e.g. personal data in TAS³) is a `SporadicObject` as it represents any physical or virtual object of limited availability.

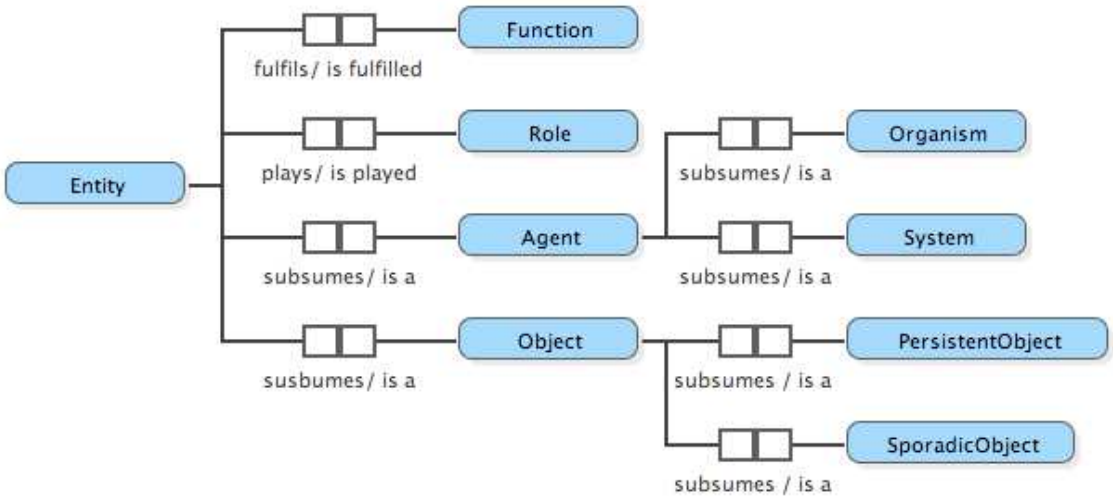

Figure 7.4: Concepts and relations under `Entity`.

7.1.2 Predicate

An `Predicate` represents anything that is happening or being done in time (Figure 7.5). We have also identified three types of activity; namely *event*, *relation* and *perception*. `Event` is the process of doing something to achieve an objective, or of reacting to or against something. For example, a transaction is a type of `Event`, where an exchange is taking place between two entities at a certain time and at a specific location. `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.

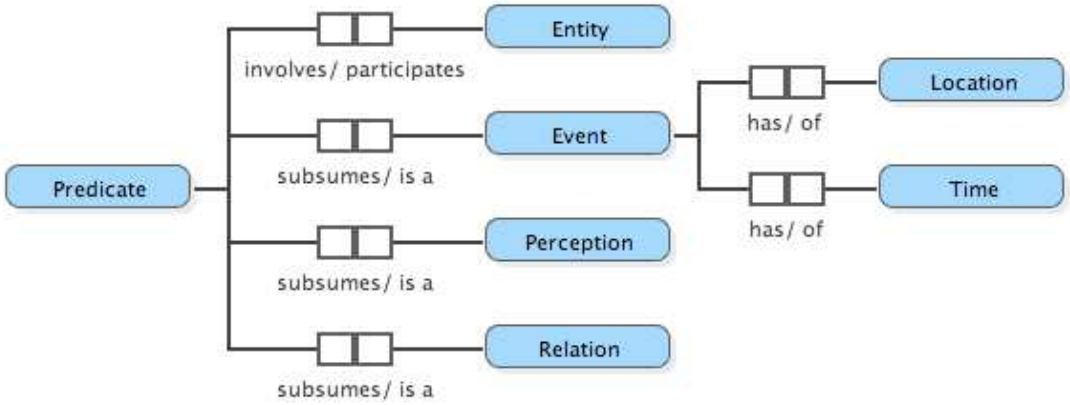

Figure 7.5: Concepts and relations under `Predicate`.

7.1.3 Descriptor

A `Descriptor` is something that is used to describe an object or an agent (Figure 7.6). `Quantity` is a descriptor that is measurable in number, amount, size, or weight. `Time` is the measure associated with time (e.g. minute, hour) characterizing particular events or circumstances. `Context` is the circumstances that form the setting for an event, statement, or idea. `Location` is a context

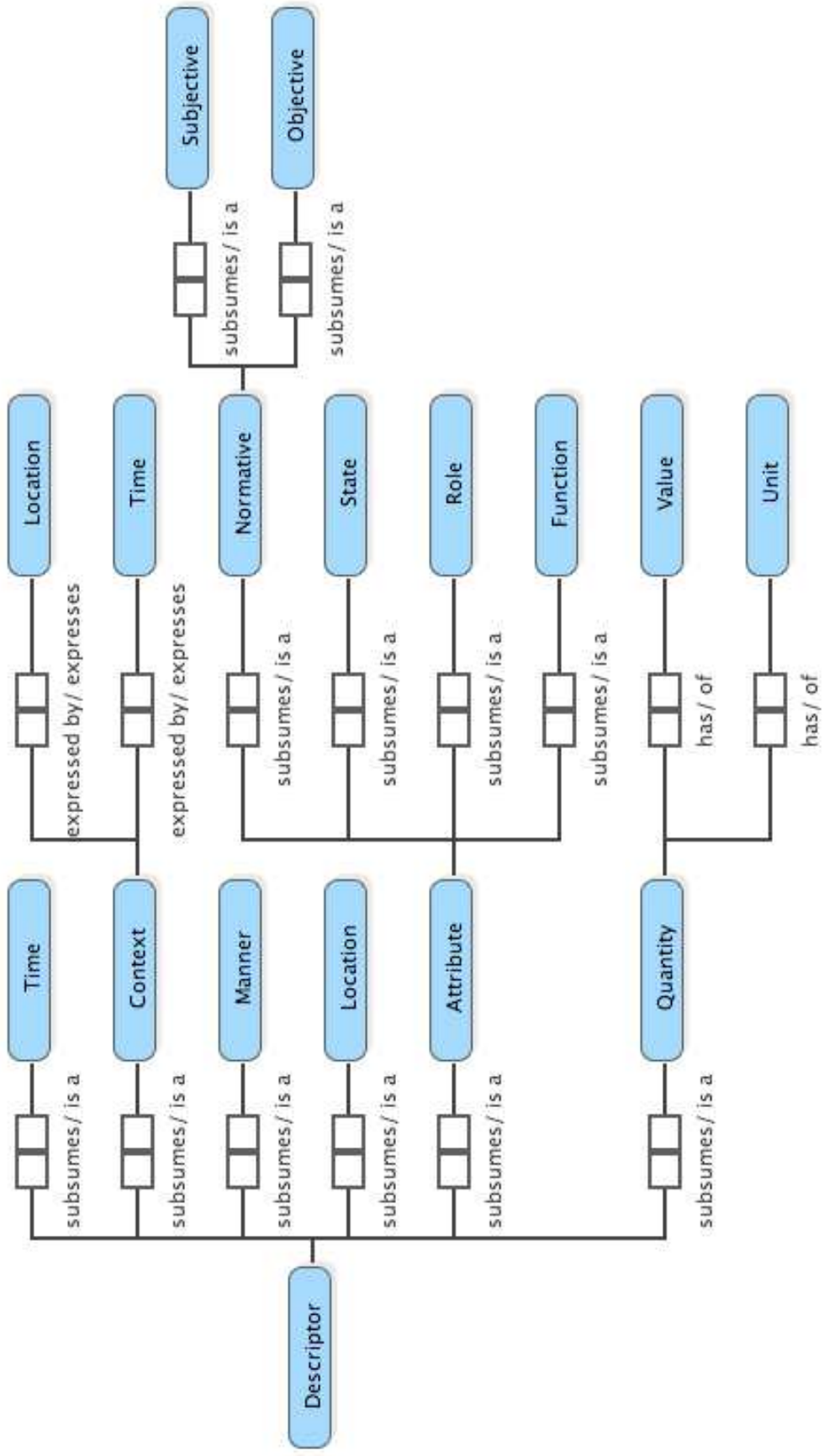

Figure 7.6: Concepts and relations under `Descriptor`.

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.

7.2 TAS³ Upper Common Ontology

The TAS³ Upper Common ontology focuses on representing key concepts in the domain of security and privacy. This section will first describe the concepts related to security before describing the concepts related to privacy and data protection.

7.2.1 Security

ISO/IEC 15408 describes the relations between the main security concepts.

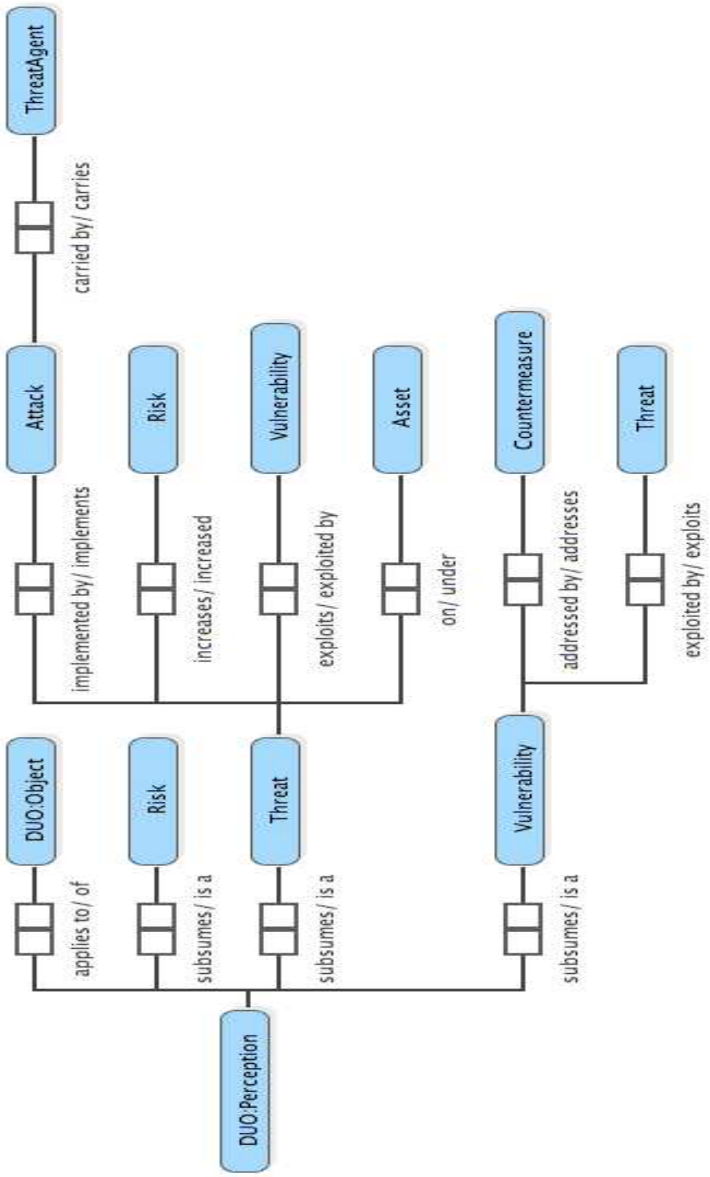

Figure 7.7: Lexon representation of Security.

Figure 7.7 represents the lexon representation of the concepts described in ISO/IEC 15408. For example, the concept of `Vulnerability` is defined as an perception of risk (i.e. `DUO:Perception`), which (i) can be exploited by a threat, and (ii) can be addressed by countermeasures (e.g. authentication policies). Note that residual vulnerabilities may remain despite the implementation of countermeasure.

In the security domain, an asset represents any resources that are valued by their owners (e.g. organization) or by the people described in the resources (Figure 7.8). In TAS³, the service provider considers personal data (e.g. patient records, CVs) as an asset.

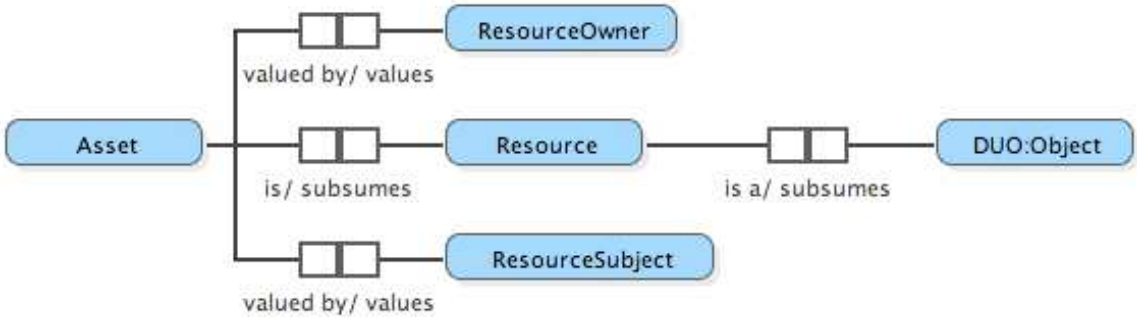

Figure 7.8: Lexon representation of Asset.

7.2.1.1 Security Agent

An agent is a person or thing that takes an active role or produces a specified effect. In security, an agent takes an active role in (i) protecting data, (ii) data loss prevention, and (iii) ensuring that all vulnerabilities have been accounted for. For instance, a system admin plays the role of data custodian and ensures that resources owned by an organisation are protected.

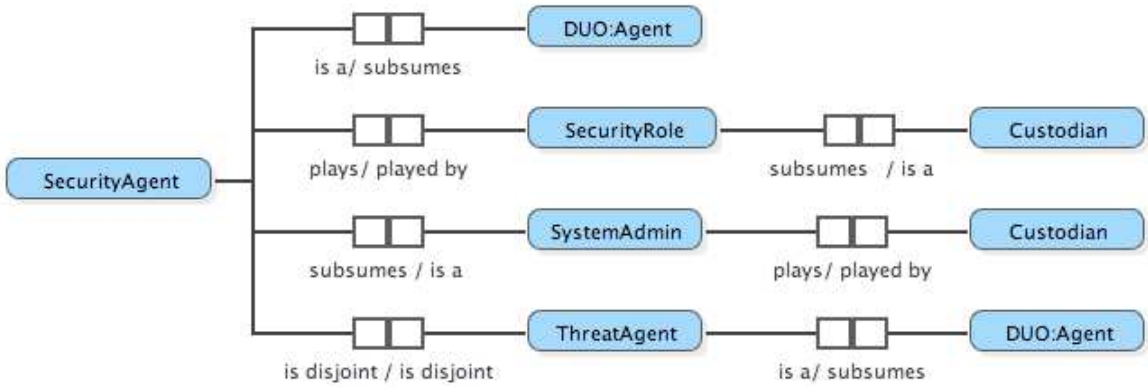

Figure 7.9: Lexon representation of SecurityAgent

Figure 7.9 provides a lexon representation of security agent. Note that a security agent is the opposite of a threat agent whose goal is to abuse resources, and take profit from it.

7.2.1.2 Security Role

A role is a set of connected obligations played by an agent in some contexts. Note that an agent can not only play multiple roles over her lifetime, but also play several roles at the same time.

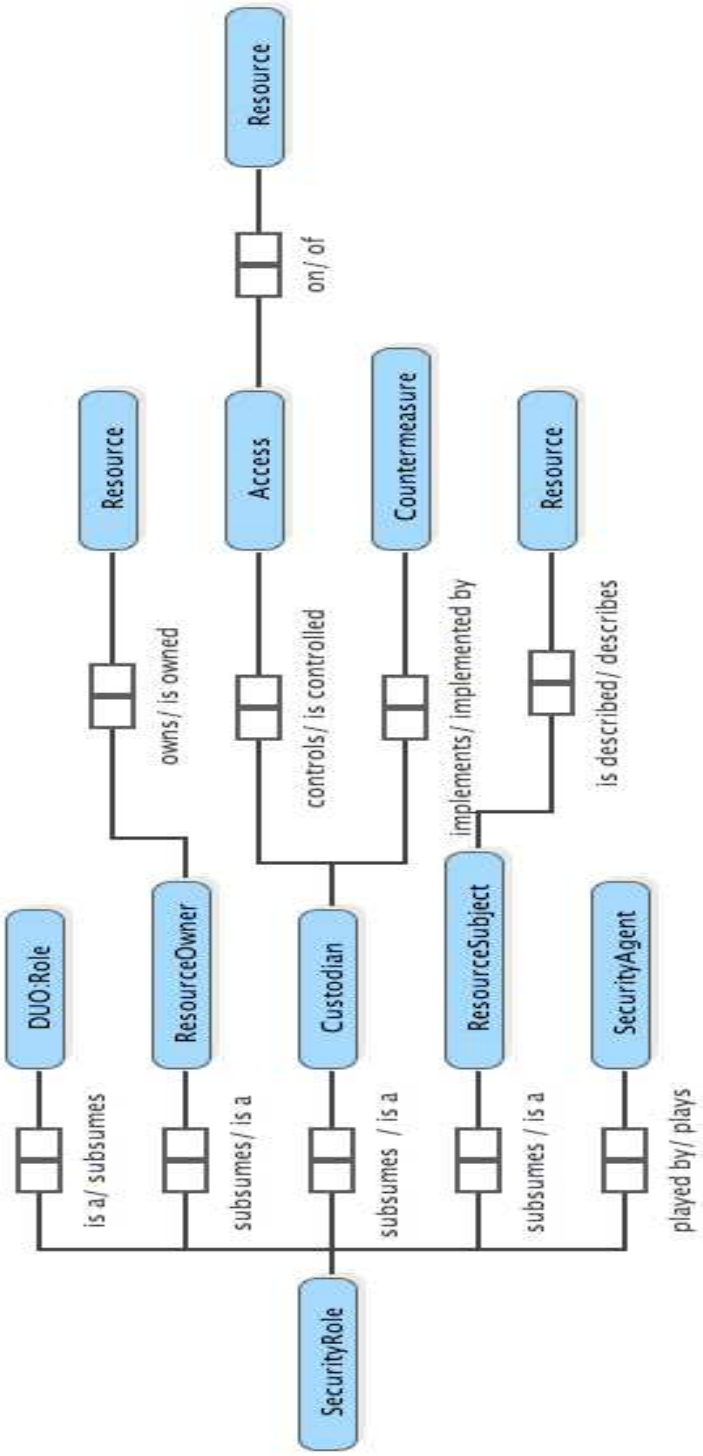

Figure 7.10: Lexon representation of SecurityRole.

A security role is a specific type of role that is played in the domain of security. Figure 7.10 presents three types of security roles; namely the subject of a

resource, the owner of a resource, and the custodian of a resource. A `ResourceSubject` is a security agent that can be identified by the information stored in a resource, while a `ResourceOwner` is an agent, which owns and values a resource. Finally, a `Custodian` is a person that controls the type of actions that can be done on a resource. More specifically, a custodian implements countermeasures to protect the resources owned by an organisation.

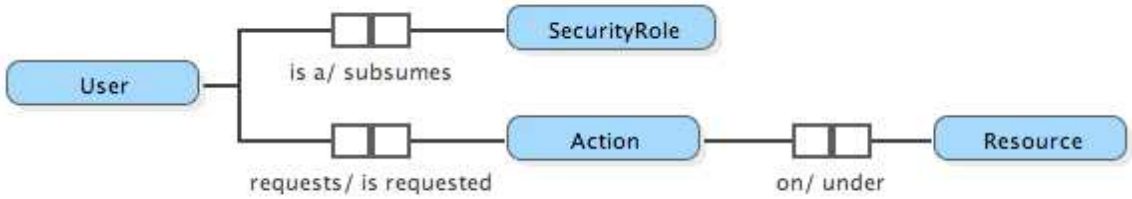

Figure 7.11: Lexon representation of User.

In the security domain, we identify a fourth role that requests to perform some actions on a resource (Figure 7.11). For instance, a doctor is the user of an Electronic Health Record (EHR) system when requesting the access to a specific patient record.

7.2.1.3 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/IEC 17799 [10], and ISO/IEC27001 [11].

Figure 7.12 represents a `SecurityActivity` based on the requirements to be fulfilled to develop a secure information system (see Section 4.2 in ISO/IEC27001). The document identifies four types of activities (i.e. `SecurityAnalysis`, `SecurityImplementation`, `SecurityMonitoring`, and `SecurityMaintenance`) to be carried during the lifecycle of such system. The system designer first needs to identify potential risks and evaluate the vulnerabilities of the system. This is very important as the identified risks and vulnerabilities could be exploited by a threat agent to gain access to data stored in the system. This tasks will lead to a sets of countermeasure to be implemented by a system admin to ensure the security of the system. For instance, a custodian might have defined several security policies controlling the access to resources in the system. The third step is to monitor actual security breach as well as measuring the effectiveness of existing countermeasure (Figure 7.13). The final activity includes the implementation of new countermeasures (if any) resulting from monitoring the system.

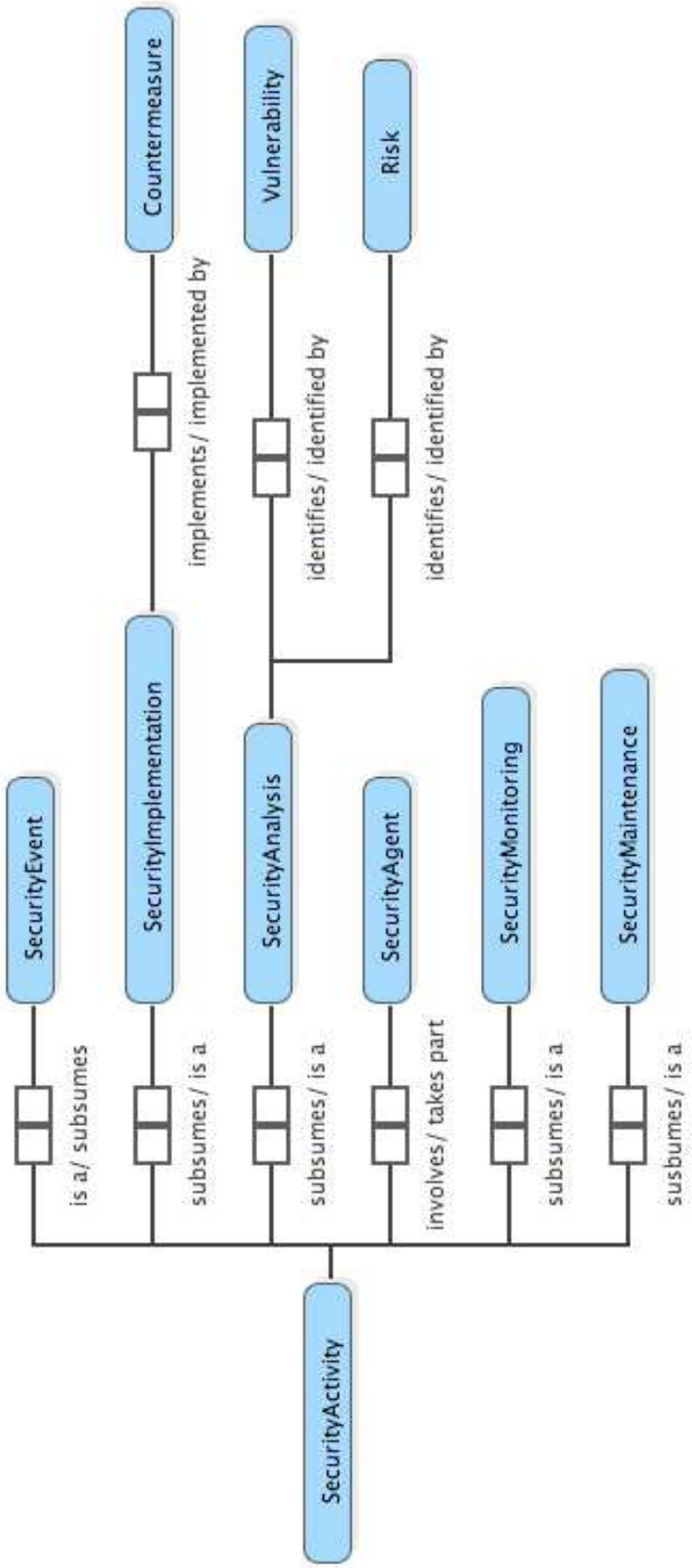

Figure 7.12: Lexon representation of SecurityActivity.

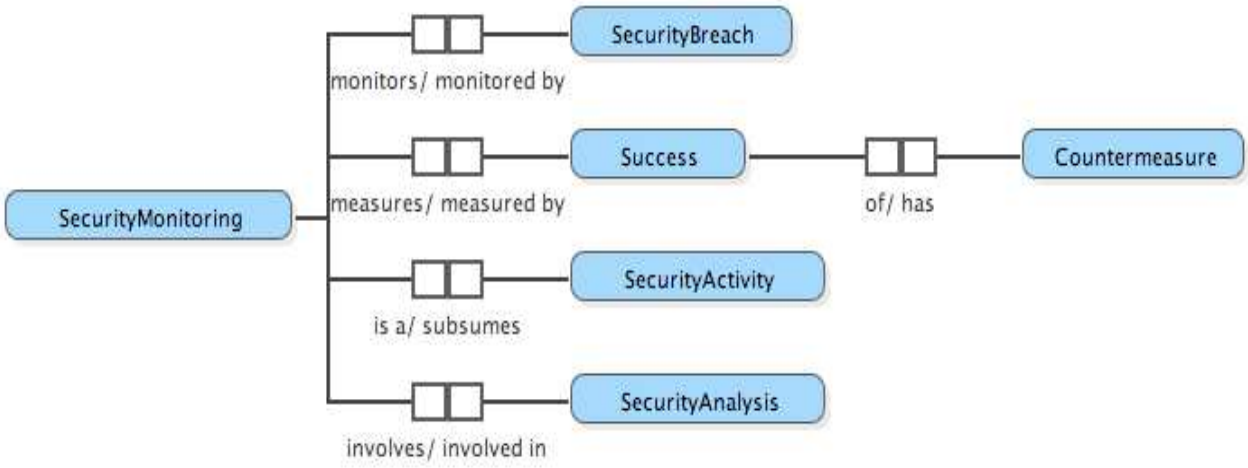

Figure 7.13: Lexon representation of SecurityMonitoring.

7.2.1.4 Risk Assessment

Hafner and Breu [19] define a risk as: "a triplet consisting of a targeted model element, a related security requirement and a threat that potentially undermines the requirement, including an assessment of its severity." In other words, a risk is caused by human errors (i.e. vulnerabilities) or by threat agent attempting to abuse an asset. In TAS³, for example, a risk would arise when an agent is able to modify data (e.g. personal data) to which the agent should not have accessed. Note that security vulnerabilities lead to the loss of availability, confidentiality and/or of integrity of an asset (Figure 7.14).

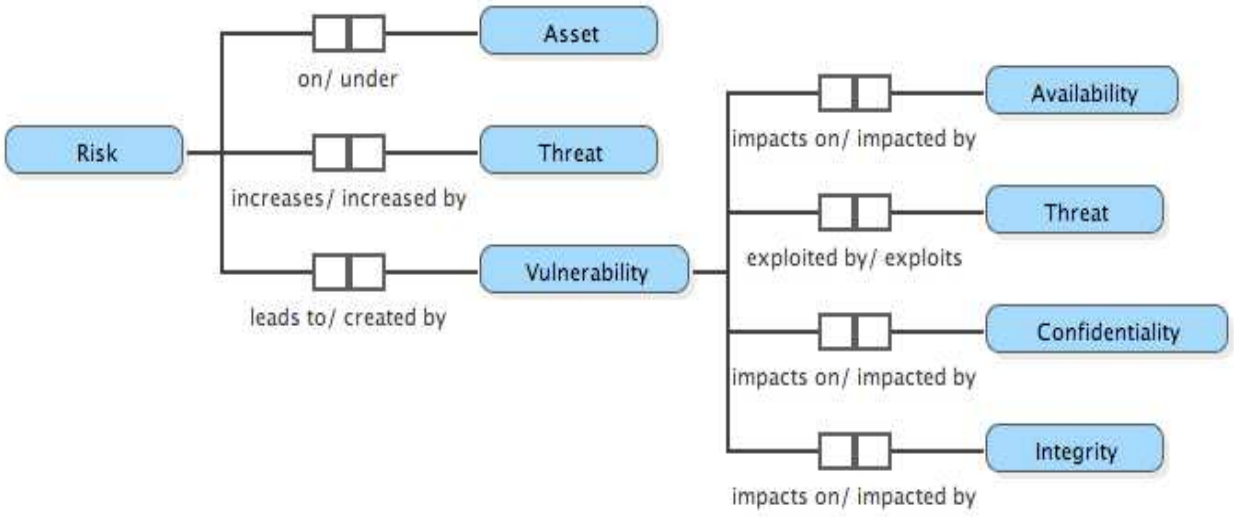

Figure 7.14: Lexon representation of Risk.

ISO/IEC 27001 defines risk assessment as: "*the overall process of risk analysis and risk evaluation*". A risk assessment analysis estimates the risks of threats encountered by an asset (Figure 7.15). The risk assessor analyses the risk based on the vulnerabilities and potential threat poised to an asset, and determines risk treatment to remediate these risks.

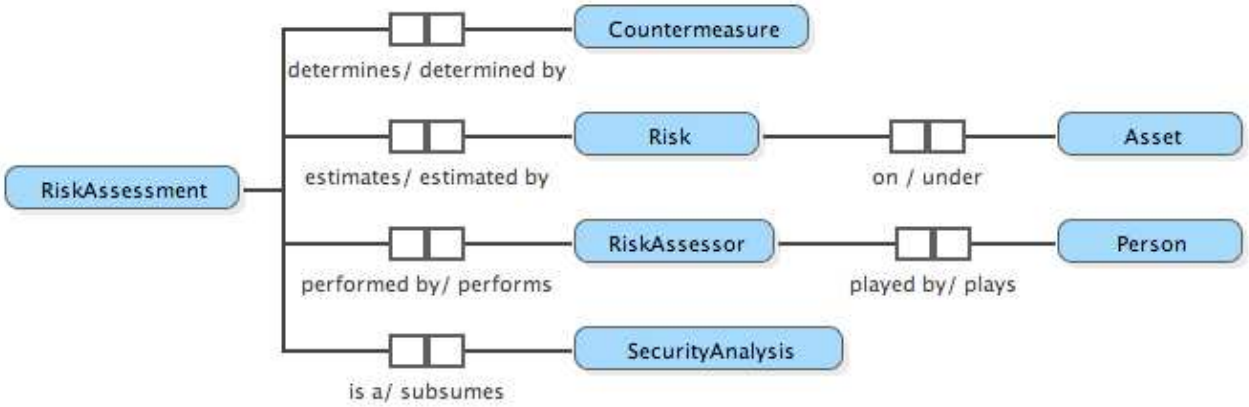

Figure 7.15: Lexon representation of RiskAssessment.

A risk assessment evaluation compares the estimated risks against given criteria to assess the significance of a risk. Note that different organization (and service providers) will have different criteria to measure the impact of risk on asset.

7.2.1.5 Risk Treatment

Risk Treatment is the activity of selecting and implementing measures to alleviate the risk encountered by an asset (Figure 7.16). Possible options for risk treatment include:

- applying appropriate countermeasure to reduce the risks;
- knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;
- avoiding risks by not allowing actions that would cause the risks to occur;
- transferring the associated risks to other parties, e.g. insurers or suppliers.

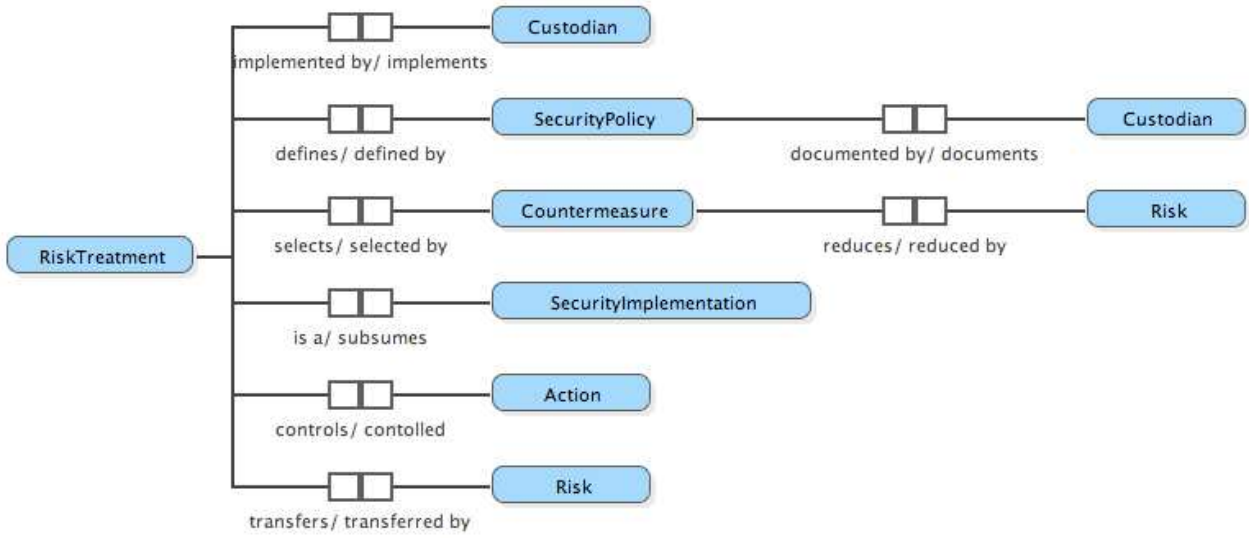

Figure 7.16: Lexon representation of RiskTreatment.

7.2.2 User Data Protection

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data list several basic principles:

- **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 excerpt 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.
- **Accountability Principle**: the use of personal data should be monitored to report and mitigate non-adherence and breaches.
- **Data Exchange Principle**: personal data should remain protected when exchanged across systems and/or countries.

Based on these principles, we were able to extract several lexons describing key concepts, such as `PersonalData`, `DataSubject`, and `DataController`. *Personal data* means any information relating to an identified or identifiable individual (Figure 7.17). 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. In TAS³, personal data can be a patient's medical record (in the eHeath domain) or any data related to his previous employment.

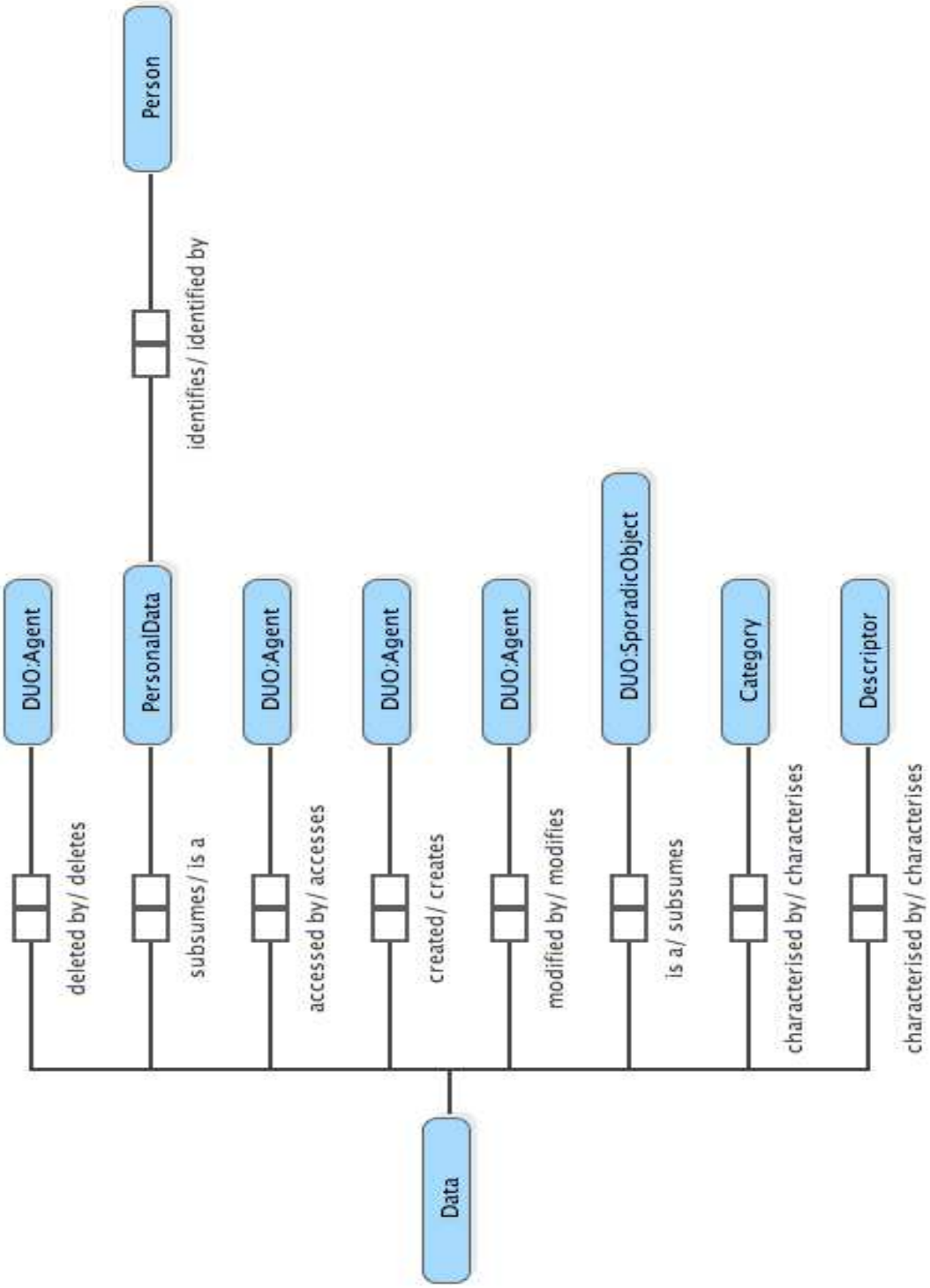

Figure 7.17: Lexon representation of Data.

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. A more extensive list of Lexons is available in Figure 7.18.

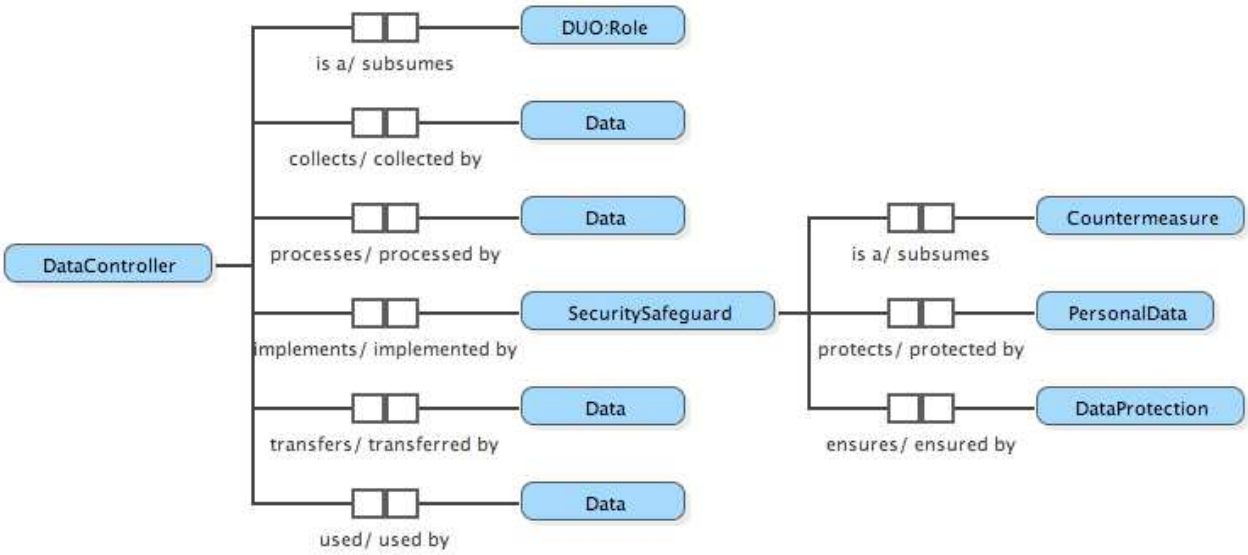

Figure 7.18: Lexon representation of DataController.

8 Integration of Ontologies within TAS3

The integration of ontologies within TAS3 has been done in the context of WP2, WP3 and WP7 around two topics:

- The Use of Ontology for Interoperation (joint work between WP2 and WP7) and
- The Use of Ontology for Creating Secure Business Process Models (joint work between WP2 and WP3).

The two topics are detailed below.

8.1.1 Ontology for Interoperation

Regarding the use of ontologies for interoperation, VUB STARLab and the University of Kent collaborated to integrate the ontologies within the TAS3 Authorization Architecture (see Deliverable D7.1). The integration is presented in Figure 8.1.

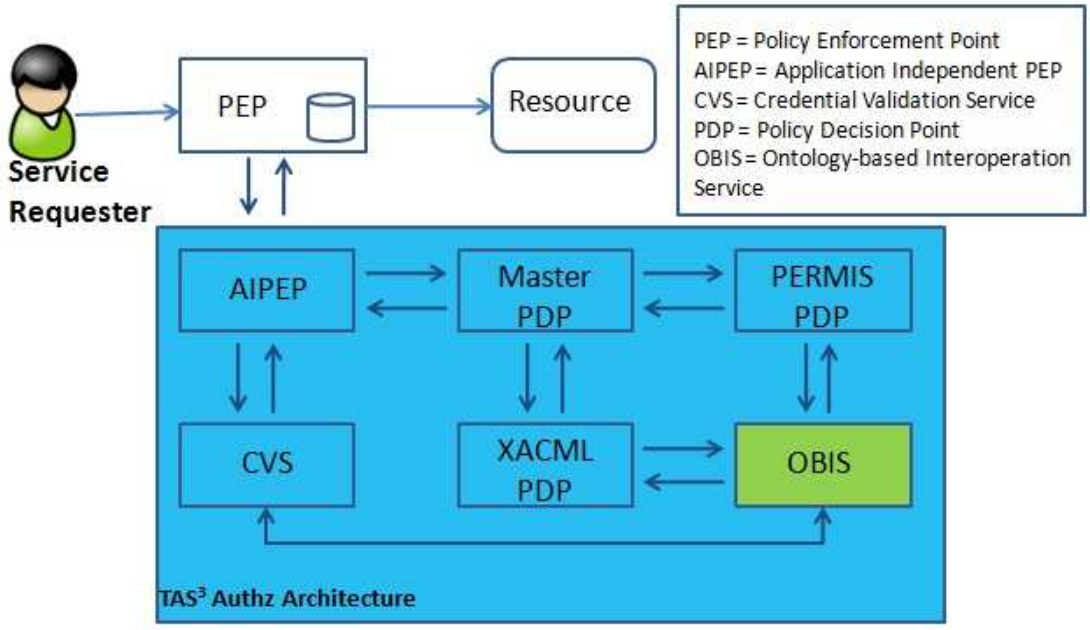

Figure 8.1: Integration of the OBIS within the TAS3 Authorization Architecture.

The Ontology-based Interoperation Service (OBIS), previously named Ontology Mapping Service (OMS), is the service responsible for the cross-organization policy interoperability, presented in Figure 4.2. It is used to determine the similarity between *subjects*, *actions*, and *targets*. More specifically, OBIS will return a relation (i.e. equal, more general, more specific, or I don't know (idk)) between values within the same category. Note that OBIS is now located within the TAS3 Authorization Architecture, but it could be located within other

services, such as trust negotiation service. The role of OBIS in the Authorization Architecture is to determine whether (i) a foreign subject dominates the subject in the authorization policy, (ii) the requested action is dominated by the action in the access control policy and(ii) the resource to be accessed by subject is dominated by the resource (i.e. target) in the security policy.
Figure 8.2 shows how OBIS could be used within the CVS developed by the University of Kent.

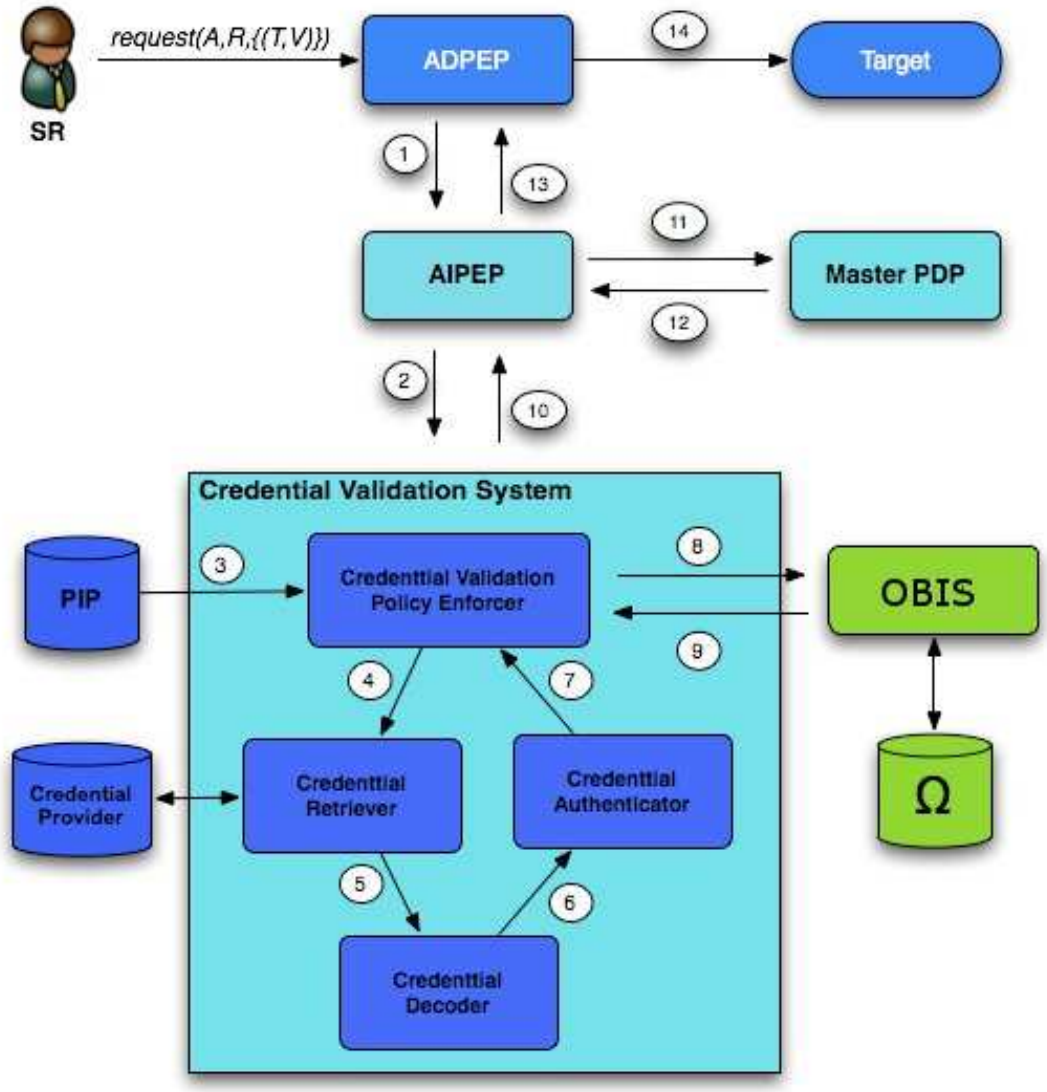

Figure 8.2: The role of OBIS within the Credential Validation System.

The integration and specification of OBIS are introduced in more detail in Deliverable D7.1.

8.1.2 Ontology for Secure Business Process Models

Regarding the use of ontologies for creating Secure Business Process Models, we defined, in collaboration with the University of Karlsruhe, an Ontology Annotator. The Ontology Annotator is intended to assist the business process designer into designing secure business process models. It integrates an ontology of security constraints for business processes and an annotated knowledge base

storing a set of previously defined annotated rules. These rules capture and store the user knowledge for further retrieval and reuse. The annotations on the BPMN level are introduced in the conceptual design of Deliverable D3.1.

The ontology annotator underpins the already existing security constraints annotations by adding semantics on top of them in order to facilitate the user's design decisions in the design phase of the Secure Business Process Models. It is intended to bridge the gap between security annotations and the business process designer through an ontology for security constraints, as shown in Figure 8.3.

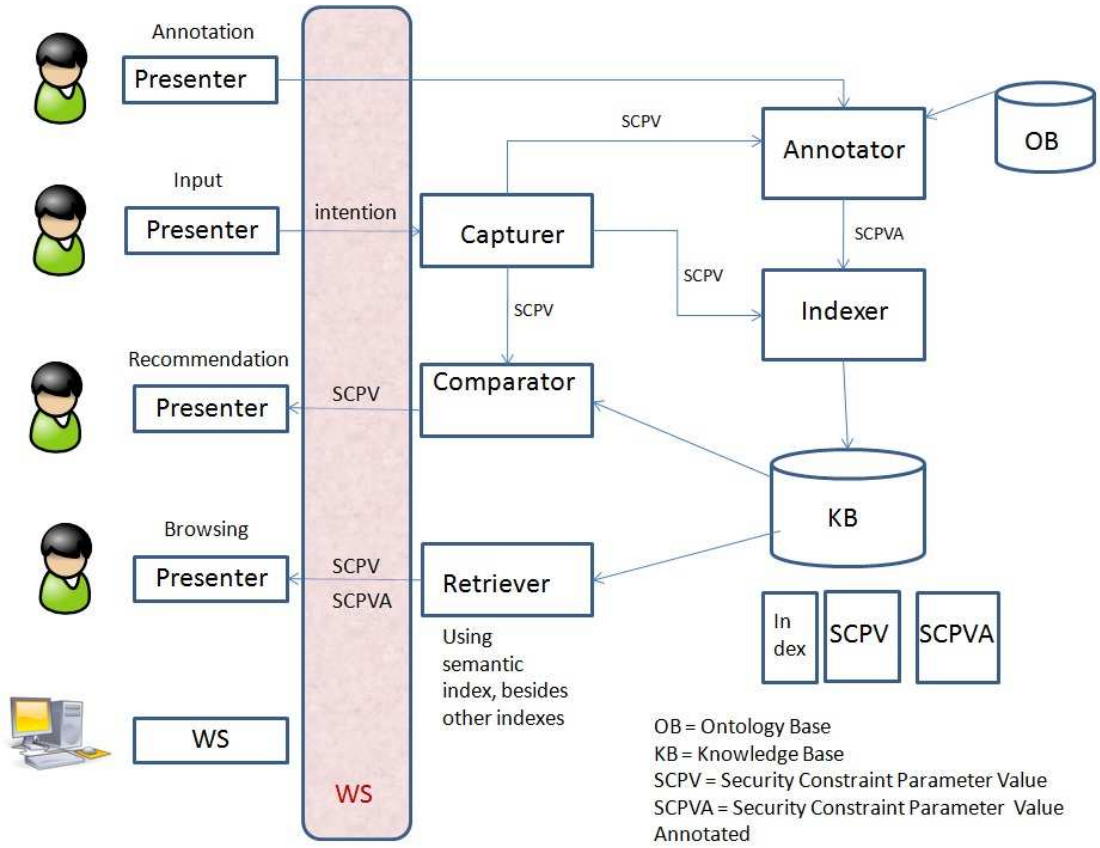

Figure 8.3: Semantic Annotation of Security Constraints with Security Ontology.

This tool is using a Lower Common Ontology of security constraints derived from the UCO presented in this deliverable. The security annotations are further transformed into security constraints, thus enabling security by design in TAS³.

The specification of the Ontology Annotator is described in Deliverable D3.1.

9 Conclusion

As part of this document, we have analysed the scope of an ontology in the TAS³ domain. The ontology is essential to achieve unambiguous and flexible meaning agreement among participants in the TN. The ontology provides a machine-readable documentation of the architecture as well as a formal vehicle to exchange explicit semantic agreements (i.e. commitments) between partners and, eventually, systems. These commitments will enable the enforcement of (organisational and/or legal) policies within the TAS³ architecture. Secondly, the 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.

Initial work into the ontology implementation has focused on the development of a domain-independent upper ontology providing a framework to describe common sense concepts (e.g. `Predicate`, `Entity`). The advantage of this upper ontology compared to existing ones (e.g. SUMO, DOLCE) is that (i) it is grounded in natural language, and (ii) provides a descriptive framework allowing the upper ontology in be re-used in a non-restrictive manner. In addition, we developed an Upper Common Ontology (UCO) covering the TAS³ domain using input from international security standards and data protection regulations. An extensive list of lexons is available in Appendix B and C. The combination of both the descriptive upper ontology and the TAS³ UCO enables its re-use in different application domains (e.g. eHealth and employability). Thus, annotating (web) services with these resources allow the correct semantic interpretation of security paradigms and data protection regulations and increase the trust in the TN.

In future work, we will extend our current work by analyzing and improving the security topics especially with regard to data processing and by introducing concepts related to trust as they emerge from use-cases and further refinement of the requirements.

Our next step is to validate the OBIS service against the eHealth application (PILS, see deliverable D9.1), which is ongoing work within TAS³, and also against other components of the TAS³ architecture (e.g. using OBIS for semantic interoperation in creating secured business processes).

References

[1] T. Berners-Lee, J. Hendler and O. Lasilla (2001). The Semantic Web. In *Scientific American, May*, pages 34-43.

[2] E. Christensen, F. Curbera, G. Meredith, and S. Weerawarana (2001). Web Services Description Language (WSDL) 1.1, *World Wide Web Consortium*. HUhttp://www.w3.org/TR/wsdlU

[3] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Nielsen, S. Thatte, and D. Winer (2000). Simple Object Access Protocol (SOAP) 1.1, *World Wide Web Consortium*. HUhttp://www.w3.org/TR/soap/U

[4] T. Gruber (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.

[5] S. Kellomaki (Eds.) (2009). TAS³ architecture. TAS³ Deliverable D2.1.

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

[7] C. Masolo, S. Borgo, A. Gangemi, N. Guarino, A. Oltramari, and L. Schneider (2003). The WonderWeb Library of Foundational Ontologies Preliminary Report. WonderWeb Deliverable D17.

[8] A. Kim, J. Luo, and M. Kang (2005). Security Ontology for Annotating Resources. In *Proceedings of the 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05)*, page 1483-1499.

[9] V. Raskin, C. Hempelmann, K. Triezenberg, and S. Nirenburg (2001). Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool. In *Proceedings of the 2001 workshop on New security paradigms*, page 53-59.

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

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

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

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

[14] Q. Reul (Eds.) (2009) TAS³ Lower Common Ontology. TAS³ Deliverable D2.3.

[15] J. Mulle (Eds.) (2009) Design of a semantic underpinned, secure & adaptable process management platform. TAS3 Deliverable D3.1.

[16] G. Hodge (2000). Systems of Knowledge Organization for Digital Libraries: Beyond Traditional Authority Files. The Council on Library and Information Resources.

[17] M. van Assem, M. Menken, G. Schreiber, J. Wielemaker, and B. Wielinga (2004). A method for converting thesauri to RDF/OWL. In *Proceedings of the 3rd International Semantic Web Conference (ISWC2004)*, pages 17-31, Hiroshima, Japan.

[18] M. Jarrar, and R. Meersman (2002). Formal Ontology Engineering in the DOGMA Approach. In *Proceedings of the International Conference on Ontologies, Databases and Applications of Semantics (ODBASE 02)*, page 1238-1254.

[19] Bechhofer, S., van Harmelen, F., Hendler, J., Horrocks, I., McGuinness, D. L., Patel-Schneider, P. F., and Stein, L. A. (2004). OWL Web Ontology Language Reference. W3C Recommendation, World Wide Web Consortium. http://www.w3.org/TR/owl-ref/.

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

[21] Institute of Electrical and Electronics Engineers (1990). IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York.

[22] I. Dahn (Eds.) (2009). Software Documentation System: Back Office Services. TAS³ Deliverable D8.2.

[23] M. Hafner, and R. Breu (2009). Security Engineering for Service-Oriented Architecture. Springer-Verlag, Berlin.

[24] OECD Guidelines for the Security of Information Systems and Networks (2002). Towards a Culture of Security. Paris: OECD, HUwww.oecd.orgUH.

[25] B. Claerhout (Eds.) (2009). Pilots Specifications and Use Case Scenarios. TAS³ Deliverable D9.1.

[26] S. Castano, A. Ferrara, S. Montanelli, G.N. Hess, and S. Bruno (2007). State of the art on ontology coordination and matching. Report FP6-027538, BOEMIE.

[27] V. I. Levenshtein (1966). Binary codes capable of correcting deletions, insertions and reversals. Soviet Physics Doklady, 10:707–+.

[28] R. Dieng, and S. Hug (1998). Comparison of "personal ontologies" represented through conceptual graphs. In Proceedings of the 13th European Conference on Artificial Intelligence (ECAI 98), pages 341–345, Brighton, UK.

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

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

[31] R. Meersman (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.

[32] David Fowler, Quentin Reul and Derek Sleeman. IPAS ontology development. In *Proceedings of the 3rd International Workshop on Formal Ontology Meet Industry Workshop (FOMI 2008)*, pages 120-131, 2008.

[33] D. Trog, S. Christiaens, G. Zhao, J. de Laaf (2008). Toward a Community Vision Driven Topical Ontology in Human Resource Management. In *Proceedings of On the Move to Meaningful Internet Systems: OTM2008 Workshops*, page 615-624.

[34] D. Martin, M. Paolucci, S. McIlraith, M. Burstein, D. McDermott, D. McGuiness, B. Parsa, T. Payne, M. Sabou, M. Solanki, N. Srinivasan, and K. Sycara (2004). Bringing Semantics to Web Services: The OWL-S Approach. In the *First International Workshop on Semantic Web Services and Web Process Composition (SWSWPC 2004).*

[35] D. Roman, U. Keller, H. Lausen, J. de Bruijn, R. Lara, M. Stollberg, A. Polleres, C. Feier, C. Bussler, and D. Fensel (2005). Web Service Modeling Ontology. In Applied Ontology, 1, pages 77-106.

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

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

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

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

[40] E. Chang, T. Dillon, and F. Hussain (2006) Trust and Reputation for Service-Oriented Environment: Technologies for Building Business Intelligence and Consumer Confidence. John Wiley & Sons Ltd, England.

Amendment History

Ver	Date	Author	Description/Comments
1.0	2009-01-06	QR	Initial submission to EC for review
1.1	2009-05-20	QR	Revised submission to EC
2.0	2009-11-30	QR	Second iteration of the deliverable

Appendix

Appendix A – Glossary

Abstract Business Process Abstract business processes are partially specified processes that are not intended to be executed. An Abstract Process may hide some of the required concrete operational details. Abstract Processes serve a descriptive role, with more than one possible use case, including observable behavior and process template.

- Source: Quentin (Quentin.Reul@vub.ac.be)

Accessibility Accessibility means any condition, disease or disability that requires special employment measures or is eligible for positive action.

- Source: Ingo (dahn@uni-koblenz.de)

APL See Accreditation of Prior Learning

Accreditation of Prior Learning

- Source: Dries (dries.pruis@kenteq.nl)

Activity An activities an agent wishes to undertake in order to fulfill his/her goals.

- Source: Ingo (dahn@uni-koblenz.de)

Action An operation on a resource.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Address An address is the identifier for a specific termination point and is used for routing to this termination point.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.2091 - Terms and definitions for Next Generation Networks

Affiliation Membership of learned, professional, civic and recreational organisations.

- Source: Ingo (dahn@uni-koblenz.de)

Agent A person (or service) entitled to act on behalf of another.

- Source: Ingo (dahn@uni-koblenz.de)

Anonymity Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behaviour such as user location, frequency of a service usage, and so on.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.1121 (04), 3.2.1

ADPDP See Application Dependent PDP

Application Dependent PDP Apply specific rules that relate to the application roles. Typically communicates with ADPEP, but may also proxy requests in relevant special cases to outside PDPs or gather Information for its decisions from outside, including from Reputation Providers.

- Source: David (d.w.chadwick@KENT.AC.UK)

ADPEP See Application Dependent PEP

Application Dependent PEP Apply specific rules that relate to the application roles. Typically communicates with ADPDP.

- Source: David (d.w.chadwick@KENT.AC.UK)

AIPDP See Application Independent PDP**Application Independent PDP** Application Independent PDP, more properly TAS3 Network PDP or External PDP Aggregator (cf. Architecture: Anatomy of PEP)

- Source: David (d.w.chadwick@KENT.AC.UK)

AIPEP See Application Independent PEP

Application Independent PEP Application Independent PEP, typically communicates with AIPDP
(cf. Architecture: Anatomy of PEP)

- Source: David (d.w.chadwick@KENT.AC.UK)

AP See Asserting Party

Asserting Party *** TBD

Assertion A collection of one or more statements about an entity (e.g. Authentication statement or Authorisation statement).

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: OMA - The Open Mobile Alliance\

Asset Anything that has value to the organization, its business, its operations and its continuity.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.2701 - Security requirements for NGN release 1

Assurance Level A quantitative expression of Authentication Assurance agreed between a Relying Party and an Identity Provider.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

Asymmetric Authentication Method A method of authentication, in which not all authentication information is shared by both entities.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Attribute A distinct characteristic of an object. An object's attributes are said to describe the object. Objects' attributes are often specified in terms of their

physical traits, such as size, shape, weight, and color, etc., for real-world objects. Objects in cyberspace might have attributes describing size, type of encoding, network address, etc.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: WSIA Glossary - Glossary for the OASIS WebService Interactive Applications

(WSIA/WSRP)

AA See Attribute Authority

Attribute Authority Trusted authorities, which assign roles to users. Normally this is also done by the SOA.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

AAPML See Attribute Authority Policy Markup Language

Attribute Authority Policy Markup Language AAPML is a XACML profile designed to allow attribute authorities to specify conditions under which information under management may be used (and possibly modified) by other applications.

- Source: Liberty Alliance Project
- Reference: http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-AAPML-spec

AC See Attribute Certificate

Attribute Certificate Attributes that are certified (digitally signed) by an Attribute Authority as belonging to a particular object. As an analogy, if a PKC corresponds to a passport, an AC corresponds to a visa.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

ACRL See Attribute Certificate Revocation List

Attribute Certificate Revocation List List of revoked ACs issued by and AA.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Attribute Type That component of an attribute which indicates the class of information given by that attribute.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.501 - Information technology - Open Systems Interconnection - The

Directory: Models

Attribute Value A particular instance of the class of information indicated by an attribute type.

- Source: David (d.w.chadwick@KENT.AC.UK)

- Reference: ITU-T X.501 - Information technology - Open Systems Interconnection – The Directory: Models

Audit An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.800 - Security architecture for Open Systems Interconnection for CCITT applications

Audition Aiming at providing only high quality service to the users, the provider of a directory service can be interested in testing that the services asking for registration are of "*good*" quality. For this purpose, the directory could submit the service under registration to a verification step before granting the registration. The implementation of such process with respect to the technical assessment is called Audition (Automatic Model-Based Interface Testing In Open Networks).
- Source: Antonia (antonia.bertolino@isti.cnr.it)

Authenticated Identity A distinguishing identifier of an entity that has been assured through authentication.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Authn See Authentication

Authentication The provision of assurance of the claimed identity of an entity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Authentication Certificate A security certificate that is guaranteed by an authentication authority and that may be used to assure the identity of an entity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Authentication Exchange A sequence of one or more transfers of exchange authentication information (AI) for the purposes of performing an authentication.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Authentication Information Information used to establish the validity of a claimed identity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.800

Authentication Initiator The entity that starts an authentication exchange.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Authentication Insurance A measure of confidence that the security features and architecture of the Identity Management capabilities accurately mediate and enforce the security policies understood between the Relying Party and the Identity Provider.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

Authorisation The granting of rights, which includes the granting of access based on access rights.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.800

Authorization Decision The result of evaluating applicable policy, returned by the PDP to the PEP. A function that evaluates to "Permit", "Deny", "Indeterminate" or "NotApplicable", and (optionally) a set of obligations

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Authoritative In the context of IdM, the Identity Provider which posses the authority under law, contractual agreement, or customary practice to definitively answer queries concerning a specific identity for which it is responsible.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

Authority Number Agents may receive an authority number from a registered authority to be uniquely identified within the authority's jurisdiction or system. Among authority numbers are included: social security numbers, enrollment numbers, etc. An authority number typically consists of a name, a scheme and a code.

- Source: Ingo (dahn@uni-koblenz.de)

Authority Provider A provider of authentication numbers, the uniques of numbers and their meaning are defined by the authority providers jurisdiction or system. Examples are governments, who can supply social security numbers, driving license numbers etc.

- Source: Ingo (dahn@uni-koblenz.de)

Availability Availability is the goal that assets have to be available to authenticated and authorized agents when needed.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Behavioural Factors Aspects of feedback used in define a reputation. For example for a helpdesk one could consider politeness, responsiveness, usefulness of supplied information, etc. These factors may be combined into the reputation differently depending on the needs of the user.

- Source: Sampo (sampo@symlabs.com)

BTM See Behavioural Trust Management

Behavioural Trust Management Class of trust management systems that use information on past performance to build trust. RTM and KPITM are examples.

- Source: Jerry (j.d.hartog@tue.nl)

BGP See Breaking-the-glass Policy

Breaking-the-glass Policy A term used to describe an access control policy that allows users who would not normally have access to a resource, to gain access themselves by "breaking the glass" in the full knowledge that they will have to answer for their actions later to their management.

- Source: David (d.w.chadwick@KENT.AC.UK)

BMO See Business Management Ontology

Business Management Ontology The Business Management Ontology (BMO) represents an integrated information model, which helps to better align IT with business. It brings together business process design, project management, requirements management, and business performance management (in the form of balanced scorecards). As such, it forms the basis for an integrated, vendor-neutral, Business Management Knowledge Base, from which various artifacts can be generated.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Ontology-Based Business Process Management - The Vision Statement

Business Process *** TBD

Business Process Engine The Business Process Engine orchestrates entities that control how FEs and SPs work together to achieve the objectives of the business process.

- Source: Sampo (sampo@symlabs.com)

BPEL See Business Process Execution Language

Business Process Execution Language WS-BPEL provides a language for the specification of Executable and Abstract business processes. By doing so, it extends the Web Services interaction model and enables it to support business transactions. WS-BPEL defines an interoperable integration model that should facilitate the expansion of automated process integration in both the intra-corporate and the business-to-business spaces.

- Source: Jutta (muelle@ipd.uka.de)
- Reference: Web Services Business Process Execution Language Version 2.0

BPEL4People See Business Process Execution Language Extension for People

Business Process Execution Language Extension for People BPEL4People addresses human interactions in BPEL. It defines a new type of basic activity which uses human tasks as an implementation, and allows specifying tasks local to a process or use tasks defined outside of the process definition.

- Source: Jutta (muelle@ipd.uka.de)
- Reference: WS-BPEL Extension for People (BPEL4People), Version 1.0

BPM See Business Process Modelling

Business Process Modelling Using a formal methodology to describe a business process. Such formal model will usually allow some of the configuration details for implementing the business model to be automatically derived.
- Source: Sampo (sampo@symlabs.com)

BPMN See Business Process Modeling Notation

Business Process Modeling Notation The Business Process Modeling Notation (BPMN) is a graphical notation that depicts the steps in a business process. BPMN depicts the end to end flow of a business process. The notation has been specifically designed to coordinate the sequence of processes and the messages that flow between different process participants in a related set of activities.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: http://www.bpmn.org/

BPO See Business Process Ontology

Business Process Ontology *** TBD
- Source: Quentin (Quentin.Reul@vub.ac.be)

Certificate A set of security-relevant data issued by a security authority or a trusted third party, together with security information which is used to provide the integrity and data origin authentication services for the data.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.800 - Security architecture for Open Systems Interconnection for CCITT applications

CA See Certification Authority

Certification Authority Issues digital certificates.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Choreography A choreography description is a multi-party contract that describes from global view point the external observable behavior across multiple clients (which are generally Web Services but not exclusively so) in which external observable behavior is defined as the presence or absence of messages that are exchanged between a Web Service and it's clients.
- Source: Antonia (antonia.bertolino@isti.cnr.it)

CoT See Circle of Trust

Circle of Trust See Trust Network.
- Source: Sampo (sampo@symlabs.com)

Claim An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject, typically an assertion which is disputed or in doubt.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Gang of Identity Commons

Claim Authentication Information Information used by a claimant to generate exchange AI needed to authenticate an entity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Client While general meaning as in "customer" is acknowledged, in protocol contexts "Client" is taken to mean requester of a service. Thus Client is the counter part of a Service Provider. Client is a business entity and quite different from a User. A Service Provider can be a Client towards other entities that it calls.
- Source: Sampo (sampo@symlabs.com)

CARML See Client Attribute Requirements Markup Language

Client Attribute Requirements Markup Language Client Attribute Requirements Markup Language is a specification that allows applications to define their attribute requirements as it relates to identity. CARML can be used to automate configuration of identity attribute services and to expose the set of identity-related data consumed by a specific application or groups of applications.
- Source: Liberty Alliance Project
- Reference: http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-CARML-spec

Competency A competency is a demonstrated ability of a natural person to apply knowledge, skills and attitudes to achieve observable results.
- Source: Ingo (dahn@uni-koblenz.de)

Confidentiality Confidentiality is the goal that data should be readable to agents with appropriate permissions.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Context A property that can be associated with a user attribute value to specify information that can be used to determine the applicability of the value.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.501 - Information technology - Open Systems Interconnection – The Directory: Models

Credential Authentication and Authorization data that can be used to authenticate the claimer is what it claims to be and authorize the claimer's access rights. What AA needs from the SOA to be able to issue ACs.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ETSI TS 132 372 V7.0.0

CTM See Credential based Trust Management

Credential based Trust Management System which builds trust on structural rules which are exchanged in the form of credentials.
- Source: Jerry (j.d.hartog@tue.nl)

Credential Chain A tree (or sequence) of credentials which ensures trustworthiness of the statement in the root credential. Each node is validated by its children and the leaf credentials are issued by trusted entities (e.g. AA).
- Source: Jerry (j.d.hartog@tue.nl)

CIS See Credential Issuing Service

Credential Issuing Service The service of issuing a digitally signed attribute assertions provided by an authoritative source of subject attributes.
- Source: David (d.w.chadwick@KENT.AC.UK)

CVS See Credential Validation Service

Credential Validation Service The service of validating digitally signed attribute assertions and determining which are trusted and which are not.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Data Origin Authentication Corroboration that the source of data received is as claimed.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.800

Data Protection *** TBD
- Source: Joseph (joseph.alhadeff@ORACLE.COM)

DB See Dashboard

Dashboard A web GUI for viewing audit records, work flow status, and/or viewing and manipulating privacy settings and permissions.
- Source: Sampo (sampo@symlabs.com)

DTM See Decentralised Trust Management

Decentralised Trust Management DEPRECATED - See CTM
- Source: Jerry (j.d.hartog@tue.nl)

Decision Request The request by a PEP to a PDP to render an authorization decision.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Delegatee The entity receiving a privilege though a delegation.

Delegation Conveyance of privilege from one entity that holds such privilege, to another entity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.509 (00), 3.3.46 - Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

Delegator The entity that holds and conveys a privilege to another entity though a delegation.

Digital Identity The digital representation of the information known about a specific individual, group or organization
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: CERIAS - Tech Report 2007-17 - Privacy Preserving Multi-factor Authentication with Biometrics

Digital Identity Provider An Agent that issues a Digital Identity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Gang of Identity Commons

Digital Subject An Entity represented or existing in the digital realm which is being described or dealt with.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Gang of Identity Commons

Directed Identity A unifying identity metasystem must support both "omni-directional" identifiers for public entities and "unidirectional" identifiers for private entities
- Source: David (d.w.chadwick@KENT.AC.UK)

Discovery Finding entities/services/objects matching a set of criteria, e.g. Service Discovery.
- Source: Jerry (j.d.hartog@tue.nl)

DNS See Domain Name System

Domain Name System The scheme for attributing alphanumeric, human readable "web addresses". DNS will map the human readable string to an IP address. Sometimes a /etc/hosts file replaces the function of the DNS, but this solution, while allowing more local control, is generally very burdensome to maintain.

Electronic Identity The information about a registered entity, that the Identity Provider has chosen to represent the Identity of that entity. The eID includes a name or an identifier for the entity that is unique within the domain of the Identity Provider.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: TF-AACE - Terena Authentication and Authorisation

Employability *** TBD

- Source: Dries (dries.pruis@kenteq.nl)

Enrolment The process of adding a Permission to an Identity.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Entity Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

Executable Business Process Executable business processes model actual behavior of a participant in a business interaction.
- Source: Quentin (Quentin.Reul@vub.ac.be)

XACML See eXtensible Access Control Markup Language

eXtensible Access Control Markup Language The OASIS Extensible Access Control Markup Language (XACML) TC was chartered "*to define a core schema and corresponding namespace for the expression of authorization policies in XML against objects that are themselves identified in XML. There are many proprietary or application-specific access control policy languages, but this means policies cannot be shared across different applications, and provides little incentive to develop good policy composition tools. XACML enables the use of arbitrary attributes in policies, role-based access control, security labels, time/date-based policies, indexable policies, 'deny' policies, and dynamic policies - all without requiring changes to the applications that use XACML.*"
- Source: OASIS
- Reference: http://xml.coverpages.org/xacml.html

Federation A federation is a collection of realms that have established a producer-consumer relationship whereby one realm can provide authorized access to a resource it manages based on an identity, and possibly associated attributes, that are asserted in another realm. A federation requires trust such that a Relying Party can make a well-informed access control decision based on the credibility of identity and attribute data that is vouched for by another realm.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: FG IdM Use Case WG - ITU-T Focus Group for Identity Management

Federated Identity A single user identity that can be used to access a group of services or applications
that are bounded by the ties and conditions of a federation.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

FIM See Federated Identity Management

Federated Identity Management The communal services provided by a group of organizations, which have set up trust relationships between themselves, so that they can send each other digitally signed attribute assertions about their users' identities in order to grant each others' users access to their resources.

- Source: David (d.w.chadwick@KENT.AC.UK)

FE See Front-end

Front-end In this context, it means web site, i.e. SP

- Source: Sampo (sampo@symlabs.com)

GA See Governing Agreement

Governing Agreement Legal document that every member of Trust Network MUST agree to. This can be seen as the charter of the Trust Network.

- Source: Sampo (sampo@symlabs.com)

Identification The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: SP800 - 47 Appendix D - National Institute for Standards and Technology -Security Guide for Interconnecting Information Technology Systems

Identifier An identifier is a series of digits, characters and symbols or any other form of data used to identify *subscriber(s)*, *user(s)*, network *element(s)*, *function(s)*, network *entity(ies)* providing services/applications, or other entities (e.g., physical or logical objects).

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.2091 - Terms and definitions for Next Generation Networks

Identity An identity is a uniquely identifiable representation of an agent. An agent can have multiple identities that do not necessarily interrelate.

- Source: Ingo (dahn@uni-koblenz.de)

IAF See Identity Assurance Framework

Identity Assurance Framework *** TBD

- Source: Liberty Alliance Project
- Reference: http://www.projectliberty.org/content/download/4315/28869/file/liberty-identity

Identity Agent It manages and supports a consistent user experience (and in some cases other kinds of interactions) with a Service Provider.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: FG IdM Use Case WG - ITU-T Focus Group for Identity Management

Identity Attribute A property of a Digital Subject that may have zero or more values.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Gang of Identity Commons

Identity Availability The availability of an identity gives an indication of the how much an agent can spend on a particular job.
- Source: Ingo (dahn@uni-koblenz.de)

Identity Based Security Policy A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.800 - Security architecture for Open Systems Interconnection for CCITT applications

Identity Context The surrounding environment and circumstances that determine meaning of Digital Identities and the policies and protocols that govern their interactions.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Gang of Identity Commons

IGF See Identity Governance Framework

Identity Governance Framework It is an open initiative to address governance of identity related information across enterprise IT systems. This initiative includes key initial draft specifications contributed by Oracle to the community. These specifications provide a common framework for defining usage policies, attribute requirements, and developer APIs pertaining to the use of identity related information. These enable businesses to ensure full documentation, control, and auditing regarding the use, storage, and propagation of identity-related data across systems and applications.
- Source: Liberty Alliance Project
- Reference: http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-Overview-02

Identity Information All the information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses. Identity information shall take the form of either a SIP URI (see RFC 2396) or a "tel" URI (see RFC 3966).
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ETSI TS 183 007 V1.1.1

Identity Layer An identity layer attempts to develop convergence and interoperability regarding identity, can draw from multiple data stores, selectively exposing, or concealing data and attributes, according to policy.
- Source: David (d.w.chadwick@KENT.AC.UK)

IdM See Identity Management

Identity Management The management by trusted providers of trusted attributes of an entity such as: a subscriber, a device or a provider.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec

IdMAA See Identity Management, Authentication and Authorisation Infrastructure

Identity Management, Authentication and Authorisation Infrastructure Application independent middleware responsible for authenticating and authorizing entities.
- Source: David (d.w.chadwick@KENT.AC.UK)

Identity Pattern A structured expression derived from the behaviour of an entity that contributes to the recognition process; this may include the reputation of the entity. Identity patterns may be uniquely associated with an entity, or a class with which the entity is associated.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: FG IdM Use Case WG - ITU-T Focus Group for Identity Management

IdP See Identity Provider

Identity Provider An entity that specializes in identifying (collecting identity information or PII), and authenticating users. IdP is usually, and in SAML case especially, charged with the role of facilitating Single Sign On (SSO). IdP often with the role of facilitating Single Sign On (SSO). IdP often also conveys PII when authenticating the User. IdP has prime visibility to the usage patterns of a User and is therefore especially vulnerable or in need of special business or administrative protections. IdP function is often associated with ID Service Discover and Token Mapping functions. Core of an IdP is a federation database where mappings between several pseudonymous identities and relationships with the service providers are evident. This database constitutes a fat target when an identity system is attached.
- Source: Sampo (sampo@symlabs.com)

Identity Registration The process of making a person's identity known to the (Personal Identity Verification) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: FIPS 201 App. F

Inactive Status A service is inactive if it needs to use services that are not yet available according to the Registry.

Integrity Integrity is the goal that data and information should not be altered if not explicitly allowed.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

IDL See Interface Description Language

Interface Description Language For example within the standards of the family WS*, WSDL is an IDL.
- Source: Sampo (sampo@symlabs.com)

Interoperability Interoperability is the ability of two or more systems or components to exchange [meaningful] information and to use the information that has been exchanged. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility of use in services outside the direct control of the issuing assigner.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

KPI See Key Performance Indicator

Key Performance Indicator Key Performance Indicators are combinations of different Business Performance factors such as Time to deliver, or number of patent application, etc.
- Source: Sampo (sampo@symlabs.com)

KPITM See Key Performance Indicator Trust Management

Key Performance Indicator Trust Management System which builds trust on economical factors such as performance on delivery times, number of patents filed, etc.
- Source: Jerry (j.d.hartog@tue.nl)

Layer Network A "topological component" that represents the complete set of access groups of the same type which may be associated for the purpose of transferring information.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

LoA See Level of Assurance

Level of Assurance A metric which is used to measure the confidence (or assurance) that a relying party can have, that an authenticated user is really who they say they are. One scale, devised by the US National Institute of Science and Technology, ranges from 1 to 4, with 4 being the highest.
- Source: David (d.w.chadwick@KENT.AC.UK)

LDAP See Lightweight Directory Access Protocol
Lightweight Directory Access Protocol *** TBD
- Source: Jutta (muelle@ipd.uka.de)

LTS See Long Tail Service

Long Tail Service It means that half of the volume of the internet use can be in myriad of low use services (the other half is in few high volume services).
- Source: Sampo (sampo@symlabs.com)

MS See Message Signer

Message Signer Digitally signs request.
- Source: Danny (decockd@esat.kuleuven.be)

MV See Message Verifier

Message Verifier Verifies digital signature and other constraints of a request.
- Source: Danny (decockd@esat.kuleuven.be)

NOC See Network Operation Center

Network Operation Center *** TBD

Non-Repudiation The ability through historical logs and logical analysis to prevent or discourage an Entity from denying that it had acted as an Identity in a given transaction, especially in a legal sense.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Object A well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication and identity management processing.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T X.680 - Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation

Obligation An operation specified in a policy that should be performed by the PEP in conjunction with the enforcement of an authorization decision
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Offline Testing Testing phase that includes the activities that are performed while no user ("paying customer) is using the service. Hence, off-line validation of a system implies that it is tested in one or more artificially evolving environments that simulate possible realb interactions.
- Source: Seda (sguerses@ESAT.KULEUVEN.BE)

Online Testing Testing phase that concerns a set of methodologies, techniques, and tools to monitora system after its deployment in its real working context.
- Source: Seda (sguerses@ESAT.KULEUVEN.BE)

Ontology An ontology is commonly defined as: "a [formal,] explicit specification of a [shared] conceptualization" (Gruber, 1993). 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.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: 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.

Orchestration The process of coordinating the sequence and data flow during (web) services interaction.

- Source: Jutta (muelle@ipd.uka.de)

Owner The registered Entity for an Identity.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Panopticon threat A especially pertinent risk in running a Trust Guarantor is that it may gain excessive knowledge to the operations of the Service Provider members or the Users and their business processes. It can be mitigated by careful division of responsibilities using externally contracted Trusted Third Parties, each of which operates in its own isolated, regulatory scheme.

Pending Status A service is in a pending status if it is registered to a directory service, but has not yet been tested by Audition.

Persistent Existing, and able to be used in services outside the direct control of the issuing assigner, without a stated time limit.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ISO Project 26324 - Digital Object Identifier (DOI) system - ISO TC46/SC9 Working Group 7

PCP See Personal Competency Profile

Personal Competency Profile *** TBD

PDS See Personal Data Store

Personal Data Store *** TBD

- Source: Luk (luk@synergetics.be)

PII See Personally Identifying Information

Personally Identifying Information Information that may allow identifying a User, or impersonation of the User.

- Source: Sampo (sampo@symlabs.com)

PUPPET See Pick UP Performance Evaluation Test-bed

Pick UP Performance Evaluation Test-bed It is an approach for the automatic generation of testbeds to empirically evaluate the QoS characteristics

of a Web Service under development. Specifically, the generation exploits the information about the coordinating scenario, the service description (WSDL) and the specification of the agreed QoS properties.

- Source: Sampo (sampo@symlabs.com)

Policy A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations. May be a component of a policy set.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PAP See Policy Administration Point

Policy Administration Point *** TBD

- Source: David (d.w.chadwick@KENT.AC.UK)

PDP See Policy Decision Point

Policy Decision Point The (application independent) part of an access control system that can answer access control requests with a granted or denied decision.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PEP See Policy Enforcement Point

Policy Enforcement Point The (application dependent) part of an access control system that is responsible for enforcing the authorization decisions returned by the PDP.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PIP See Policy Information Point

Policy Information Point *** TBD

- Source: Sampo (sampo@symlabs.com)

PMS See Policy Management Service

Policy Management Service Handles the management of user policies and 'organization wide' policies. Moreover it will have a functionality to attach policies to a request respectively a response. This is an ongoing task in WP8 under the name of 'Aggregating Policies'.

- Source: Sampo (sampo@symlabs.com)

Principal See Entity.

- Source: Jerry (j.d.hartog@tue.nl)

Privacy *** TBD

- Source: Joseph (joseph.alhadeff@ORACLE.COM)

Privacy Policy A set of rules and practices that specify or regulate how a person or organization collects, processes (uses) and discloses another party's personal data as a result of an interaction.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: W3C Glossary and Dictionary

Private Identifier A Claimed Identifier that is intended to be private information used only the context of the End User's relationship with one or more specific Relying Parties (typically one or a small number). The use of Private Identifiers reduces or eliminates the ability of multiple Relying Parties to do correlation of an End User.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: OpenID

Privilege A right to carry out a particular permission (act) that is assigned to a role with some constraints or conditions. A role is (can be) associated with multiple privileges.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: FG IdM Use Case WG - ITU-T Focus Group for Identity Management

PMI See Privilege Management Infrastructure

Privilege Management Infrastructure A highly scalable infrastructure, based on digitally signed attribute assertions, which allows subjects to be authorised to use the resources of relying parties based on their mutual trust in Attribute Authorities. A component of FIM.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PVS See Privilege Verification Subsystem

Privilege Verification Subsystem Decision Engine consisting of PEP and PDP.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PMF See Process Modelling Framework

Process Modelling Framework *** TBD
- Source: Intalio

Provisioning Automatically providing an Identity with access to a role, resource or service, or automatically changing or removing that access, based on the life cycle of events or work requests or changed attributes.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Pseudonym A fictitious identity that an Entity creates for itself, whereby the Entity can remain pseudonymous, or perhaps even fully anonymous, in certain contexts.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Pseudonymity See Pseudonym.

PKC See Public Key Certificate

Public Key Certificate An electronic document that using a digital signature binds together a public key and an identity. As an analogy, if an AC corresponds to a visa, a PKC corresponds to a passport.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

PKI See Public Key Infrastructure

Public Key Infrastructure A highly scalable infrastructure, based on public key cryptography, which allows subjects to authenticate to relying parties based on their mutual trust in Public Key Certification Authorities (a type of TTP). A component of FIM.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

Public Private Partnership *** TBD
- Source: Luk (luk@synergetics.be)

QoS See Quality Of Service

Quality Of Service *** TBD

RTM See Real-Time Trust Management

Real-Time Trust Management DEPRECATED
- Source: Jerry (j.d.hartog@tue.nl)

Registry *** TBD

RP See Relying Party

Relying Party A Party that makes known through its Agent one or more alternative sets of Claims that it desires or requires, and receives through this same Agent a Digital Identity purportedly including the required Claims from a Digital Identity Provider or other Agent of another Party.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Repository *** TBD

Repudiation Denial by one of the entities involved in a communication of having participated in all or part of the communication
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: X.800 (91), 3.3.44

Reputation The reputation of an entity is the view on that entity based on its past performance. Reputations are computed based on recommendations and on feedback on interaction with the entity.
- Source: Jerry (j.d.hartog@tue.nl)

RTM See Reputation based Trust Management

Reputation based Trust Management System which builds trust on past performance expressed in feedback and recommendation.
- Source: Jerry (j.d.hartog@tue.nl)

PDP-R See Requester Policy Decision Point

Requester Policy Decision Point *** TBD
- Source: David (d.w.chadwick@KENT.AC.UK)

PEP-R See Requester Policy Enforcement Point

Requester Policy Enforcement Point *** TBD
- Source: David (d.w.chadwick@KENT.AC.UK)

Resource Data, service or system component
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

RS See Response Signer

Response Signer Digitally signs request
- Source: Danny (decockd@esat.kuleuven.be)

RV See Response Verifier

Response Verifier Verifies digital signature and other constraints of a response.
- Source: Danny (decockd@esat.kuleuven.be)

Risk A Risk is defined as a triplet consisting of a targeted model element, a related security requirement and a threat that potentially undermines the requirement, including an assessment of its severity. Moreover, every risk is evaluated in the context of the currently implemented security controls.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Role Type of attribute that is typically used to signify the position that someone has in an organisation.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

RBAC See Role Based Access Control

Role Based Access Control A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

S&T See Science and Technology

Science and Technology *** TBD

SAML See Security Assertion Markup Language

Security Assertion Markup Language It is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Security Control A Security Control is any managerial, operational, and/or technical measure or safeguard that has been put in place to mitigate identified risks.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Security Domain A set of elements, a security policy, a security authority and a set of securityrelevant activities in which the elements are managed in accordance with the security policy. The policy will be administered by the security authority. A given security domain may span multiple security zones.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.2701 - Security requirements for NGN release 1

Security Domain Authority A security authority that is responsible for the implementation of a security policy for a security domain.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.810

SO See Security Officer

Security Officer A job function or role at Trust Guarantor. Similar function, with the same name, may also exist at Trusted Third Parties, and Service Providers. Security Officer's job is to on continuing basis verify and validate that the members of a Trust Network adhere to the rules. To do this Security Officer usually operates and monitors automated auditing and systems monitoring tools. If discrepancies are found, or complaints are reported, the Security Officer will investigate manually in more detail. Security Officer also participates in approving new members to the network and in taking disciplinary action, such as removal from the network, against the offenders.

Security Objective A Security Objective describes a general security goal to the system. Security Objectivess in many cases originate in legal requirements and general availability, integrity and confidentiality requirements.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Security Policies A Security Policy realises a specific Security Objective (or a combination thereof). A Security Policy is defined as a statement of what is and what is not allowed.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Security Requirement A Security Requirement is a detailed context-dependent explanation of a Security Objective. It breaks security objectives down in severla more detailed descriptions. The context of a Security Requirement is derived from the model element for which it is defined.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

Semantics Semantics provide a (semi-)formal meaning to concepts in a domain of discourse. It allows computer programs and humans to understand what is meant by a concept.

- Source: Quentin (Quentin.Reul@vub.ac.be)

SoD See Separation of Duties

Separation of Duties A security procedure whereby a high risk task is split into at least two subtasks which have to be carried out by different people.

- Source: David (d.w.chadwick@KENT.AC.UK)

Disco See Service discovery

Service discovery Service discovery, sometimes specifically identity enabled service discovery such as Liberty ID-WSF Discovery Service. Discovery service corresponds to one of the bulletin boards in Danny's "snake" diagram.

- Source: Sampo (sampo@symlabs.com)

SOA See Service Oriented Architecture

Service Oriented Architecture A conglomeration of web services, or in a broader sense any kind of services. SOA paradigm attempts to abstract the services so that they are reusable components that can be composed in different arrangements at will. Parallel to the orchestration, there is identity propagation infrastructure and authorization infrastructure, which in its turn relies on trust infrastructure. Real life SOAs are much less generic and recomposing the components in any reliable way remains a dream.

- Source: Sampo (sampo@symlabs.com)

SP See Service Provider

Service Provider An entity that provides a kind of electronic service to users. In TAS3 context the service is foreseen to be provided over a network, usually the Internet.
- Source: Sampo (sampo@symlabs.com)

PDP-P See Service Provider Policy Decision Point

Service Provider Policy Decision Point *** TBD
- Source: David (d.w.chadwick@KENT.AC.UK)

PEP-P See Service Provider Policy Enforcement Point

Service Provider Policy Enforcement Point *** TBD
- Source: David (d.w.chadwick@KENT.AC.UK)

SPPE See Service Provider Process Engine

Service Provider Process Engine Controlling logic of the Service Provider.
- Source: Danny (decockd@esat.kuleuven.be)

SRPE See Service Requester Process Engine

Service Requester Process Engine Controlling logic of the Client.
- Source: Danny (decockd@esat.kuleuven.be)

STM See Session Trust Management

Session Trust Management System which builds trust from session parameters such as authentication parameters used. Establishing a given LoA is an example of STM.
- Source: Jerry (j.d.hartog@tue.nl)

SOAP See Simple Object Access Protocol

Simple Object Access Protocol SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: http://www.w3.org/TR/soap/

SLO See Single Log-Off

Single Log-Off The converse of SSO, whereby a user is simultaneously logged out of all the services that he is currently logged into via SSO.
- Source: David (d.w.chadwick@KENT.AC.UK)

SSO See Single Sign-On

Single Sign-On The process whereby a user can sequentially gain access to a number of computer services by only providing his login credentials once to the first service he contacts.
- Source: David (d.w.chadwick@KENT.AC.UK)

SoA See Source of Authority
Source of Authority Root of trust, issues ACs and may have subordinate AAs.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

StTM See Structural Trust Management
Structural Trust Management Class of trust management systems which use formally expresses trust facts and relations to establish trust. CTM and STM are examples.
- Source: Jerry (j.d.hartog@tue.nl)

Structural Trust Rules It can be simple trust statements as Provider X is trusted to supply Job Vacancies and the combinations trust relations for example when the party trusted to issue credentials is itself determined by trust rules; Provider X is trusted to supply Job Vacancies if a trusted Accreditation agency certifies them. An Accreditation agency is trusted to certify Providers if it is registered at a national registry and has a good reputation, etc.
- Source: Sampo (sampo@symlabs.com)

Subcontinent *** TBD
- Source: Sampo (sampo@symlabs.com)

Subject An actor who wants to perform an action on a target.

Symmetric Authentication Method A method of authentication in which both entities share common authentication information.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Target A resource on which a subject tries to perform an action.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

TAS3 Trust Network See Trust Network.
- Source: Sampo (sampo@symlabs.com)

Test Driver A dedicated software service that is able to run test suites on a service under test.
- Source: Seda (sguerses@ESAT.KULEUVEN.BE)

Test Storage A dedicated software repository that stores test suites to be used by Audition.
- Source: Seda (sguerses@ESAT.KULEUVEN.BE)

TAXI See Testing by Automatically generated XML Instances

Testing by Automatically generated XML Instances A tool by CNR that generates XML instances from an XML Schema automatically. The methodology is largely inspired by the Category Partition testing technique.
- Source: Antonia (antonia.bertolino@isti.cnr.it)

Threat A threat is the description of an adverse event that is considered as potentially having a negative impact. A Threat by itself is not interesting, but becomes relevant when associated with a targeted model element and a security requirement.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

TTL See Time-To-Live
Time-To-Live Parameter that indicates how long a cache entry is valid. Generally a cache entry will not be re-fetched until TTL expires. This concept is especially used by the DNS.
- Source: Sampo (sampo@symlabs.com)

TLG See Top Level Guarantor

Top Level Guarantor See Trust Guarantor.

Trail A "transport entity" which consists of an associated pair of "unidirectional trails" capable of simultaneously transferring information in opposite directions between their respective inputs and outputs.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

Transmission Media Layer Network A "layer network" which may be media dependent and which is concerned with the transfer of information between transmission media layer network "access points" in support of one or more "path layer networks".
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

Transport The functional process of transferring information between different locations.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

Transport Entity An architectural component which transfers information between its inputs and outputs within a layer network.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

TLS See Transport Layer Security

Transport Layer Security *** TBD
- Source: Sampo (sampo@symlabs.com)

Transport Network The functional resources of the network which conveys user information between locations.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T G.805 - Generic functional architecture of transport networks

Trust Is used to refer to both the subjective notion of trust, i.e. a perceived likelihood that an entity/system will behave/perform as required as well as to a formalization of this notion into a measurable quantity.
- Source: Jerry (j.d.hartog@tue.nl)

TPN See Trust and Privacy Negotiator

Trust and Privacy Negotiator *** TBD

T&S See Trust and Security

Trust and Security DEPRECATED
- Source: Sampo (sampo@symlabs.com)

Trust Consortium Convener See Trust Guarantor.
- Source: Joseph (joseph.alhadeff@ORACLE.COM)

Trust Ecosystem The users, members, suppliers, and stake holders of a Trust Network.
- Source: Sampo (sampo@symlabs.com)

Trust Information Collector A point which gathers feedback information needed to calculate reputations (see also WP2 D2.1 deliverable).
- Source: Sampo (sampo@symlabs.com)

TG See Trust Guarantor

Trust Guarantor Governing entity of a Trust Network. The top level Trusted Third Party that administers the Trust Network.
- Source: Sampo (sampo@symlabs.com)

TM See Trust Management

Trust Management An approach to making decisions about interacting with something or someone we do not completely know. It formalizes the subjective notion of trust into measurable trust levels by quantifying and combining sources of trust such as credentials expressing trust statements by entities, recommendations and feedback on performance, etc.

- Source: Jerry (j.d.hartog@tue.nl)
- Reference: Deliverable TAS3D5.1

Trust Negociation The process whereby two entities negotiate a trusting relationship between themselves, by sharing their credentials that were issued to them by TTPs that both of them trust.

- Source: David (d.w.chadwick@KENT.AC.UK)

TN See Trust Network

Trust Network An online business environment where parties can interact with each other securely. While the network does not warrant hones behaviour of the members in the network, it does ensure that everybody adheres to some basic principles especially in non-repudiation, data security, communications security, and IT security. Thus a Trust Network promotes trust between its members.

- Source: Sampo (sampo@symlabs.com)

Trust Network Domain *** TBD

TO See Trust Operator

Trust Operator See Trust Guarantor.

- Source: Sampo (sampo@symlabs.com)

T-PDP See Trust Policy Decision Point

Trust Policy Decision Point A Policy Decision Point specialised in evaluating trust policies. Will answer authorization request with a granted (trusted) or denied (insufficient trust established) decision by combining different trust management techniques.

- Source: Jerry (j.d.hartog@tue.nl)

Trust Seal A seal awarded by a proprietary company, usually a certification authority, to business web sites to display in an attempt to boost consumer confidence in the site. Seals are often awarded when the web sites purchase SSL certificates from the CA. The seals are usually trademarked or copyrighted to prevent them from being copied illegally.

- Source: David (d.w.chadwick@KENT.AC.UK)

TAS3 See Trusted Architecture for Securely Shared Services

Trusted Architecture for Securely Shared Services EU FP7 Project.

Trusted Entity An entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do.

- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.810

TTP See Trusted Third Party

Trusted Third Party An entity that is technically trusted by the infrastructure to assure correctness of some transaction or relationship. TTP is generally subordinate to Trust Operator, the latter being responsible for the overall oversight.
- Source: Sampo (sampo@symlabs.com)
- Reference: ITU-T Y.IdMsec, X.800, X.810

Trusted Zone From the viewpoint of a NGN provider a security domain where a NGN provider's network elements and systems reside and never communicate directly with customer equipment. The common characteristics of NGN network elements in this domain are that they are under the full control of the related NGN provider, are located in the NGN provider premises (which provides physical security), and they communicate only with elements in the "trusted" domain and with elements in the "trusted-but-vulnerable" domain.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.2701 - Security requirements for NGN release 1

Trustworthiness The amount in which an entity is worthy of being trusted. Is used for both the subjective notion of trust; i.e. is the entity likely to behave as expected and the formalized notion, i.e. has a sufficiently high trust level been established for the entity.
- Source: Jerry (j.d.hartog@tue.nl)

User Human that uses the Trust Network. In Liberty and SAML contexts User is synonymous with Principal.
- Source: Sampo (sampo@symlabs.com)
- Reference: Identity Dictionary

User Identifier Identifiers that represent users in their interactions with other parties. Users may present their identifiers verbally, on paper, on plastic cards, or in any other appropriate manner. Electronic user identifiers are electronically presented over data communication channels by user-operated computing devices (client devices) such as PCs, laptops, mobile phones, and smartcards.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: http://blog.onghome.com/glossary.htm

User Identity A code or string uniquely identifying a user across a multi-user, multi-service infrastructure.

Verification The process of confirming a claimed Identity. For example; any one-to-one precise matching of an identity's registered credentials, such as in a logon or any non-AFIS process. Usually performed in real-time, with a yes/no outcome.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: Identity Dictionary

Verification Authentication Information Information used by a verifier to verify an identity claimed through exchange Authentication Information.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Verifier An entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: ITU-T Y.IdMsec, X.811

Vulnerability A Vulnerability is a flaw in a system's design or its implementation. It is a weakness that might be exploited to cause a sytem to malfunction, ultimately resulting in some harm or loss.
- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: Hafner & Breu, Security Engineeing for Service-Oriented Architectures, Springer, 2009

X.500 Series of computer networking standards covering electronic directory access. Similar to LDAP.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

X.509 A joint standard by the ITU-T, ISO and IEC which describes both PKI and PMI. X.509 public key certificates are ubiquitously used on the web for SSL/TLS communications with web servers.
- Source: David (d.w.chadwick@KENT.AC.UK)
- Reference: PERMIS Glossary

WS See Web Service

Web Service Web Service is SOAP based machine to machine communication. Sometimes specifically Identity enabled web service, e.g. Liberty ID-WSF based WS.
- Source: Sampo (sampo@symlabs.com)

WSC See Web Service Client

Web Service Client See Service Requester.
- Source: Sampo (sampo@symlabs.com)

WSDL See Web Service Description Language

Web Service Description Language WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.

- Source: Quentin (Quentin.Reul@vub.ac.be)
- Reference: http://www.w3.org/TR/wsdl20/

WSP See Web Service Provider

Web Service Provider *** TBD
- Source: Sampo (sampo@symlabs.com)

Workflow *** TBD

Appendix B – Security Lexons

Context	Term1	Role	Co-role	Term2
ISO/IEC 17799 Clause 4.2	Organisation	defines	is-defined	SecurityCriteria
ISO/IEC 27001 Clause 4.3 d),e)	RiskTreatment	is-a	subsumes	SecurityImplementation
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	includes	is-included	IdentifyTreatment
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	includes	is-included	AcceptRisk
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	includes	is-included	AvoidRisk
ISO/IEC 27001 Clause 4.3 f)	RiskTreatment	includes	is-included	TransferRisk
ISO/IEC 27001 Clause 4.3 g)	RiskTreatment	includes	is-included	SelectCtrlObj
ISO/IEC 27001 Clause 4.3 g)	RiskTreatment	includes	is-included	SelectControl
ISO/IEC 17799 Clause 4.2	RiskTreatment	includes	is-included	ApplyControl
ISO/IEC 27001 Clause 4.3 g)	Agent	selects	is-selected	ControlObjective
ISO/IEC 17799 Clause 4.2	Agent	implements	is-implemented	Control
ISO/IEC 17799 Clause 4.2	Control	reduces	is-reduced	Risk
ISO/IEC 17799 Clause 4.2	Control	avoids	is-avoided	Risk
ISO/IEC 27001 Clause 4.3 f)	Control	transfers	is-transferred	Risk
ISO/IEC 27001 Annex A.5	SecurityPolicyCtrl	is-a	subsumes	Control
ISO/IEC 27001 Annex A.5.1.1	SecurityPolicyCtrl	includes	is-included	SecurityPolicyDocument
	SecurityPolicyDocument	contains	is-contained	SecurityPolicy
ISO/IEC 27001 Annex A.5.1.2	SecurityPolicyCtrl	includes	is-included	SecurityPolicyReview
ISO/IEC 27001 Annex A.5.1.1	Agent	documents	is-documented	SecurityPolicy
ISO/IEC 27001 Annex A.6	Control	subsumes	subtypeOf	OrganizationSecurityCtrl
ISO/IEC 27001 Annex A.6.1	OrganizationSecurityCtrl	subsumes	subtypeOf	InternalOrgSecurityCtrl
ISO/IEC 27001 Annex A.6.2	OrganizationSecurityCtrl	subsumes	subtypeOf	ExternalPartiesSecurityCtrl
ISO/IEC 27001 Annex A.6.1	Agent	controls	is-controlled	InternalOrganizaionSecurity
ISO/IEC 27001 Annex A.6.2	Agent	controls	is-controlled	ExternalPartiesSecurity
ISO/IEC 27001 Annex A.7	Control	subsumes	subtypeOf	AssetManagement
ISO/IEC 27001 Annex A.7.1	AssetManagement	comprises	is-comprised	ResponsibilityAssetMgt
ISO/IEC 27001 Annex A.7.2	AssetManagement	comprises	is-comprised	InformationClassification
ISO/IEC 27001 Annex A.7.1	Agent	clarifies	is-clarified	ResponsibilityAssess
ISO/IEC 27001 Annex A.7.2	Agent	classifies	is-classified	Information
ISO/IEC 27001 Annex A.8	Control	subsumes	subtypeOf	HumanResouceSecurity
ISO/IEC 27001 Annex A.8.1	HumanResouceSecurity	comprise	is-comprised	PriorEmploymentSecurity
ISO/IEC 27001 Annex A.8.2	HumanResouceSecurity	comprises	is-comprised	DuringEmploymentSecurity
ISO/IEC 27001 Annex A.8.3	HumanResouceSecurity	comprises	is-comprised	TerminationEmplSecurity
ISO/IEC 27001 Annex A.8.1	Agent	ensures	is-ensured	PriorEmployment
ISO/IEC 27001 Annex A.8.2	Agent	ensures	is-ensured	DuringEmployment
ISO/IEC 27001 Annex A.8.3	Agent	ensures	is-ensured	TerminationEmployment

ISO/IEC 27001 Annex A.9	Control	subsumes	subtypeOf	PhysicalEnvironmentSec
ISO/IEC 27001 Annex A.9.1	PhysicalEnvironmentSec	comprises	is-comprised	SecureAreas
ISO/IEC 27001 Annex A.9.2	PhysicalEnvironmentSec	comprises	is-comprised	EquipmentSecurity
ISO/IEC 27001 Annex A.9.1	Agent	ensures	is-ensured	SecureArea
ISO/IEC 27001 Annex A.9.2	Agent	ensures	is-ensured	SecureEquipment
ISO/IEC 27001 Annex A.10	Control	subsumes	subtypeOf	CommunicationOpMgt
ISO/IEC 27001 Annex A.10.1	CommunicationOpMgt	comprises	is-comprised	OperationalProcedureResponsibilityMgt
ISO/IEC 27001 Annex A.10.2	CommunicationOpMgt	comprises	is-comprised	ThirdPartyServiceDeliveryMgt
ISO/IEC 27001 Annex A.10.3	CommunicationOpMgt	comprises	is-comprised	SystemPlanningAcceptance
ISO/IEC 27001 Annex A.10.4	CommunicationOpMgt	comprises	is-comprised	ProtectionAgainstMaliciousMobileCode
ISO/IEC 27001 Annex A.10.5	CommunicationOpMgt	comprises	is-comprised	Backup
ISO/IEC 27001 Annex A.10.6	CommunicationOpMgt	comprises	is-comprised	NetworkSecurityMgt
ISO/IEC 27001 Annex A.10.7	CommunicationOpMgt	comprises	is-comprised	MediaHandlingMgt
ISO/IEC 27001 Annex A.10.8	CommunicationOpMgt	comprises	is-comprised	ExchangeInformationMgt
ISO/IEC 27001 Annex A.10.9	CommunicationOpMgt	comprises	is-comprised	E_CommerceSecurity
ISO/IEC 27001 Annex A.10.10	CommunicationOpMgt	comprises	is-comprised	MonitoringInformation
ISO/IEC 27001 Annex A.10.1	Agent	clarifies	is-clarified	OperationProcedureResponsibility
ISO/IEC 27001 Annex A.10.2	Agent	ensures	is-ensured	ThirdPartyServiceDelivery
ISO/IEC 27001 Annex A.10.3	Agent	performs	is-performed	SystemPlanningAcceptance
ISO/IEC 27001 Annex A.10.4	Agent	against		MaliciousMobileCode
ISO/IEC 27001 Annex A.10.5	Agent	performs	is-performed	Backup
ISO/IEC 27001 Annex A.10.6	Agent	ensures	is-ensured	NetworkSecurity
ISO/IEC 27001 Annex A.10.7	Agent	ensures	is-ensured	MediaHandling
ISO/IEC 27001 Annex A.10.8	Agent	ensures	is-ensured	ExchangeInformation
ISO/IEC 27001 Annex A.10.9	Agent	ensures	is-ensured	E_Commerce
ISO/IEC 27001 Annex A.10.10	Agent	monitors	is-monitored	Information
ISO/IEC 27001 Annex A.11	Control	subsume	subtypeOf	AccessControl
ISO/IEC 27001 Annex A.11.1	AccessControl	comprises	is-comprised	ClarifyAccessControlPolicy
ISO/IEC 27001 Annex A.11.2	AccessControl	comprises	is-comprised	UserAccessMgt
ISO/IEC 27001 Annex A.11.3	AccessControl	comprises	is-comprised	ClarifyUserResponsibilities
ISO/IEC 27001 Annex A.11.4	AccessControl	comprises	is-comprised	NetworkAccessCtrl
ISO/IEC 27001 Annex A.11.5	AccessControl	comprises	is-comprised	OperatingSystemAccessCtrl
ISO/IEC 27001 Annex A.11.6	AccessControl	comprises	is-comprised	ApplicationInfoAccessCtrl
ISO/IEC 27001 Annex A.11.7	AccessControl	comprises	is-comprised	MobileCompTeleworking
ISO/IEC 27001 Annex A.11.1	Agent	clarifies	is-clarified	AccessControlPolicy
ISO/IEC 27001 Annex A.11.2	Agent	manages	is-managed	UserAccess
ISO/IEC 27001 Annex A.11.3	Agent	clarifies	is-clarified	UserResponsibilities
ISO/IEC 27001 Annex A.11.4	Agent	manages	is-managed	NetworkAccess

ISO/IEC 27001 Annex A.11.5	Agent	manages	is-managed	OperatingSystemAccess
ISO/IEC 27001 Annex A.11.6	Agent	manages	is-managed	ApplicationInfoAccess
ISO/IEC 27001 Annex A.11.7	Agent	ensures	is-ensured	MobileCompTeleworking
ISO/IEC 27001 Annex A.12	Control	subsumes	subtypeOf	InfoSysAcquistionDvtMain
ISO/IEC 27001 Annex A.12.1	InfoSysAcquistionDvtMain	comprises	is-comprised	ClarifyInformationSystemSecurityRequirements
ISO/IEC 27001 Annex A.12.2	InfoSysAcquistionDvtMain	comprises	is-comprised	ApplicationCorrectProcess
ISO/IEC 27001 Annex A.12.3	InfoSysAcquistionDvtMain	comprises	is-comprised	CryptographicCtrl
ISO/IEC 27001 Annex A.12.4	InfoSysAcquistionDvtMain	comprises	is-comprised	SystemFilesSecurity
ISO/IEC 27001 Annex A.12.5	InfoSysAcquistionDvtMain	comprises	is-comprised	DvtSupportProcessSecurity
ISO/IEC 27001 Annex A.12.6	InfoSysAcquistionDvtMain	comprises	is-comprised	TechnicalVulnerabilityMgt
ISO/IEC 27001 Annex A.12.1	Agent	clarifies	is-clarified	InformationSystemSecurityRequirements
ISO/IEC 27001 Annex A.12.2	Agent	ensures	is-ensured	SecureApplicationProcess
ISO/IEC 27001 Annex A.12.3	Agent	adopts	is-adopted	Cryptography
ISO/IEC 27001 Annex A.12.4	Agent	ensures	is-ensured	SystemFiles
ISO/IEC 27001 Annex A.12.5	Agent	ensures	is-ensured	DvtSupportProcess
ISO/IEC 27001 Annex A.12.6	Agent	manages	is-managed	TechnicalVulnerability
ISO/IEC 27001 Annex A.13	Control	subsumes	subtypeOf	SecurityIncidentMgt
ISO/IEC 27001 Annex A.13.1	SecurityIncidentMgt	comprises	is-comprised	EventWeaknessesReport
ISO/IEC 27001 Annex A.13.2	SecurityIncidentMgt	comprises	is-comprised	IncidentImprovementMgt
ISO/IEC 27001 Annex A.13.1	Agent	reports	is-reported	EventWeakness
ISO/IEC 27001 Annex A.13.2	Agent	improves	is-improved	IncidentManagement
ISO/IEC 27001 Annex A.14	Control	subsumes	subtypeOf	BusinessContinuityMgt
ISO/IEC 27001 Annex A.14	Agent	ensures	is-ensured	BusinessContinuity
ISO/IEC 27001 Annex A.15	Control	subsumes	subtypeOf	Compliance
ISO/IEC 27001 Annex A.15.1	Compliance	comprises	is-comprised	LegalCompliance
ISO/IEC 27001 Annex A.15.2	Compliance	comprises	is-comprised	PolicyStandardCompliance
ISO/IEC 27001 Annex A.15.3	Compliance	comprises	is-comprised	EnsureAuditEffectiveness
ISO/IEC 27001 Annex A.15.1	Agent	ensures	is-ensured	Legalrequirement
ISO/IEC 27001 Annex A.15.2	Agent	ensures	is-ensured	PolicyStandard
ISO/IEC 27001 Annex A.15.3	Agent	ensured	is-ensured	AuditEffectiveness
ISO/IEC 27001 Annex A.11.4.1	NetworkSecurityMgt	comprises	is-comprised	ClarifyNetworkServicesPolicy
ISO/IEC 27001 Annex A.11.4.2	NetworkSecurityMgt	comprises	is-comprised	UserAuthentication
ISO/IEC 27001 Annex A.11.4.3	NetworkSecurityMgt	comprises	is-comprised	EquipementIdentificaion
ISO/IEC 27001 Annex A.11.4.4	NetworkSecurityMgt	comprises	is-comprised	RemoteDiagnosticConfigurationPortProtection
ISO/IEC 27001 Annex A.11.4.5	NetworkSecurityMgt	comprises	is-comprised	NetworkSegregation
ISO/IEC 27001 Annex A.11.4.6	NetworkSecurityMgt	comprises	is-comprised	NetworkConnectionCtrl
ISO/IEC 27001 Annex A.11.4.7	NetworkSecurityMgt	comprises	is-comprised	NetworkRoutingCtrl
ISO/IEC 27001 Annex A.11.4.1	Agent	clarifies	is-clarified	NetworkServicesPolicy

ISO/IEC 27001 Annex A.11.4.4	Agent	performs	is-performed	RemoteDiagnosticConfigurationPortProtection
ISO/IEC 27001 Annex A.11.4.5	Agent	separates		Network
ISO/IEC 27001 Annex A.11.4.6	Agent	manages		NetworkConnection
ISO/IEC 27001 Annex A.11.4.7	Agent	manages		NetworkRouting
ISO/IEC 27001 Annex A.11.5.1	OperatingSystemAccessCtrl	comprises	is-comprised	LogOnProcedure
ISO/IEC 27001 Annex A.11.5.2	OperatingSystemAccessCtrl	comprises	is-comprised	UserIdentificationAuthentication
ISO/IEC 27001 Annex A.11.5.3	OperatingSystemAccessCtrl	comprises	is-comprised	PasswordManagement
ISO/IEC 27001 Annex A.11.5.4	OperatingSystemAccessCtrl	comprises	is-comprised	SystemUtilitiesUse
ISO/IEC 27001 Annex A.11.5.5	OperatingSystemAccessCtrl	comprises	is-comprised	SessionTimeOut
ISO/IEC 27001 Annex A.11.5.6	OperatingSystemAccessCtrl	comprises	is-comprised	ConnectionTimeLimitation
ISO/IEC 27001 Annex A.11.5.1	Agent	clarifies		LogOnProcedure
ISO/IEC 27001 Annex A.11.5.2	Agent	identifies	is-identified	UserToOS
ISO/IEC 27001 Annex A.11.5.2	Agent	authenticate		UserToOS
ISO/IEC 27001 Annex A.11.5.3	Agent	manages		Password
ISO/IEC 27001 Annex A.11.5.4	Agent	uses		SystemUtilities
ISO/IEC 27001 Annex A.11.5.5	Agent	timeOut		Session
ISO/IEC 27001 Annex A.11.5.6	Agent	limits		ConnectionTime

Table 1: List of risk treatment lexons.

Appendix C – Data Protection Lexons

Context	Term1	Role	Co-role	Term2
OECD data protection Guideline	Process	fulfils	fulfilledBy	Purpose
OECD data protection Guideline	Process	characterisedBy	of	Time
OECD data protection Guideline	Process	characterisedBy	of	Purpose
OECD data protection Guideline	Process	characterisedBy	of	Context
OECD data protection Guideline	Process	characterisedBy	of	Manner
OECD data protection Guideline	Process	characterisedBy	of	Means
OECD data protection Guideline	Process	subsumes	is-a	Collect
OECD data protection Guideline	Process	subsumes	is-a	Store
OECD data protection Guideline	Process	subsumes	is-a	Disseminate
OECD data protection Guideline	Process	subsumes	is-a	Transfer
OECD data protection Guideline	Process	subsumes	is-a	Use
OECD data protection Guideline	Process	subsumes	is-a	SecuritySafeguard
OECD data protection Guideline	Process	endangers	endangeredBy	Privacy
OECD data protection Guideline	Process	endangers	endangeredBy	Liberty
OECD data protection Guideline	Manner	characterisedBy	of	Attribute
OECD data protection Guideline	Manner	subsumes	is-a	Means
OECD data protection Guideline	Attribute	subsumes	is-a	Fairness
OECD data protection Guideline	Attribute	subsumes	is-a	Lawfulness
OECD data protection Guideline	Attribute	subsumes	is-a	Appropriateness
OECD data protection Guideline	Attribute	subsumes	is-a	Accuracy
OECD data protection Guideline	Attribute	subsumes	is-a	Completeness
OECD data protection Guideline	Attribute	subsumes	is-a	Relevence
OECD data protection Guideline	Attribute	subsumes	is-a	Necessity

Table 1: List of data protection lexons.