

Universitat Politècnica de Catalunya
Departament de Llenguatges i Sistemes Informàtics
Master in Computing

MASTER THESIS

**Modeling and exploiting Security
and Trust using Semantic
Technologies**

Student Ana Ballester Funes
Advisor Francisco Jordan Fernández
Ponent Alberto Abelló Gamazo
Date 08/09/09

TÍTULO	Modeling and exploiting Security and Trust using Semantic Technologies
AUTOR	Ana Ballester Funes
DIRECTOR	Francisco Jordan Fernández
PONENTE	Alberto Abelló Gamazo
FECHA	08/09/09
RESUMEN	<p>Providing applications with semantics is an upward trend, so it may also seem interesting to add semantic technologies to the security and trust field, because of its multiple benefits. Semantic technologies allow us to improve systems' interoperability and integration and also permit the use of inference techniques.</p> <p>In this thesis we will analyze the state of the art around semantic technologies and already developed ontologies in the security and trust field. On the basis of this study, we will develop a proposal on security and trust to define which concepts need to be modeled, giving more importance to the PKI field which is our main interest, developing the needed ontologies in case some of the concepts are not modeled yet by any ontology.</p>
KEYWORDS	semantic web, pki, security, segur@, thesis, ontology, CPS, TSL, certificate, PKI, trust
IDIOMA	Castellano
MODALIDAD	Trabajo de investigación

Agradecimientos

En primer lugar, me gustaría dar las gracias a mi director de tesis Francisco Jordán, por la confianza depositada para este nuevo proyecto.

También dar las gracias a todos los compañeros del DMAG y Safelayer Secure Communications que participan conmigo en el proyecto Secur@.

Y finalmente dar las gracias a mi familia y a Marc por estar siempre a mi lado.

ÍNDICE

1	Introducción	1
1.1	Contexto del proyecto.....	2
1.2	Objetivos de la tesis de máster	2
1.3	Estructura del documento.....	3
2	Tecnologías semánticas.....	5
2.1	Beneficios	7
2.1.1	Integración	7
2.1.2	Interoperabilidad.....	8
2.1.3	Inferencia	9
2.2	Lenguajes de la web semántica	10
2.3	Razonadores	11
3	Estado del arte	13
3.1	Ontologías de seguridad	13
3.1.1	DAML Security Ontology	13
3.1.2	SECONT: Security Ontology	14
3.1.3	NRL Security Ontology	15
3.1.4	OWL-S Coalition	17
3.1.5	SAWSDL.....	19
3.1.6	SemDRMS.....	19
3.1.7	Trust Ontology	19
3.1.8	Higgins Ontology	20
3.1.9	NIST.....	21
3.1.10	FOAF y WOT.....	22
3.2	Propuesta de ontología global de seguridad y confianza	23
3.2.1	Conceptos.....	24
3.2.1.1	Context	24
3.2.1.2	Security and trust	24
3.2.1.3	Vulnerabilities and Risks	25
3.2.1.4	Identity	25
3.2.1.5	Resource	26
3.2.1.6	Capa de inferencia	26
3.2.1.7	Capa de confianza	26
3.2.2	Ontologías a utilizar	26
4	Ontologías PKI	29

4.1	Introducción	29
4.2	Entidades PKI	30
4.2.1	Modelar el dominio PKI	30
4.2.1.1	Ampliación de la ontología	31
4.2.2	La ontología	32
4.3	Certificados X.509	34
4.4	Declaración de Prácticas de Certificación	35
4.4.1	Definición	35
4.4.2	Problemática en la creación de la ontología	36
4.4.3	Conjunto de parámetros	37
4.4.4	La ontología	38
4.5	Listas de servicios de confianza.....	39
4.5.1	Introducción	39
4.5.2	Necesidad de modelar el concepto	39
4.5.3	Uso de las TSL	40
4.5.4	Esquema de la TSL	40
4.5.5	La ontología	41
5	Conclusión	43
5.1	Conclusiones generales	43
5.2	Líneas futuras	43
6	Referencias.....	45