FI-WARE Security
WP8 Security

USDL-SEC
Security Service Description

Francesco Di Cerbo

Slim Trabelsi

SAP Research

Sophia Antipolis

Context: PPP Fi-Ware

- Integration EU Project
  - Delivering “Generic Enablers”
  - Services, Software, Infrastructure
- Security WP
  - Identity Management
  - **Data Handling (Privacy)**
  - **DB Anonymizer (Privacy)**
  - **USDL-SEC**
  - Security Monitoring
  - Secure Storage
- IoS
  - USDL

USDL

- The Unified Service Description Language (USDL) is a platform-neutral language for describing services.
- The language is able to describe services from business to technical perspective.
- It will provide means to compare and select services according to consumer needs.
- Targets scenarios:
  - Cloud computing,
  - Service marketplaces,
  - Business networks.
  - Security services

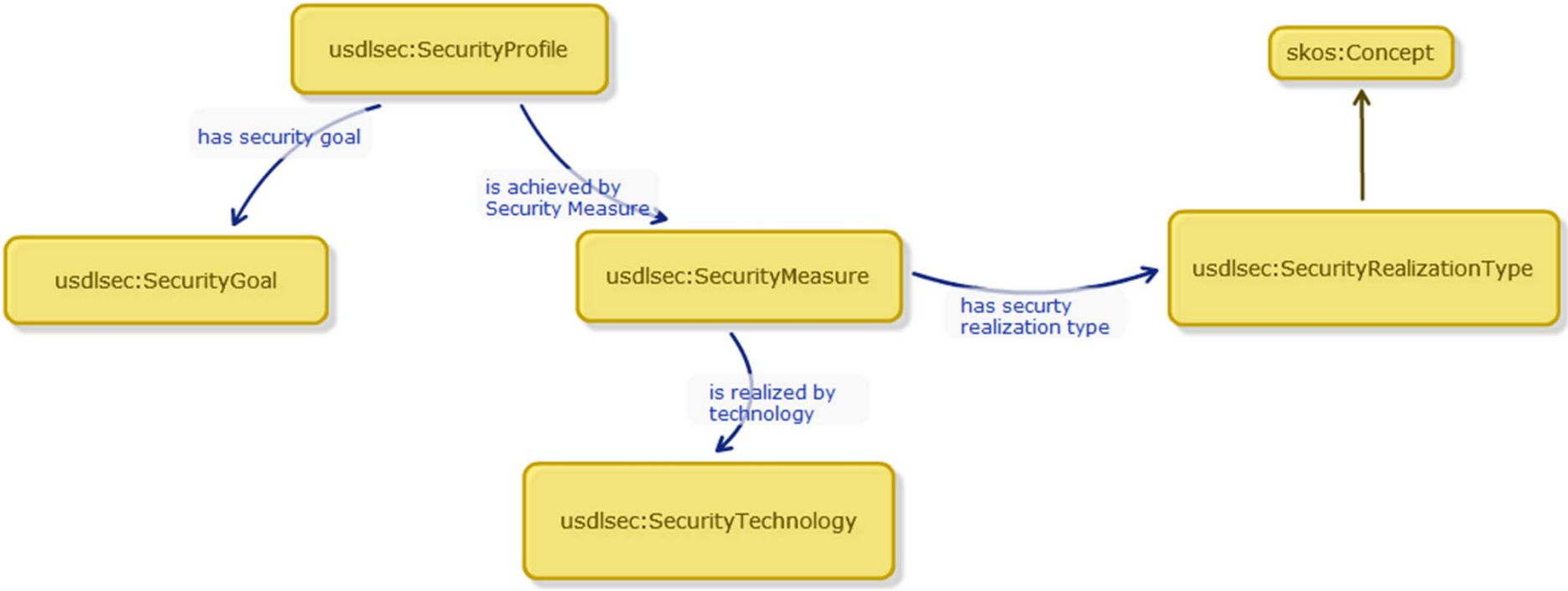
Overview

- USDL-SEC is conceived as a means for expressing security features of services, described with USDL.
- A motivation for USDL-SEC introduction is to allow customers (even when not security experts) to express their security requirements in a declarative way.
  - An abstract description of business service security characteristics enables on the consumer side to express certain security demands and find business services that comply with these demands.
- Service providers can use this specification to describe the security features of their services, and thus to support users in finding adequate alternatives to fulfil their needs.
- Three major requirements
  - explicit representation
  - machine readability
  - advanced composition support

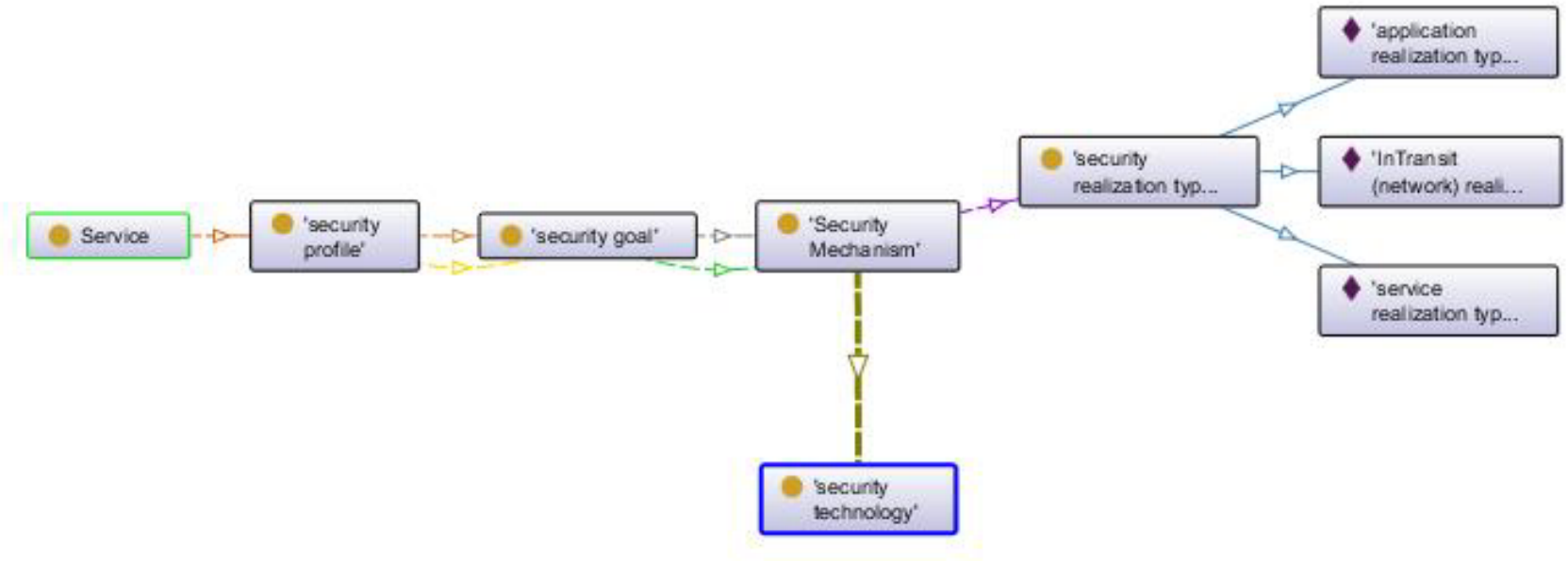
USDL-SEC structure

- The USDL-SEC description can be expressed using a top-down approach, and is globally organised in three main categories:
  - Security topic: This is a high level representation of the security feature of a service.
  - Security solution: This is a security mechanism that contributes towards satisfying a particular security topic.
  - Security technology: It refers to the technical implementations of the security solutions.

The Big Picture

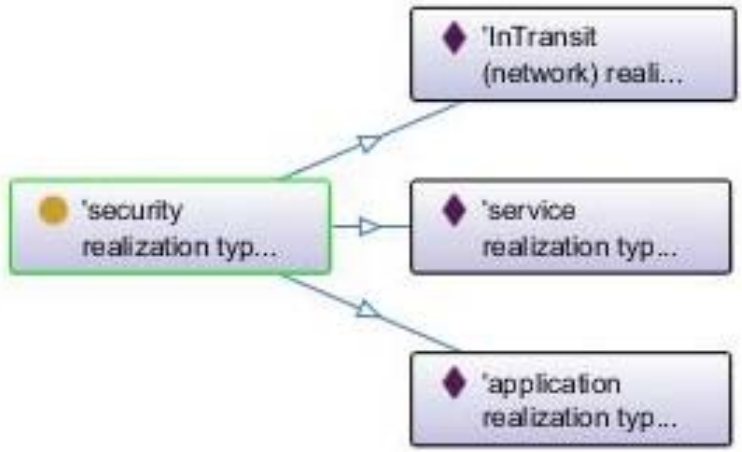


USDL-SEC Model



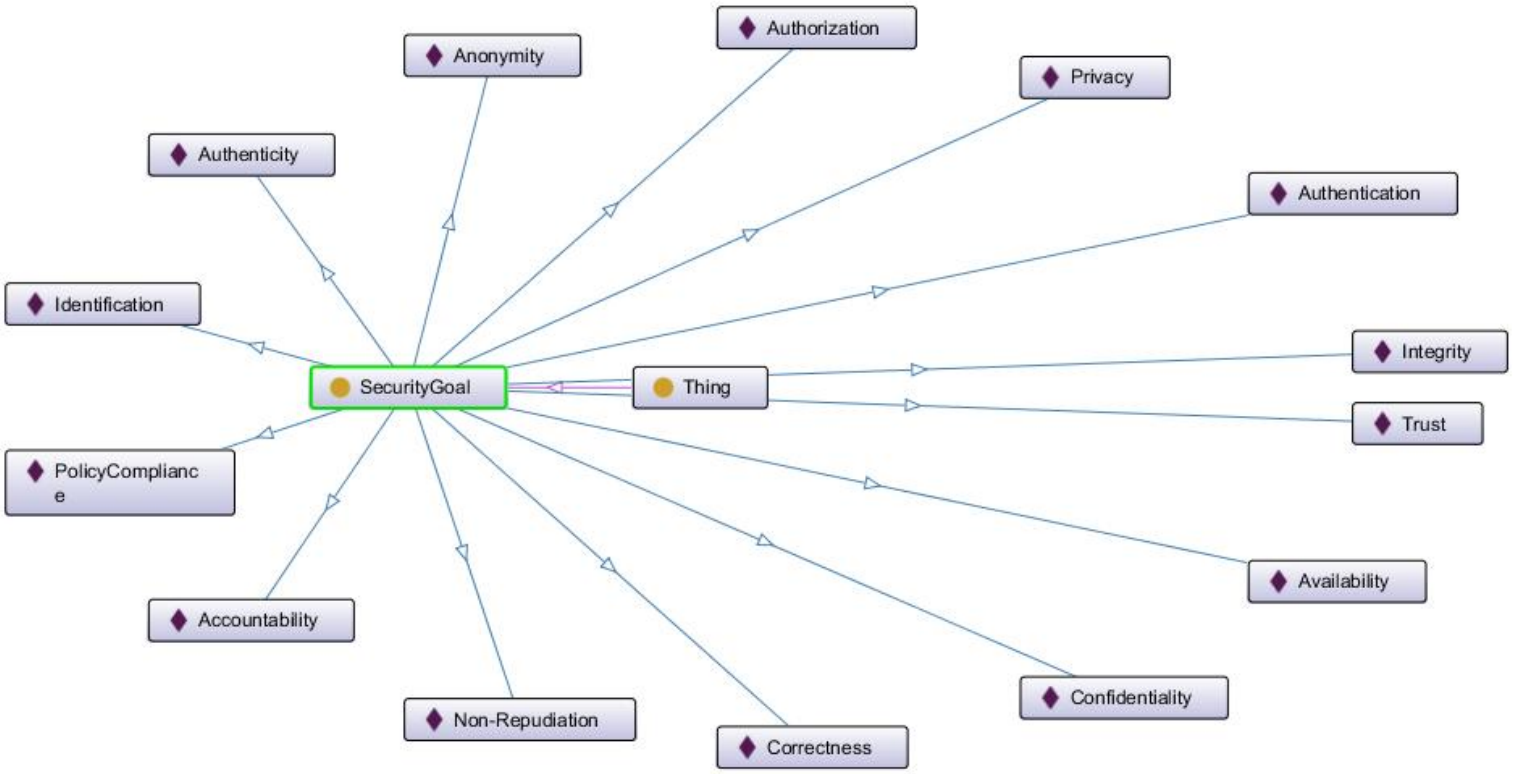
USDL-SEC Model Description

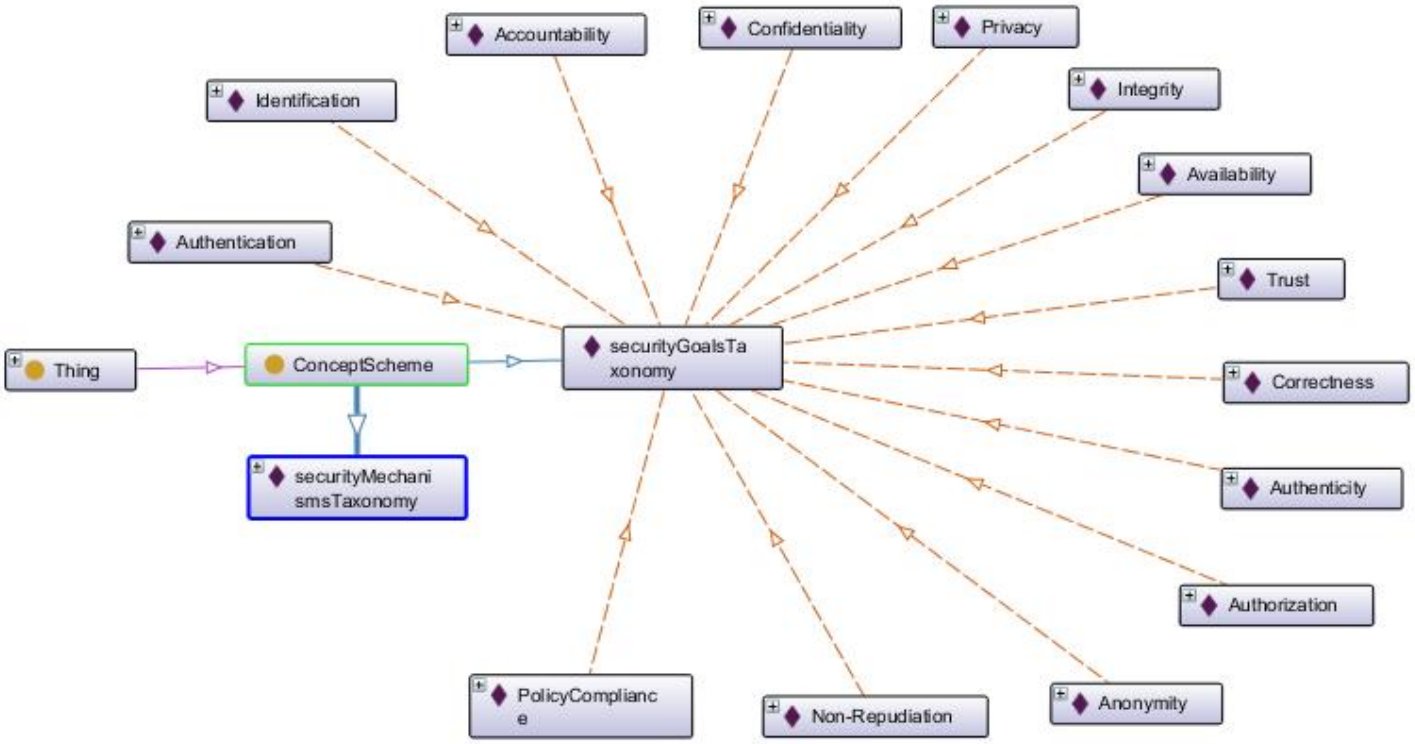
- This three-layered model is materialized into a concrete description model, composed by the following elements:
  - Security Profile: this class contains all USDL-SEC information.
  - Security Goal: the highest abstraction class, referring to a security topic. It encompasses well known security concepts like Anonymity, Confidentiality, Privacy, Authentication etc.
  - Security Mechanism: this class includes a set of security solutions that can contribute to achieve a secu ions that answer to specific sec control, Cryptography, Obligations, e
    - These solutions can be appl
      - The network level,
      - the application level and
      - the service level.



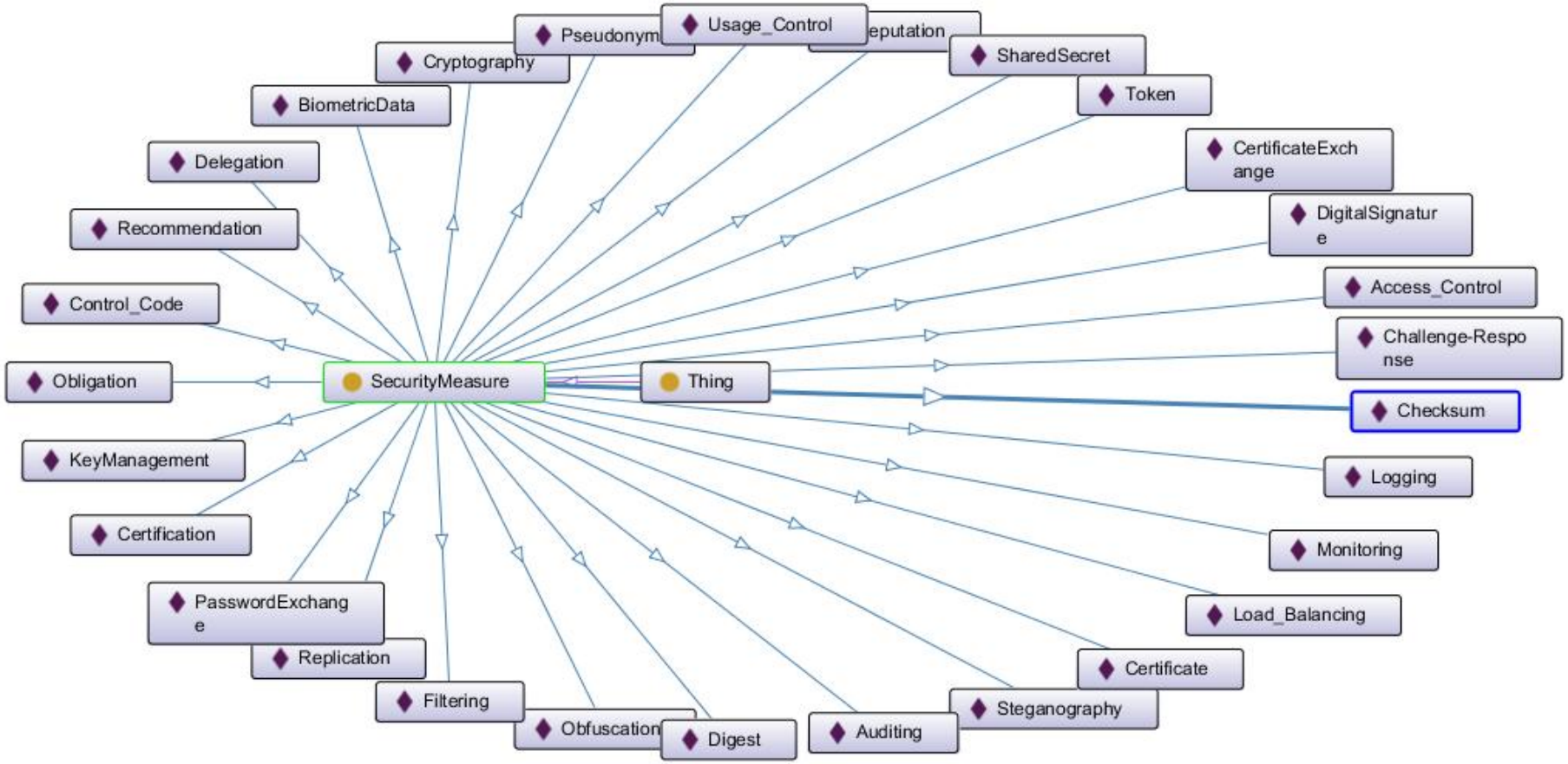
  - Security Technology: this cl ions and tools that realizes the se nple the encryption on the network level is implemented by IPSec.

The Security Goals




Accountability
Confidentiality
Privacy
Identification
Integrity
Availability
Authentication
Trust
Thing
ConceptScheme
securityGoalsTaxonomy
Correctness
securityMechanismsTaxonomy
Authenticity
Authorization
PolicyCompliance
Non-Repudiation
Anonymity

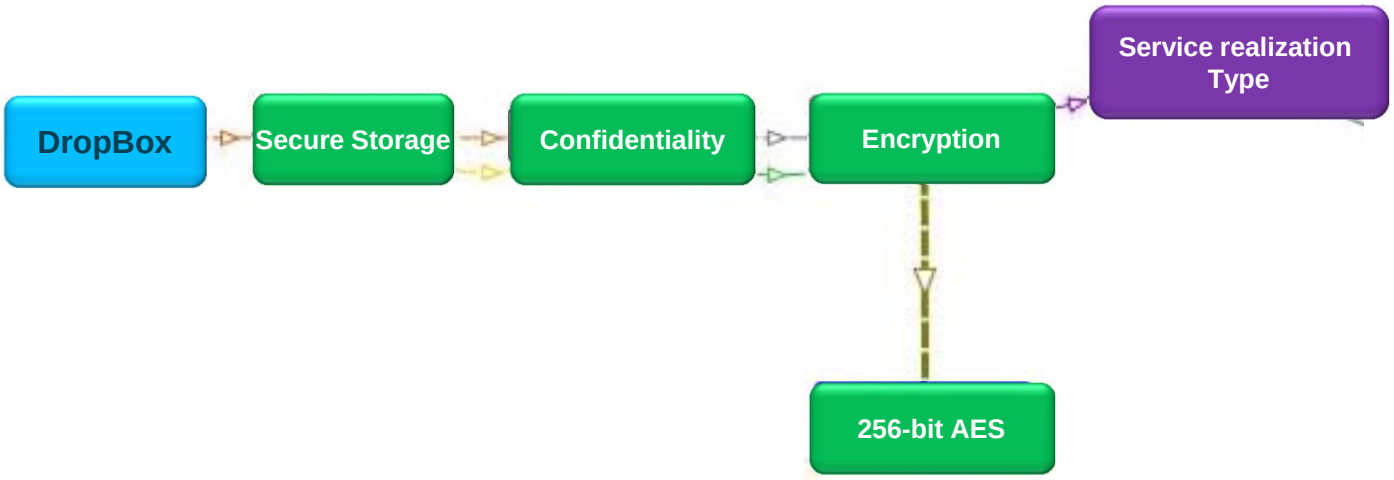
The Security Mechanisms



The Security Technologies

- Security Technologies are not prescribed by USDL-SEC.
- This is due to a number of reasons:
  - the high number of available technologies,
  - their significant changeability,
  - the possibility to use technologies in different contexts to meet different security goals and measures.
- For these reasons, the Security Technology class is conceived as a link with other Linked Open Data vocabularies, that can provide domain-specific technology descriptions.

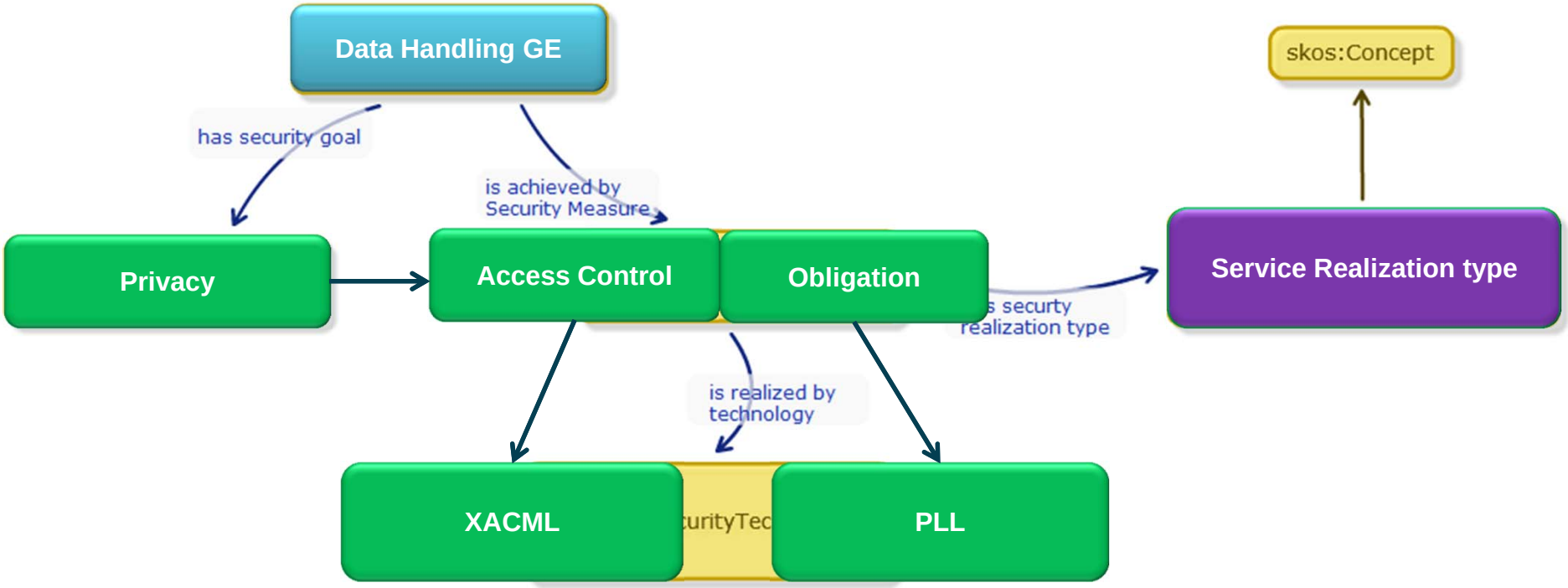
Example: Secure DropBox



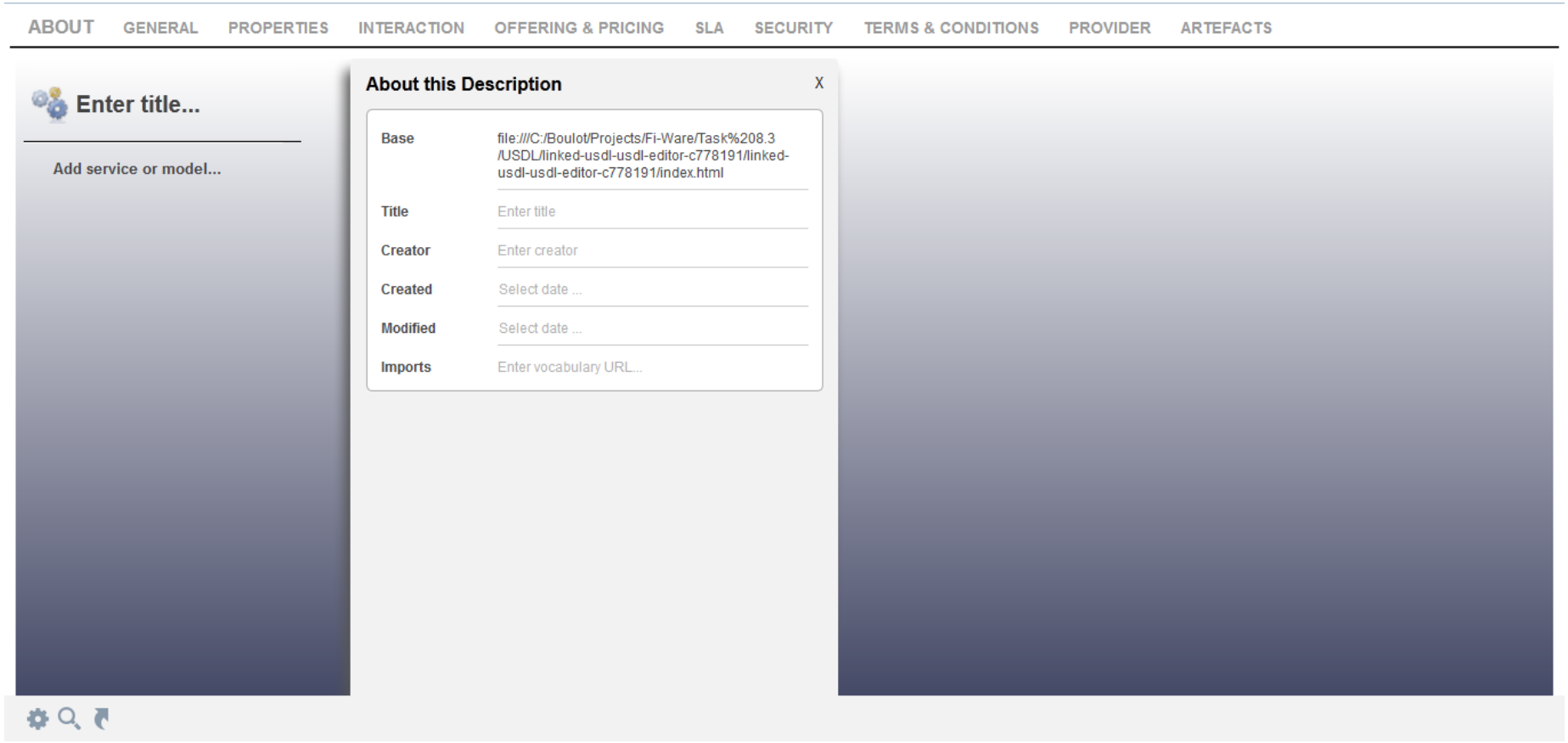
Example: Fi-Ware Data Handling GE

- The Data Handler GE is a privacy-friendly attribute-based access/usage control system to (sensitive) data
- Based on the sticky Policy mechanism, DH GE offers the possibility to attach privacy constraints directly to the data to facilitate the enforcement and the traceability
- And enforcement engine is proposed to perform the access control decisions and the obligation executions (Retention period, usage notification, logging, etc.)
- More details is available here : http://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/FIWARE.Architecture Description.Security.Data_Handling_Generic_Enabler
- Definition of Privacy (challenging !!!)

Describing the Data Handling GE



USDL/USDL-SEC Editor



Interactions and application scope

- Assert4SOA (FP7)
  - Current security certification schemes (Common Criteria) have proven to be a valid means for assurance of security properties of **static** systems towards a human user.
  - Certification composition
- Posecco (FP7)
  - Security configuration checking and compliance for service interaction
  - Security configuration details contained in the USDL-SEC description
- Optet (FP7)
  - Marketplaces for Mobile and Cloud
  - Adding a security structure to the “Store” platforms

Conclusion

- The first release of USDL-SEC comes along the first FI-WARE major release.
- Work in progress: SparQL based query based tool for consumer lookup
- The vocabulary namespace is:
  - http://linked-usdl.org/ns/usdl-sec
- The linked-usdl.org website will be used as main community reference websites.

Thank You!

Slim Trabelsi, slim.trabelsi@sap.com