Future Internet PPP Security Core Platform

FI-WARE Security

October 2011

Antonio García-Vázquez, Pedro Soria-Rodriguez, Pascal Bisson, Daniel Gidoin, Slim Trabelsi, Gabriel Serme

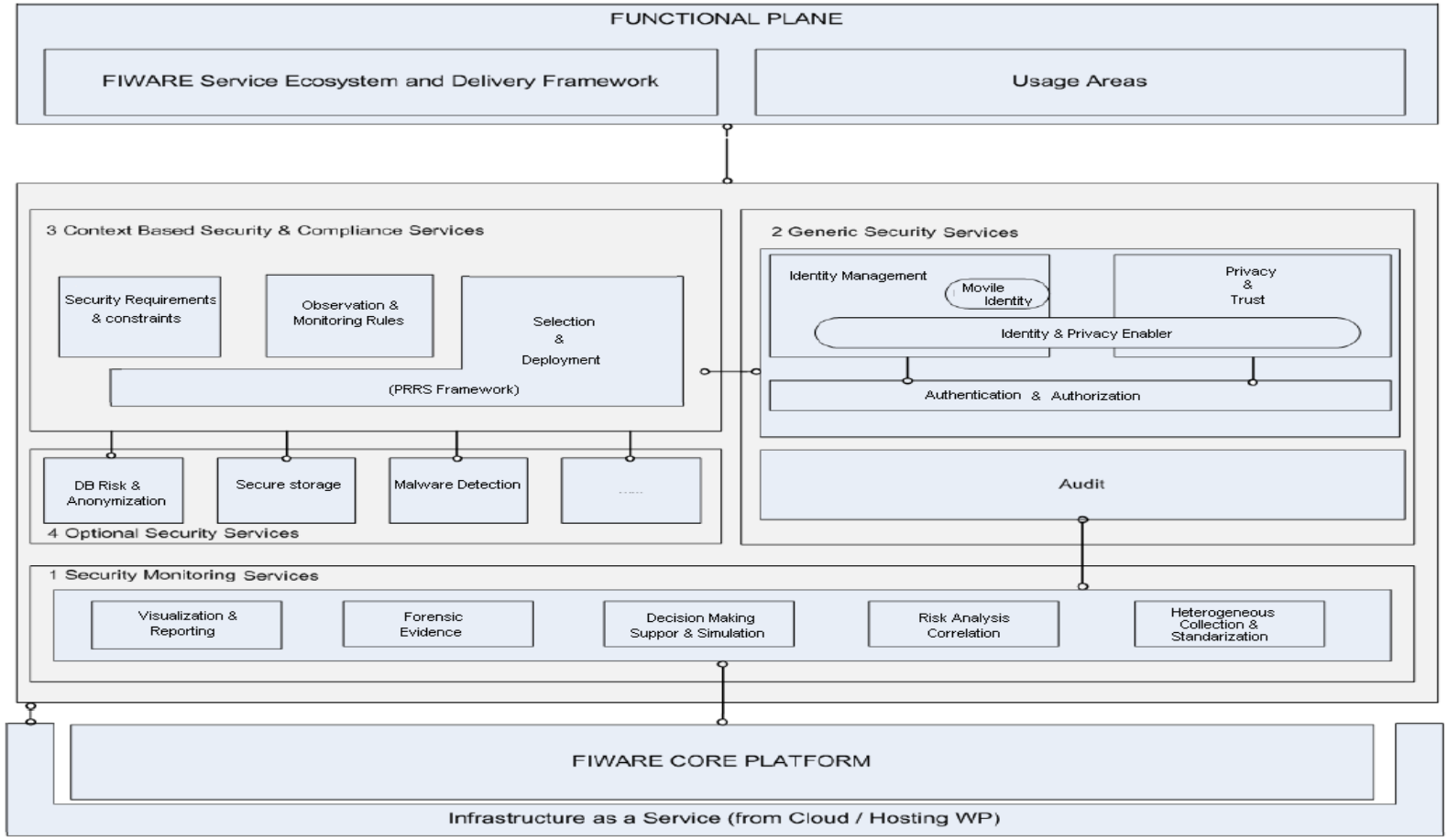
Index

1. Architecture
2. Generic Security Enablers
3. Security Monitoring
4. Context-based Security & Compliance
5. USDL-SEC Language
6. Optional Security Enablers

FI-WARE Architecture

- Open service oriented architecture based in reusable functional building blocks (Generic enablers)
- Security, Privacy and Trust at the heart of Architectural design
- Clear focus on Core Generic Enablers but with the possibility to have completed by optional generic enablers (especially true for what concerns Security domain)
- Extensible Architecture which will be able to meet security requirements from user applications, in run-time mode, by deploying the appropriate enabler
- Services market place where new enablers could be registered and offered.
- Context Based and Compliant Security Services

FI-WARE Architecture



FI-WARE Security Architecture in the context of overall architecture

Generic Security Enablers

- They are the Generic Enablers that will define the core security mechanisms of the Future Internet.
- They will be present by default in any FI-WARE instance to assure that trust, security and privacy are its default mode of operation
- They will provide FI-WARE core security services
  - Security monitoring
  - Context based security & compliance
  - IDM Core (Identity and Access Management, Privacy and Trust, Authentication & Authorization, etc)

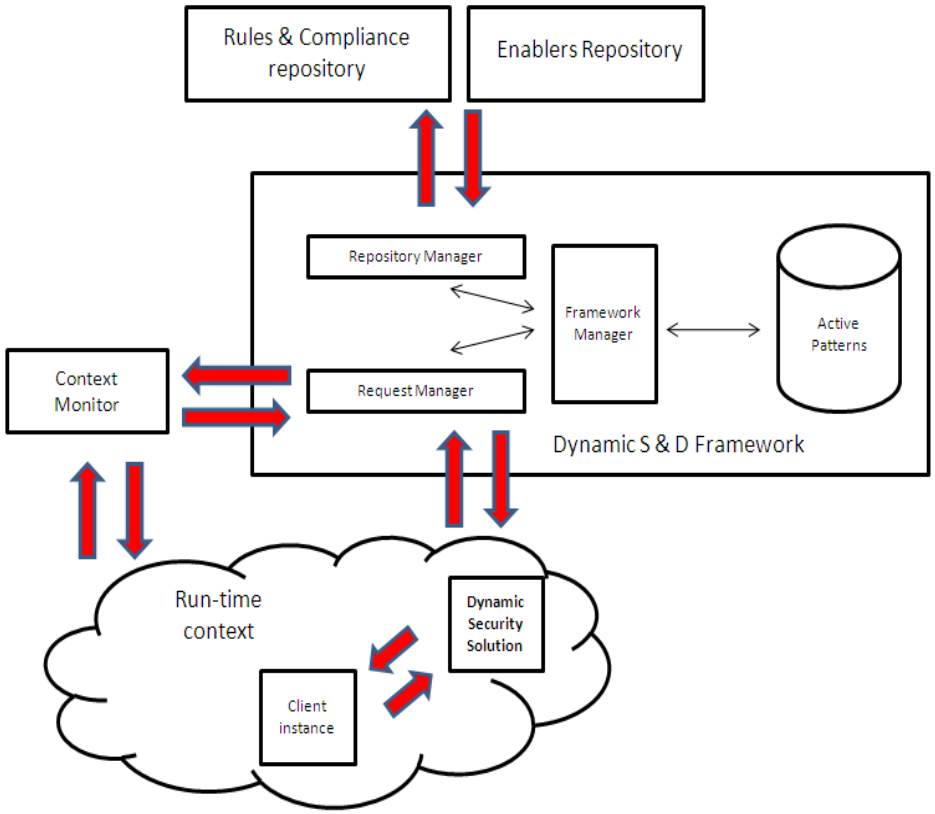
Security Monitoring

- The advanced Security Monitoring system will cover the whole spectrum from acquisition of events up to visualization and reporting.

- It will offer:
  - Correlation of heterogeneous events
  - Risk Analysis
  - Decision making support
  - Visualization and reporting
  - Digital forensics for evidence

Context-based Security & Compliance

- The framework provides run-time support to applications, by managing S&D solutions and monitoring the systems' context.
- End-user applications send requests in order to fulfill their security requirements to the framework.
- Rules repository support the description of laws and agreements that should be applied.

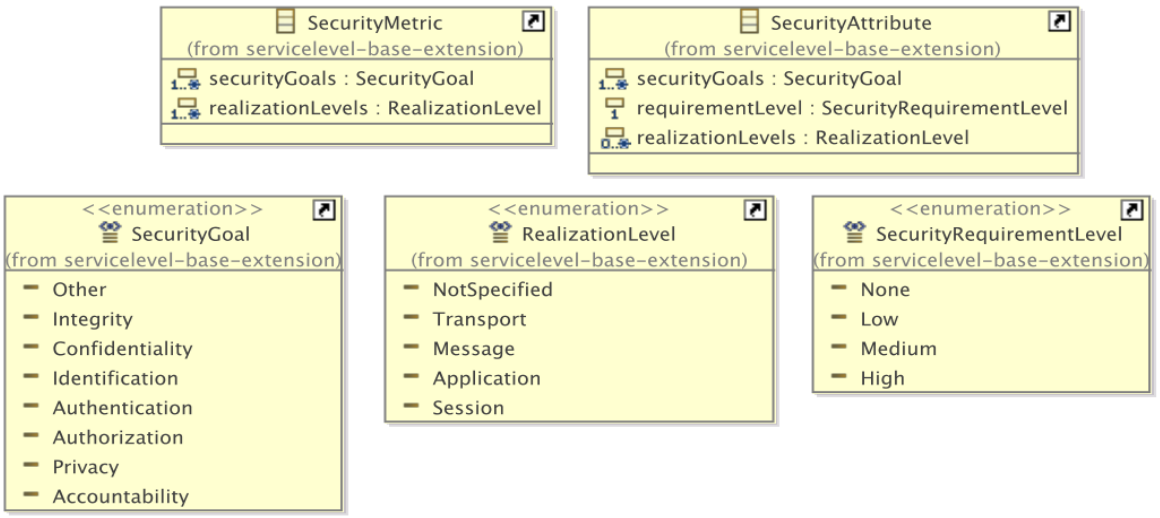


Context-based Security & Compliance

- From the enablers repository, where optional security enablers created by any secure aware developer will be registered, the framework will select the most suitable solution to fulfill the end-user applications requirements.
- This enabler is translated into a S&D solution to be deployed as an executable component in the context where the end-user application is running.
- The framework also provides external monitoring components with the rules that the end-user applications context must fulfill.
- The communication between end-user applications, the deployed executable solutions, the framework and the different components of the enabler is supported by the USDL-SEC language.

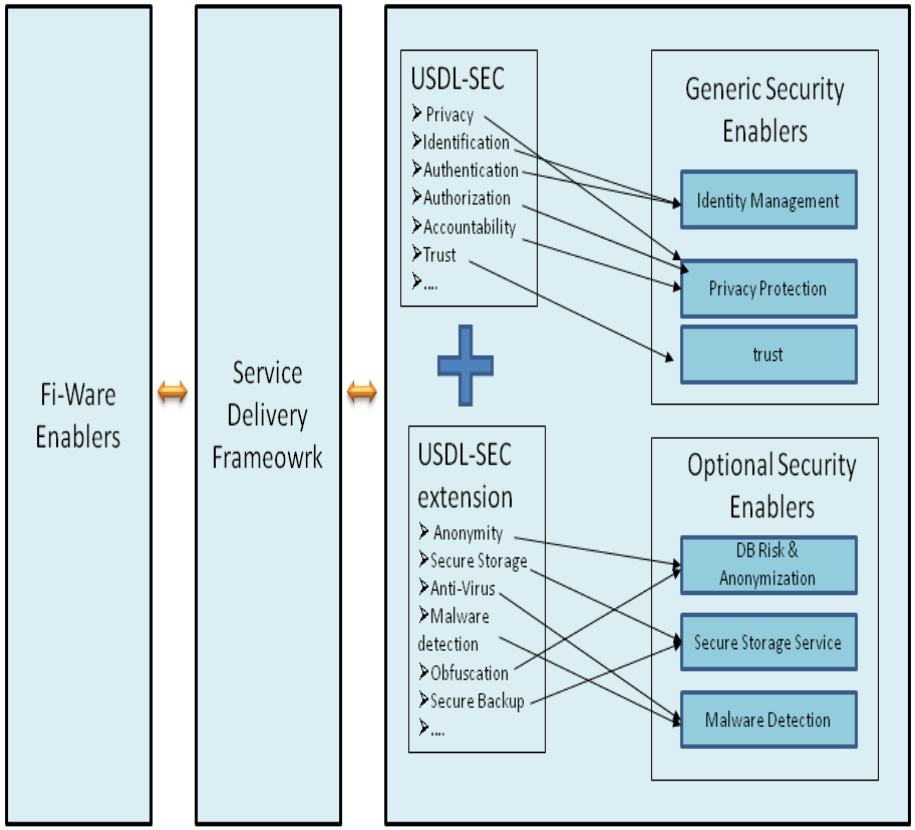
USDL-SEC language

- USDL-SEC will be developed as a security oriented module extension from the existing standard USDL 3.0.
- It will describe a service along with functional and non-functional properties in single and complete description file.
- USDL-SEC will provide means to compare and select services according to consumer needs



Draft UDSL-SEC version schema

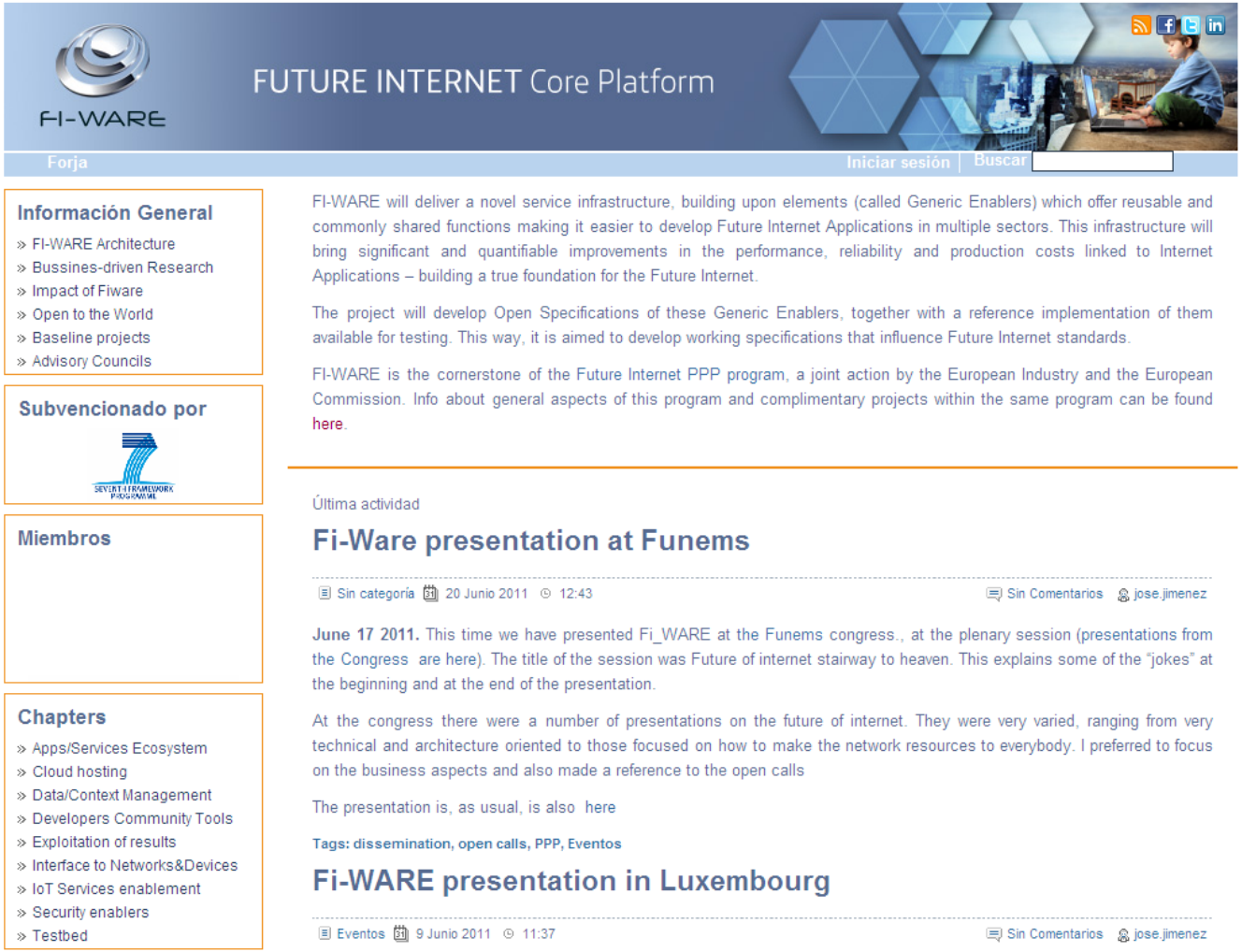
Optional Security Service Enablers



- Optional security service enablers are used to customize the security service description within USDL-SEC.
- Will help developers to define and describe their own services through the USDL standard by adding new functionalities and new capabilities.
- The registry entity is charge of publishing and discovering the services in order to provide an efficient search engine.
- Some of the optional enablers to be developed are Malware Detectors, Secure storage and DB Risk & anonymization services

More Details on

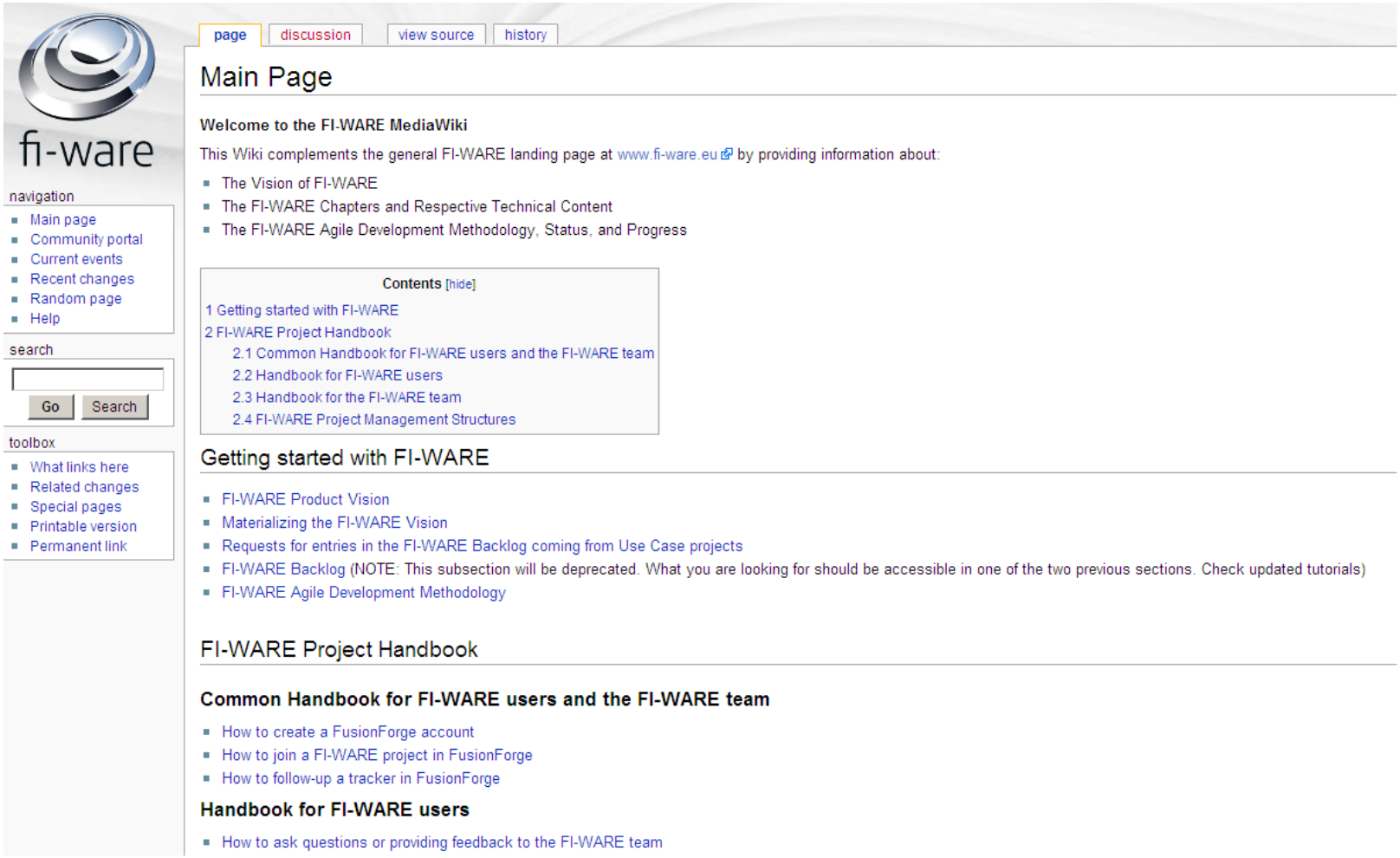
- FI-WARE official Web project: http://www.fi-ware.eu/



More Details on

- FI-WARE MediaWiki:

https://forge.fi-ware.eu/plugins/mediawiki/wiki/fiware/index.php/Main_Page



Thank You !!

Atos:

Antonio García-Vázquez (antonio.garcia@atosresearch.eu)

Pedro Soria-Rodriguez (pedro.soria@atosresearch.eu)

Thales:

Pascal Bisson (pascal.bisson@thalesgroup.com)

Daniel Gidoin, (daniel.gidoin@thalesgroup.com)

SAP:

Slim Trabelsi (slim.trabelsi@sap.com)

Gabriel Serme (gabriel.serme@sap.com)