Project acronym: FI-WARE
Project full title: Future Internet Core Platform
Contract No.: 285248
Strategic Objective: FI.ICT-2011.1.7 Technology foundation: Future Internet Core Platform
Project Document Number: ICT-2011-FI-285248-WP8-D.8.2.3
Project Document Date: 2014-09-25
Deliverable Type and Security: PP
Author: FI-WARE Consortium
Contributors: FI-WARE Consortium
1.1 Executive Summary

This version of the deliverable provides the details of the second software release of FI-WARE.

The software releases take place following three standard methods:

- **Publicly**: under the tool Files of the project called FI-WARE under the FI-WARE forge
- **Restricted to PPP members and the EC**: under the tool Files of the project called FI-WARE PPP Restricted under the FI-WARE forge
- **Offered as a service**: exceptionally, a few partners host their software delivery themselves on their private infrastructures or within the Testbed, available for FI-PPP members. They can supply access to the PPP members or the EC (password protected location) if requested.
1.2 About This Document

The original purpose of this document (associated to the official deliverable D.8.2.2), is to accompany the official deliverable, marked as "P". The EC requires a report with each one of the deliverables of such nature and the present document satisfies such request by giving a succinct account of the software delivered for Release 2 for the respective chapter.

1.3 Intended Audience

This document and the sw deliverables described are mainly oriented to provide an orderly report to the EC but it could also be used by anyone who has interest in installing the GEi or who wants to gain knowledge of the actual software delivered in the 2nd Release of FI-WARE.

1.4 Chapter Context

The overall ambition of the Security Architecture of FI-WARE is to demonstrate that the Vision of an Internet that is "secure by design" is becoming reality. Based on achievements to date and/or to come in the short-term (both from a technological but also a standardization perspective) we will show that "secure by design" is possible for the most important core (basic) and shared (generic) security functionalities as anticipated by the FI-WARE project and in accordance with the requirements of external stakeholders and users such as the FI PPP Use Case projects. The “secure by design” concept will, therefore, address both the security properties of the FI-WARE platform itself and the applications that will be built on top of it.

In this section the foreseen high-level functional architecture is described, introducing the main modules and their expected relationships, then depicting the most important modules in detail along with their main functionalities.

The high level architecture is formed by four main modules: Security monitoring mechanisms (M1), a set of General Core Security Mechanisms (e.g. Identity Management and Privacy solutions) (M2), Context-Based Security and Compliance (M3) where an enhanced version of USDL for security will support the matching of security goals with available security services while addressing compliance management, and a set of universally discoverable Optional Generic Security Services (M4) that will be instantiated at runtime and can be dynamically reconfigured (triggered by M3) based on the needs of specific scenarios.

The overall security plane of the FI-WARE architecture will interlink with practically all its functional modules. In order to simplify the description of these links subsequently the main components as well as their technical relationships with only the Application and Service Ecosystem and Delivery Framework and FI PPP Use Case projects are depicted:

The core general security mechanisms for the FI-WARE project will be provided by M2, including support for Identity Management, Authentication Authorization and Access, and Privacy. M3 will provide the required language and tools for describing services in the FI and their security needs.
Where specific scenarios will require optional generic security services these can be consumed on a basis of what is provided by M4. A key architectural assumption is that security services may fail. Security monitoring mechanisms as provided by M1 may detect deviations with respect to the expected behaviour and signal this to M3 to take action (e.g. invoke alternative security services or trigger countermeasures if under attack).

FI-WARE GEs to be developed and/or integrated as part of the Security chapter will materialize the (Security) Reference Architecture sketched in Figure below. This Reference Architecture comprises:

- A component able to dynamically invoke and compose security services to answer related security needs while dealing with constraints which may apply (e.g. regulatory).
- A set of GEs for a number of shared security concerns (i.e. identity and access management as well as privacy and auditing) that are considered core and therefore present in any FI-WARE Instance.
- A set of optional Security GEs to address current and future requests from concrete Usage Areas.
- An advanced security monitoring system that covers the whole spectrum from acquisition of events up to display, going through analysis but also going beyond thanks to a digital forensic tool and assisted decision support in case of cyber attacks.
Future Internet Core Platform

D.8.2.3 FIWARE SW Release

FIWARE High Level Security Architecture

More information on the Security Chapter and FI-WARE in general can be found within the following pages:

http://wiki.fi-ware.org

The Architecture of Security in FI-WARE

Materializing Security in FI-WARE

1.5 Structure of this Document

The document is generated out of an ad hoc wiki page.

The following resources were used to generate this document:

D.8.2.3 FI-WARE SW Release front page

D.8.2.3 FI-WARE SW Release report
1.6 Acknowledgements

The current document has been elaborated using a number of collaborative tools, with the participation of the Working Package Leader and Architect as well as those partners in their teams acting as GEi owners.

1.7 Keyword list


1.8 Changes History

<table>
<thead>
<tr>
<th>Release</th>
<th>Major changes description</th>
<th>Date</th>
<th>Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>Version</td>
<td>2014-09-25</td>
<td>Thales</td>
</tr>
</tbody>
</table>

1.9 Table of Contents

1.1 Executive Summary .................................................................2
1.2 About This Document ...............................................................3
1.3 Intended Audience .................................................................3
1.4 Chapter Context .................................................................3
1.5 Structure of this Document .................................................5
1.6 Acknowledgements ...............................................................6
1.7 Keyword list .................................................................6
1.8 Changes History .................................................................6
1.9 Table of Contents ...............................................................6
2 D.8.2.3 FI-WARE SW Release report ..............................................7
D 8 2 3 FIWARE SW Release report
You can find the content of this chapter as well in the wiki of fi-ware.

The following table provides a summary of the GEi’s delivered for Release 3 in this chapter.

<table>
<thead>
<tr>
<th>GE Name</th>
<th>GE implementation</th>
<th>Partner</th>
<th>Repository</th>
<th>Release Code</th>
<th>Optional Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Management</td>
<td>GCP</td>
<td>DT</td>
<td>SaaS</td>
<td>N/A</td>
<td>To be provided by the partner upon request.</td>
</tr>
<tr>
<td>Identity Management</td>
<td>KeyRock</td>
<td>UPM</td>
<td>FIWARE</td>
<td>SECURITY-KeyRock 3.3.1</td>
<td></td>
</tr>
<tr>
<td>Identity Management</td>
<td>DigitalSelf</td>
<td>NSN</td>
<td>SaaS</td>
<td>N/A</td>
<td>To be provided by the partner upon request.</td>
</tr>
<tr>
<td>Data Handling</td>
<td>PPL</td>
<td>SAP</td>
<td>FIWARE FI-PPP Restricted</td>
<td>SECURITY-PPL 3.3.3</td>
<td>Source code is publicly available at: <a href="https://github.com/fi-ware-security-sap/fiware-ppl">https://github.com/fi-ware-security-sap/fiware-ppl</a></td>
</tr>
<tr>
<td>Context-based security &amp; compliance</td>
<td>PRRS</td>
<td>ATOS</td>
<td>FIWARE</td>
<td>SECURITY-PRRS 3.2.3</td>
<td></td>
</tr>
<tr>
<td>DB Anonymizer</td>
<td>DBA</td>
<td>SAP</td>
<td>FIWARE FI-PPP Restricted</td>
<td>SECURITY-DBA 3.3.3</td>
<td>Source code is publicly available at: <a href="https://github.com/fi-ware-security-sap/fiware-dba">https://github.com/fi-ware-security-sap/fiware-dba</a></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Service Level SIEM (SLS)</td>
<td>ATOS</td>
<td>FIWARE</td>
<td>SECURITY-ServiceLevelSIEM 3.3.3</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view.</td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Visualisation Framework</td>
<td>THALES</td>
<td>FIWARE</td>
<td>SECURITY-SecurityMonitoring-VisualisationFramework 3.2.1</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view. Visualisation is currently</td>
</tr>
<tr>
<td>Component Type</td>
<td>Component Name</td>
<td>Provider</td>
<td>Type</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------</td>
<td>----------</td>
<td>------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Security Monitoring Engine Web Application</td>
<td>THALES</td>
<td>FIWARE</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view.</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>MulVAL-Attack-Paths-Engine</td>
<td>THALES</td>
<td>FIWARE</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view.</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Remediation App</td>
<td>THALES</td>
<td>FIWARE</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view.</td>
<td></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>ScoredAttackPaths</td>
<td>THALES</td>
<td>FIWARE</td>
<td>This is a component of the Security Monitoring GEi, but considered as a GEi from a sw releasing point of view.</td>
<td></td>
</tr>
<tr>
<td>Malware Detection Service</td>
<td>Morphus</td>
<td>INRIA</td>
<td>Saas</td>
<td>To be provided by the partner upon request. Sample client application mentioned in the User and Programmer Guide and used in the Unit Tests is available in FI-WARE PPP Restricted as release SECURITY-Morphus 3.2.0.</td>
<td></td>
</tr>
<tr>
<td>Content-based Security</td>
<td>CBS</td>
<td>THALES</td>
<td>FIWARE</td>
<td>The CBS GE offers RESTful APIs for content producing and consuming applications to incorporate content based security.</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>Access Control</td>
<td>THALES</td>
<td>FIWARE</td>
<td>SECURITY-AccessControlGE 3.3.3</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>--------</td>
<td>--------</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>Secure Storage Service</td>
<td>SecureStorageService</td>
<td>THALES</td>
<td>FIWARE FI-PPP Restricted</td>
<td>SECURITY-SecureStorageService 2.2.0</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy</td>
<td>IBM</td>
<td>FIWARE</td>
<td>SECURITY-privacyPreservingAuthentication 3.3.3</td>
<td></td>
</tr>
</tbody>
</table>

Notes:

- The field "Repository" has three possible values ("FI-WARE", "FI-WARE PPP Restricted" or "SaaS"), depending on the standard delivery method chosen.
- An empty GEi column means that the name of the GEi is the same as the GE name (only for GEi with a single implementation)