Deliverable Number: D33.3
Deliverable title: FI Utility Services first prototype – M18 issue

Document Owner:	Maria Carla Mantuano (ENG), Mauro Isaja (ENG)
Contributors:	Ioan Toma (UIBK), Iker Larizgoitia (UIBK), Jerry Dimitriou (SINGULAR)
Dissemination:	Public
Contributing to:	WP33
Date:	29/03/2013
Revision:	1.0

Version history

VERSION	DATE	NOTES AND COMMENTS
1.0	29/03/2013	FIRST RELEASE

Table of Contents

1   Executive Summary

An Utility Service is a commodity service addressing any common functionality that is used in enterprise systems.

Utility Services in MSEE provide basic and generic services used by MSEE Use Cases and by any other Manufacturing Service Ecosystem scenario.

The deliverable **D33.1 FI Utility Services specification and architecture** lists and describes different categories of utility services, in the context of the Future Internet, starting from necessities and requirements elicited from MSEE Use Cases.

Particularly the deliverable identifies two concrete utility services that are actually needed by the MSEE use cases, i.e. **Single Sign On** and **Feedback Management**.

Single Sign On is an authentication mechanism which allows users to provide their credentials once, and then have seamless access to a vast array of protected network resources. With Single Sign On in place, authentication can be enforced in a complex system with no negative impact on user experience, as users are not required to submit new credentials (*sign on*) to each application they reach.

Feedback Management enables enterprises to collect customers' and partners' comments and feedback, trying to understand market trends and estimate customer satisfaction to improve their products and services.

Among the objectives of WP33, there is the design and development of the two services above described; this document is to be considered as an introduction to their prototypal implementation.

In this release, the Single Sign On Utility Service was renamed to **Federated Single-Sign-On**, to clearly mark the new functionality layer introduced on top of *traditional* single-sign-on solutions.

The source code of the prototypical implementation of Federated Single-Sign-On and of the Feedback Management Utility Services can be retrieved from the following address:

svn://repo.nimbus-ware.com/MSEE/SP3/WP33/D33.3/trunk

---

2 Introduction to the prototype modules and components

This section, after a general introduction to the utility services, introduces the software components that have been developed in WP33, that are described in details and from a technical point of view in [1], [2] and [3].

2.1 Utility Services

In MSEE WP33, Utility services are conceived as extension of Interoperability Service Utility (ISU), as a generalization that includes services that go beyond interoperability issues, addressing any commoditized functionality that is used in enterprise systems.

As specified by deliverable **D33.1 FI Utility Services specifications and architecture**, Utility Services are characterized by the following features:

- Cheap and near universal access
- Seamless quality of service across multiple providers
- Well understood, regulated and monitored service properties
- Potentially high internal complexity, but limited external configurability/heterogeneity
- Well-defined and standardised interfaces for utility usage and control
- Easiness of use.

Briefly, an Utility Service is a non-functional service that has reached such a high level of maturity that is affordable to all, both from a technical and an economic point of view, being the result of the diffuse ICT commoditization trend.

2.1.1 Federated Single-Sign-On

MSEE Use Cases expressed the necessity to elaborate concepts and IT services to cover/ensure privacy in the network through the management of roles and permissions in accessing resources and services. Such necessity depends on the nature of ecosystems, which represent an interaction environment where different parts collaborate and cooperate toward common objectives, but with different roles and potential risk of disclosure of key information assets.

Single-Sign-On (SSO) provides a central authentication point for users of complex, distributed, multi-tier web applications and services: users authenticate themselves once and then are granted access to the entire environment, without repeating annoying login operations. Furthermore, increased security is ensured, as user credentials shared between users and the SSO system are invisible to applications.

A typical SSO installation is a central web application which provides a common login page and a security token validation service, and which is connected to a central user/credential database. This DB may either come embedded into the SSO application itself or belong to an enterprise-level IT infrastructure.

In the MSSE scenario, multiple MSEE platforms (Ecosystems) may exist, each exposing its own instances of SSO-enabled web applications and services.

Multiple Enterprises may take part in a single Ecosystem, and the same Enterprise may take part in multiple Ecosystems. A set of one or more Ecosystems placed under the authority of the same SSO system is called a **MSEE Ecosystem Federation.**

So in the MSEE context we refer to SSO as **Federated SSO.** Federated means that while authentication is centralized, user data is not: Enterprises should be able to join the federation without sharing their internal user's data with any external system.

Basic SSO is a system integration tool: Enterprises use it to bring together several different end-user applications living on their intranet / extranet. MSEE aims at bringing together different Enterprises living in the same business ecosystem, and also at ecosystem interoperability; from this point of view, **Federated SSO is an *enterprise integration* tool.**

Users of a MSEE Federation are registered at the Enterprise, Ecosystem or Global level. Each system entity on these levels – that is, the single Enterprise, the single Ecosystem and the MSEE Federation itself – may have the role of Local Security Authority (LSA). Every LSA contributes with its own user-base to the Federated SSO system, without any duplication or sharing of sensitive user data. When an user requires login, the central SSO service will match the user to the LSA of origin, and will delegate authentication to it; the delegation process is totally transparent to the end user.

The Federated SSO Utility Service not only deals with authentication, but also supports the *attributes release* feature, which is the capability of "annotating" users with attributes after a successful login. Due to the multi-layered approach used, this means that LSAs are also responsible for maintaining the relevant set of attributes for each user.

The following diagram (Figure 1) illustrates the relationship between Federated-SSO components.
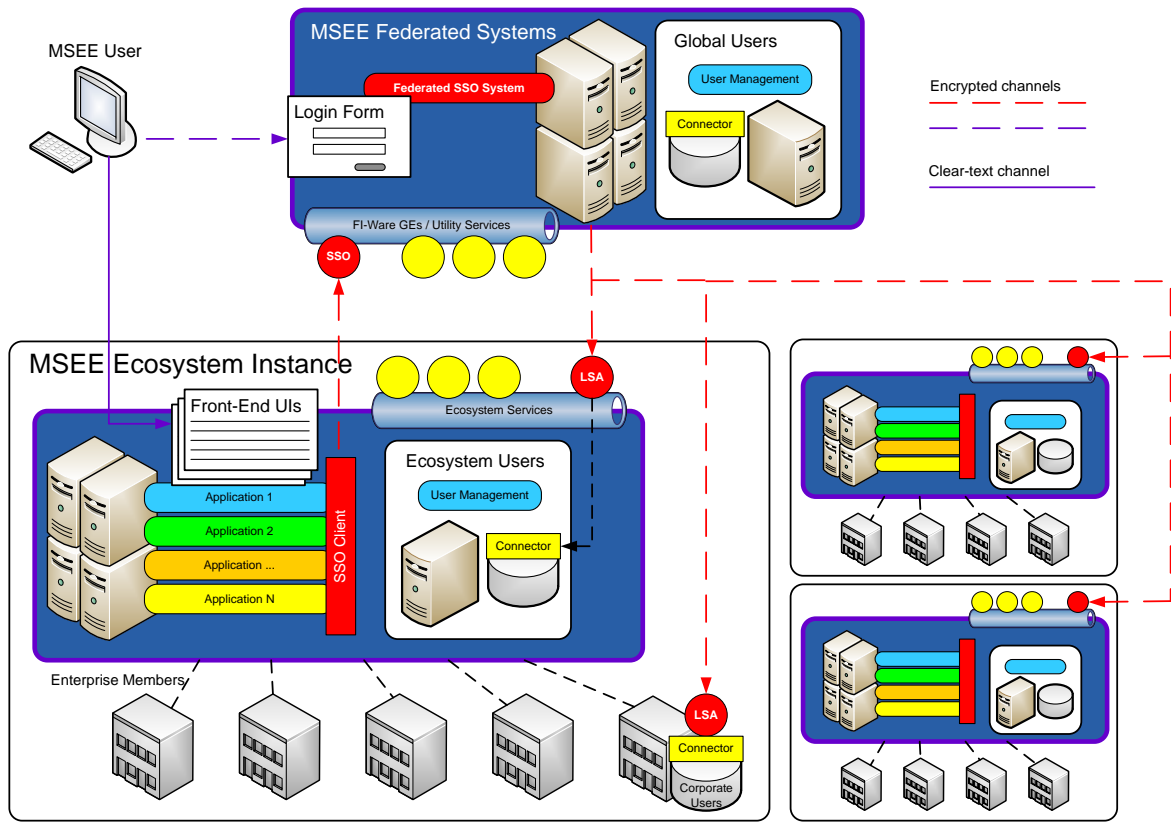

Figure 1 - Relationship between Federated-SSO components

2.1.2 Feedback Management

With the latest developments of the Web in the direction of social media, user-generated content and information sharing, it became a must for Enterprises to be present on the various web and social channels, to monitor and to react to posts and comments expresses online that are about the products and services they offer. Enterprises actually need to 'listen the voice' of customers and partners involved in the VME to continuously improve the offer and the overall business process. According to a study realized by the Aberdeen Group in 2011, companies using customer feedback management services have better customer retention's rate. The exponential growth in terms of number of communication channels where the information about products and services offered by an Enterprise can be disseminated and from where feedback can be collected, make the situation even more complicated. Enterprise lack often the skills and resources to react in a competitively advantageous manner to customers' comments and reviews, shape their product and service offerings to reflect the public perception, and manage their reputation online.

The goal of the Feedback Manager Service in MSEE is provide a solution to the challenges mentioned before. The Feedback Management Service aims at providing a unified publication method in a multichannel environment and the associated automatic aggregation of the feedback provided there, releasing from the burden of manually publish and collect information from these channels separately. Additionally the Feedback Management Service will also offer scalable means to publish on various channels (Facebook, Twitter, LinkedIn, etc).

The Feedback Management Service will be generic enough to be reused for different purposes, thus representing a Utility Service that can respond to the needs of any industrial domain. Enterprises can use the service to:

- ***Define the information to be disseminated*** (text, video, images) independently of the different channels available.

- ***Automatically publish this information in selected channels***. The information is transformed and published automatically into the different selected channels.

- ***Collection of feedback*** associated to the published information in the different channels. Each publication in different channels can be tracked to collect feedback, according to the channel (likes in Facebook, number of retweets in Twitter, comments, etc…) that could be further analyzed to measure the impact, e.g. with sentiment analysis tools.

3   Prototype modules

3.1   Federated Single-Sign-On

The following table provides the list of the software components that D33.3 delivers in the scope of the MSEE project.

Component	Implemented functionalities
Federated SSO Server	This module is a customized version of the Jasig's Central Authentication Service (CAS) open source product [4]. For any given MSEE Ecosystem Federation, one single deployment of the server is needed: some place of the network where it is visible to each client (the end user browser and every federated web application and service) and has visibility of each LSA Service (see below). The server exposes a centralized login form. At user sign-on, the server identifies the Local Security Authority which is actually responsible for the validation of the provided credentials and delegates user authentication to the corresponding LSA Service. This delegation process is totally transparent to the end user. Federated web applications and services have a relation of trust with the centralized server, so that the user does not have to repeat the sign-on procedure each time she reaches a new application. The client modules, used to integrate web applications and services in the federation, are technology-specific: a different module exists for each supported environment – i.e., Java, PHP, .NET. Detailed technical information for this component is available in [1].
Federated SSO Client Libraries	This module is a library of Java classes enabling the integration of J2EE-based web applications and services with a CAS server [4]. It is a stock redistribution of the open source product from Jasig: no modifications were introduced for MSEE. Detailed technical information for this component is available at [5]. Note that other web application technologies are supported by Jasig, most notably PHP and .NET: see the Jasig site [6] for more information.
LSA Service	This module is a web service responsible for user credential validation and attribute release on behalf of the Federated SSO Server (see above). The service can be deployed anywhere on the network, provided it is visible from the Federated SSO Server. The Federated SSO Server delegates user authentication to an LSA Service, which checks the provided credentials against its own private user data repository. If the user is successfully authenticated, the service replies releasing name and value of all the attributes that are *assigned* to

the user in the local repository.

Within a MSEE Federation, each federated Ecosystem *should* run an instance of LSA Service; additionally, each participating Enterprise *may* also run its own.

Detailed technical information for this component is available in [2].

3.2   Feedback Management

The following table provides the list of the software modules that are part of the Feedback Management Service.

Component	Implemented functionalities
Role Management	This module provides role management functionality for those that are using the Feedback Management Service. Two roles are envisioned and supported for the moment i.e. system *user* and *administrator*. A *user* is allowed to use the functionality of the service. An *administrator* has additional rights being able to administrate (add, delete, etc.) user accounts and has an overview about the health of the service. Detailed technical information for this component is available in [3].
Publication	This module is responsible for the publication of content into channels. The Publication module is also responsible for adaptation of content to be published to the specific requirements of the different channels. The adaption is made on the base of the channel capabilities, e.g. shortened messages are posted to microblog platform, such as twitter. To achieve scalability the Feedback Management Service uses a message-oriented architecture to implement an asynchronous publication process. For this purpose the Advanced Message Queuing Protocol, short AMQP[1] is used. Detailed technical information for this component is available in [3].
Feedback Collection	This module is responsible for the collection of various feedbacks across multiple channels. Feedback can have different forms. It can either be textual (comments, replies, etc.), a certain amount of positive (like, +1, thumbs up, etc.) or negative feedback (thumbs down, bury, down vote, etc.), or some other measurement of a user's response to a published item. The Feedback Management Service can collect all these different types of feedback using various polling strategies. Detailed technical information for this component is available in [3].

The Feedback Management Service and its component are provided as a RESTfull service. In addition to them a ***Front-end Web application*** is provided. The Front-end Web application provides the GUI to access the functionality of the Feedback Management Service including publication, feedback collection and role management.

---

[1] http://amqp.org/

4   Summary and conclusions

This deliverable provides the first prototypical implementation of the **Federated Single-Sign-On** and **Feedback Management** Utility Services**.** This document is to be considered as an introduction to these prototypes**,** whereas [1], [2] and [3] provide the technical details of the components that have been delivered at month 18. In future developments of MSEE Project, the prototypes may be refined and extended, and utility services categories may be further analyzed to identify other services needed from MSEE Use Cases.

5   References

[1] 33.3 Factsheet#1 – Federated SSO Utility Service – Federated SSO Server

[2] 33.3 Factsheet#2 - Federated SSO Utility Service – Local Security Authority Service

[3] 33.3 Factsheet#3 – Feedback Management Utility Service

[4] Jasig's Central Authentication Service home site: http://www.jasig.org/cas

[5] Jasig's Central Authentication Service Java client v.3.1:
https://wiki.jasig.org/display/CASC/CAS+Client+for+Java+3.1

[6] Jasig's Central Authentication Service client integration site:
http://www.jasig.org/cas/client-integration