



A7.D5.3 – Evaluation Criteria for Communication scenario v2.0

A. Armenteros, L. García

Document Number	A7.D5.3
Document Title	Evaluation Criteria for Communication scenario v2.0
Version	1.0
Status	Final
Work Package	WP 7.5
Deliverable Type	Report
Contractual Date of Delivery	31 December 2007
Actual Date of Delivery	24 January 2008
Responsible Unit	TID
Contributors	DBL, KUL, STM, THA
Keyword List	Evaluation, Criteria, Objective
Dissemination level	PU

Change History

Version	Date	Status	Author (Unit)	Description
0.1	14/01/08	Draft	A. Armenteros (TID) L. García (TID)	Initial draft
1.0	24/01/08	Final	A. Armenteros (TID) L. García (TID)	Final. Ready for quality check

Executive Summary

The purpose of this document is to state the evaluation criteria that is going to be used to assess the degree of achievement of Communication scenario prototype implementation in its new version from Telefónica I+D as the new partner in the SERENITY project.

SERENITY project has been broken down into several activities, each coping with specific issues of each layer and providing suitable solutions for them. As described in deliverable A7.D5.1, which represents a mandatory previous reading to this document, each activity has its own evaluation criteria. Furthermore, in order to ensure the correct evaluation of integration of different levels of SERENITY architecture, it includes evaluation criteria for scenarios defined in A7 (and its S&D requirements). This document amends that deliverable to cover the new proposed Communication scenario.

Table of Contents

1. Introduction.....	5
1.1. Scope and Objectives	5
1.2. SERENITY objectives	5
2. Evaluation criteria for Communication scenario	6
2.1. Objective I: Appropriateness of scenario and S&D requirements	6
2.2. Objective II: Evaluating Usability.....	6
2.3. Objective III: Iteration of security pattern.....	7

1. Introduction

1.1. Scope and Objectives

SERENITY approach to evaluation criteria definition stands on two pillars: activity-based and scenario-based evaluation criteria. Deliverable A7.D5.1 covered both parts. Now this document amends that deliverable in order to include the new proposed scenario by Telefónica I+D, which covers the Communication domain.

Evaluation will be performed by defining appropriate evaluation criteria based on the characteristics and S&D requirements of the scenario, the use of patterns, integration schemes, and the different versions of the SERENITY framework to provide S&D solutions for the reference scenario, the assessment of the framework based on the reference scenario, and the provision of feedback to the project's focus activities.

1.2. SERENITY objectives

General objectives which have been stated for SERENITY at a very general level (see section 2.3 of the DoW) are shown here as a reminder. Such general high-level objectives instantiate into several different criteria that are largely dependent on the nature of the problems addressed and solution proposed.

- **Objective I.** To make validated security solutions available to AmI ecosystems and promote their assurance and evolution.
- **Objective II.** To support the definition of security requirements which arise in different business, private and legal activities in order to enable a requirements-driven selection of appropriate security mechanisms within integration schemes at run-time.
- **Objective III.** To provide mechanisms for monitoring security at run-time and dynamically react to threats or breaches of security, and context changes.
- **Objective IV.** To integrate security solutions, requirements definition and solution selection, and monitoring and reaction mechanisms in a common framework.

2. Evaluation criteria for Communication scenario

In A7.D5.1 the SERENITY approach was evaluated by exposing it to a set of industrial case studies emerging from a number of reference scenario domains showing the characteristics and complexity of the communication and information infrastructures the SERENITY framework is expected to manage. The scenario domain and its respective case study are each provided by TID and carefully selected to:

- Address current industrial needs in managing heterogeneous environments on different layers
- State S&D requirements for system and service landscapes that are not completely controlled by a single owner and may be characterised by conflicting interests of the parties involved
- Require solutions that can cope with dynamic environments and evolving S&D objectives by implementing run-time monitoring mechanisms
- Being suitable to evaluate all aspects of the SERENITY framework
- Being able to be developed iteratively to provide both early and continuous feedback and evaluation results.

New Communication scenario comes as the contribution from Telefónica I+D as new industrial partner in the SERENITY project.

2.1. Objective I: Appropriateness of scenario and S&D requirements

- **Interviews with End Users:** this activity aims at evaluating whether the offered S&D patterns has to be modified and need to be re-injected in the scenarios for the validation process. End users will be asked to evaluate their personal feeling of safety with the offered S&D patterns. By holding an interview with the end users, the subjective level of security can be evaluated. The interaction between the first set of patterns, the affected people and the scenarios could assure the evolution and continuous refinement of patterns and requirements. It also may lead to an adjustment of the scenario to focus on certain aspects.
- **Interviews with Security Office of larger enterprise:** this activity aims at stating whether the level of security offered by the patterns is applicable and appropriate for real world company environments. The communication patterns must be suitable for this kind of enterprise environment. The interview should also point out certification issues, company security testing processes and needed add-on's to the scenario and its pattern.

2.2. Objective II: Evaluating Usability.

- **Usability (Transparency and Seamlessness) of the solution:** Level of seamlessness and transparency of the security mechanism must be assessed too: SERENITY runtime framework offers dynamic adaptation behaviour when dealing with changing context parameters. Such adaptation implies new potential application of security measures on user's devices, communication channels, etc. All this changes ideally should not be perceptible by end users. Interviews with users can reveal flaw points of the runtime behaviour and may lead to better implementations.

- **Usability of the user interface:** checking the usability of the administration interface for security officers in terms of easiness of use, intuitive use, etc.

2.3. Objective III: Iteration of security pattern.

- The received feedback will be fed back into the process and result in an **iterative process of requirements refinement**. This is obtained through the previous objectives above. Also the integration issues will lead to an iteration of the pattern and improve it's applicability to a real environment.