



## A2.D3.1 - Preliminary version of workflow security analysis tool

A. Piñuela, P.Kostaki, S.Kokolakis

<b>Document Number</b>	A2.D3.1
<b>Document Title</b>	Preliminary version of workflow security analysis tool
<b>Version</b>	2.3
<b>Status</b>	Final
<b>Work Package</b>	WP 2.3
<b>Deliverable Type</b>	Prototype
<b>Contractual Date of Delivery</b>	31 December 2006
<b>Actual Date of Delivery</b>	15 January 2007
<b>Responsible Unit</b>	ATO
<b>Contributors</b>	UNA, ATO
<b>Keyword List</b>	Workflow security analysis tool, Formal analysis, S&D patterns
<b>Dissemination level</b>	PU

## Change History

<b>Version</b>	<b>Date</b>	<b>Status</b>	<b>Author (Unit)</b>	<b>Description</b>
1.0	10/01/2007	Initial	Ana Piñuela (ATO)	
2.0	12/01/2007	Draft	Paraskevi Kostaki (UNA)	Amendments for the quality check
2.2	15/01/2007	Final	Spyros Kokolakis (UNA)	Revision
2.3	15/01/2007	Final	Spyros Kokolakis (UNA)	Changes to make the document compliant to the Quality Plan

## Executive Summary

In this document we define and analyse high-level needs and features of the Workflow Security Analysis Tool (WoSAT), which is a product of the SERENITY Project (Activity 2). The focus is on the capabilities needed by the stakeholders, and the target users, and the rationale of these needs. The document also provides the WoSAT tool use case model and consequently we provide a description of the use cases. Finally, this deliverable describes WoSAT functionality and some useful information such as the installation instructions of the first prototype.

## Table of Contents

1. Introduction.....	6
1.1. Purpose .....	6
1.2. Scope .....	6
1.3. Definitions, Acronyms, and Abbreviations .....	6
1.4. References .....	6
1.5. Overview .....	6
2. Positioning .....	8
2.1. Business Opportunity .....	8
2.2. Problem Statement .....	8
2.3. Product Position Statement .....	8
3. Stakeholder and User Descriptions.....	9
3.1. Stakeholder Summary .....	9
3.2. User Summary .....	9
3.3. User Environment.....	9
3.4. Stakeholder Profiles .....	10
3.4.1. User organisations' managers .....	10
3.4.2. SERENITY industrial partners .....	10
3.5. User Profiles .....	11
3.5.1. Security engineer.....	11
3.5.2. SERENITY engineers .....	11
3.6. Key Stakeholder or User Needs .....	12
4. Product Overview .....	13
4.1. Product Perspective .....	13
4.2. Installation instructions .....	13
5. Product Features and Functionalities.....	14
5.1. Graphical design of workflows .....	14
5.2. Translation of the graphical representation of workflows into WS-BPEL and vice versa .	14
5.3. Import WS-BPEL workflow models.....	14
5.4. Graphical representation of WS-BPEL workflows .....	14
5.5. Graphical representation of S&D requirements/properties .....	14
5.6. Translation of graphical S&D requirements/properties in a formal language and vice versa .....	15

6. Summary and conclusions ..... 16

# 1. Introduction

---

This report is a companion to Deliverable A2.D3.1 of the SERENITY project. The latter is a software prototype. It is part of Activity A2 “Workflow & Services” and Workpackage (WP) 2.3 “Development of workflow security analysis and pattern verification tools”. This document elaborates the features of the Workflow Security Analysis Tool (from now on WoSAT). It focuses on the capabilities needed by the stakeholders, and the target users, and why these needs exist. The details of how the WoSAT fulfils these needs are defined in the use-case and supplementary specifications. WoSAT’s prototype functionalities and some useful information such as the installation instructions are also presented.

## 1.1. Purpose

The purpose of this document is to describe the purpose and use of WoSAT.

## 1.2. Scope

This document applies to WoSAT, the tool that is under development in the context of the SERENITY project. This tool will assist security engineers in the design and static validation of S&D patterns for workflows.

## 1.3. Definitions, Acronyms, and Abbreviations

WoSAT	Workflow Security Analysis Tool
S&D	Security and Dependability
GUI	Graphical User Interface
S&D properties	S&D properties that are satisfied by the proposed solution
EC	European Commission
WS-BPEL	Web Services Business Process Execution Language

## 1.4. References

SERENITY Contract - Annex I: “Description of Work”
SERENITY Deliv. A2.D1.1: “Report on the State of the Art workflow security technology”

## 1.5. Overview

The rest of this document is organised as follows: Section 2 describes the positioning of WoSAT, why it is needed and what it does. Section 3 defines the WoSAT stakeholders and users. Section 4 provides a high level view of WoSAT capabilities and installation instructions. In section 5 the

WoSAT features are listed and briefly described. Finally, section 6 provides a summary of the document.

## 2. Positioning

---

### 2.1. Business Opportunity

The prime purpose of WoSAT is to support security engineers in the design of security patterns for workflows. The tool will be used as a supplement to the SERENITY framework. The SERENITY framework provides validated solutions for security problems in dynamic systems (in the form of security patterns) and monitors the application of these solutions. SERENITY framework shall provide solutions at different levels of abstraction (i.e. organizational, workflow, network and devices). There is, however, a need for designing these solutions, which will not be covered by the SERENITY framework. With regard to workflows, this need will be addressed by WoSAT. Nevertheless, WoSAT will be valuable for any engineer concerned with the security of workflow-based systems, whether she uses the SERENITY framework or not.

Currently, it seems that there is no tool that can serve the needs of security engineers for the design of security solutions for workflow-based systems able to be statically validated. Thus, if we consider the rapid proliferation of workflow-based systems, we can anticipate a large base of users.

### 2.2. Problem Statement

The problem of	lacking an appropriate tool to design S&D solutions for workflows
affects	security engineers and users of workflow-based systems
the impact of which is	application of ad hoc solutions that may not address S&D requirements effectively and efficiently
A successful solution would be	a tool which can support the above process and will be easy to use and effective.

### 2.3. Product Position Statement

For	security engineers
Who	want to design security patterns for workflows
WoSAT	is a software product
That	supports security engineers in the design of re-usable security solutions that can be statically validated and disseminated in the form of security patterns.

## 3. Stakeholder and User Descriptions

In this section the users and stakeholders of WoSAT are identified. Stakeholders include people involved in the development of workflow-based systems and people involved in the SERENITY project. End users include the security engineers who will use WoSAT to design security solutions for workflow-based systems. In the development process of WoSAT, users are represented by industrial partners in the SERENITY consortium.

### 3.1. Stakeholder Summary

In this section we identify the stakeholders that are not end users. Users are presented in section 3.3

Name	Description	Responsibilities
User organisations' managers	User organisations are system development and system integration companies. We refer to all levels of management involved in system engineering projects.	To overlook the provision of high quality solutions with minimum cost.
SERENITY industrial partners	People involved in testing and validating the SERENITY security patterns.	To use the SERENITY framework and the security patterns that shall be developed and to validate them through the user scenarios.

### 3.2. User Summary

Name	Description	Responsibilities	Stakeholder
Security engineer	Security engineers working in system development or system integration projects that involve workflows.	Provide effective S&D solutions for workflow-based systems.	Represented by user organizations in the SERENITY project.
SERENITY engineers	People in SERENITY who design patterns.	To provide a set of S&D patterns for workflows.	Self-represented

### 3.3. User Environment

The target of WoSAT is security engineers who fully understand concepts like security patterns, workflows, and S&D requirements. In the most common case, they work for system development and system integration companies and they design patterns either for using them in the systems they develop or to provide them to the public (or to cooperating parties) for use. We assume that the

relevant systems are dynamic systems that use workflow technologies based on web services. No further information about the user environment is currently available.

### 3.4. Stakeholder Profiles

#### 3.4.1. *User organisations' managers*

<b>Representative</b>	Management executives in SAP, NOKIA, THALES, ATOS ORIGIN and ENGINEERING
<b>Description</b>	User organisations are system development and system integration companies. We refer to all levels of management involved in system engineering projects.
<b>Type</b>	Non-expert
<b>Responsibilities</b>	To observe the provision of high quality solutions with minimum cost.
<b>Success Criteria</b>	Solutions to S&D problems are easily statically validated, documented, and re-used.
<b>Involvement</b>	Involved through their representatives in the project (industrial partners).
<b>Deliverables</b>	Preliminary version of WoSAT (prototype).
<b>Comments / Issues</b>	The management of industrial partners is not represented in the project and this might be an issue. Most of the participants in the project are engineers and researchers.

#### 3.4.2. *SERENITY industrial partners*

<b>Representative</b>	The Activity 7 team
<b>Description</b>	Member of the SERENITY project.
<b>Type</b>	Expert
<b>Responsibilities</b>	Provide a test bed for SERENITY results (among other).
<b>Success Criteria</b>	The patterns are of high quality and provided in such a format that allows an easy and effective application in the user scenarios.
<b>Involvement</b>	Provide the needs and high-level requirements of end users.
<b>Deliverables</b>	Preliminary version of WoSAT (prototype).
<b>Comments / Issues</b>	-

### 3.5. User Profiles

#### 3.5.1. Security engineer

<b>Representative</b>	Industrial partners
<b>Description</b>	Security engineers working in system development or system integration projects.
<b>Type</b>	Expert
<b>Responsibilities</b>	Provide effective security solutions for workflow-based systems.
<b>Success Criteria</b>	Ease of use of the tool; useful results.
<b>Involvement</b>	Involved through their representatives in the project, who will review the tool.
<b>Deliverables</b>	Preliminary version of WoSAT (prototype).
<b>Comments / Issues</b>	-

#### 3.5.2. SERENITY engineers

<b>Representative</b>	People in the A2 team that will design S&D patterns for the purposes of the project.
<b>Description</b>	People in SERENITY that design patterns.
<b>Type</b>	Expert
<b>Responsibilities</b>	Provide S&D patterns for workflow-based systems.
<b>Success Criteria</b>	Ease and effective development of S&D patterns for workflows
<b>Involvement</b>	Directly involved in A2 activities
<b>Deliverables</b>	Preliminary version of WoSAT (prototype) in M9.
<b>Comments / Issues</b>	-

### 3.6. Key Stakeholder or User Needs

Need	Priority	Concerns	Current Solution	Proposed Solutions
Visualise workflows, identify S&D requirements and properties.	High	There is no tool to assist security engineers in designing security solutions for workflows.	Security engineers must depend on manual solutions	The visual representation of workflows and the ability to identify and set security requirements on them will allow the development of valid S&D solutions.

## 4. Product Overview

---

This section provides a high level view of WoSAT capabilities, interfaces to external systems, and the system configuration.

### 4.1. Product Perspective

WoSAT is a static analysis tool that will support security engineers in the design of re-usable security solutions that can be statically validated in the form of security patterns. It captures the security engineers' specific knowledge about a particular solution. This knowledge is represented in the form of S&D Patterns and Integration Schemas, which are created by the Pattern Specification Tool. The latter is being developed as part of Activity 6 work.

### 4.2. Installation instructions

The WoSAT software (plugins.rar) can be downloaded from this web page:  
<https://bscw.sit.fraunhofer.de/bscw/bscw.cgi/d818343/plugins.rar>.

The following instructions will help the user to install the WoSAT tool.

1. Download the zip file from  
<http://www.eclipse.org/downloads/download.php?file=/webtools/downloads/drops/R1.5/R-1.5.2-200610261841/wtp-all-in-one-sdk-R-1.5.2-200610261841-win32.zip>
2. Unzip the file you previously downloaded
3. Unzip the plugins.rar file
4. Start Eclipse to install the WoSAT code:
  - a. Open the File menu
  - b. Select Import – General – Existing projects into Workspace
  - c. Choose Select root directory. Click on Browse button and select the plugins folder in which you unzip the plugins.jar file
  - d. Select the Plugins folder and click on Finish. After that, you will see a plugins folder and the org.eclipse.bpel.XXXX directories inside.
  - e. Select one of those directories. Click on the right button of the mouse and select Run as Java Application.

## 5. Product Features and Functionalities

---

The main functionalities of the WoSAT tool are:

- Graphical Design of Workflows
- Translation of the graphical representation of workflows into BPEL and vice-versa
- Import BPEL workflow models
- Graphical representation of BPEL workflows
- Graphical representation of S&D requirements/properties
- Translation of graphical S&D requirements/properties in a formal language and vice-versa
- Import patterns
- Validation of S&D solutions

A brief description of each one is provided in the following paragraphs.

### 5.1. Graphical design of workflows

WoSAT will exhibit the appropriate interface for the graphical representation of workflows. The GUI will have grouping, expanding and collapsing functions for the elements (actors, tasks etc.) of the workflow. The user will have the ability to revise the workflows at any time.

### 5.2. Translation of the graphical representation of workflows into WS-BPEL and vice versa

Workflows will have a dual representation: in the aforementioned graphical notation and in BPEL format. Users should have access to both formats. The translation from one format to another shall be automated.

### 5.3. Import WS-BPEL workflow models

WoSAT will import BPEL workflow specifications from other workflow tools like BPEL Designer.

### 5.4. Graphical representation of WS-BPEL workflows

WoSAT will provide a graphical representation of imported BPEL workflow specifications (in the aforementioned graphical notation).

### 5.5. Graphical representation of S&D requirements/properties

The user will be provided with the appropriate tools for specifying (embedding) through the GUI the security requirements that apply to each workflow element. There will, also, be overall workflow S&D properties, i.e. properties that refer to the whole workflow and not to a particular element. (Note that S&D properties are S&D requirements that are satisfied.) Any relevant prerequisites, constraints and other dependencies are specified.

The user can “pick” security requirements from the security requirements/properties toolbox maintained by WoSAT, or he/she can specify new ones.

## **5.6. Translation of graphical S&D requirements/properties in a formal language and vice versa**

S&D requirements/properties will have a dual representation: in a graphical notation, and in formal language. Users should have access to both formats. Translation from one format to another shall be automated.

## **5.7. Validation of S&D properties**

WoSAT shall support the static validation of S&D requirements in a WS-BPEL workflow.

## 6. Summary and conclusions

---

WoSAT is a static analysis tool that will support security engineers in the specification of S&D requirements for workflows and the design of re-usable security solutions that can be statically validated in the form of security patterns. In this document the first prototype is presented as well as technical details for the releases to come.

## References

- [1] Jacobson, I., G. Booch, and J. Rumbaugh. *The Unified Software Development Process*. Reading, Mass.: Addison-Wesley, 1999.
- [2] Gomaa, H. *Designing Concurrent, Distributed, and Real-Time Applications with UML*. Upper Saddle River, NJ: Addison-Wesley, 2000.