Automated VAlidatioN of Trust and Security
of Service-oriented ARchitectures

FP7-ICT-2007-1, Project No. 216471

www.avantssar.eu

Deliverable D1.1
PROJECT PRESENTATION

Abstract
This document describes the objectives, the description of work, the expected results, the duration, the cost, and the partners of the AVANTSSAR project. It also describes a set of slides and a poster that have been prepared for presenting the project, as well as the project website.

Deliverable details
Deliverable version: v1.1
Date of delivery: 17.04.2008
Person-months required: 1
Due on: 31.03.2008
Classification: public
Total pages: 27
Editors: UNIVR (Luca Viganò)

Project details
Start date: January 01, 2008
Duration: 36 months
Project Coordinator: Luca Viganò
Partners: UNIVR, ETH Zurich, INRIA, UPS-IRIT, UGDIST, IBM, OpenTrust, IEAT, SAP, SIEMENS
Contents

1 Project Overview
   1.1 Project information ........................................... 3
   1.2 List of beneficiaries ........................................... 4
   1.3 The overall goal of the AVANTSSAR project ............... 4
   1.4 Overall strategy of the work plan ......................... 7

2 Project Presentation Slides ....................................... 10

3 Project Presentation Poster ....................................... 25

4 Project Website .................................................... 27
1 Project Overview

1.1 Project information

Project title: Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures
Acronym: AVANTSSAR
Project number: 216471
Programme: Seventh Framework Programme (FP7)
Call identifier: FP7-ICT-2007-1
Objective: ICT-2007.1.4 (Secure, dependable and trusted Infrastructures)
Instrument: Specific Targeted Research Project (STREP)
Start date: January 01, 2008
End date: December 31, 2010
Duration: 36 months
Total cost: € 6,070,954.80
EC contribution: € 3,800,000.00
Website: www.avantssar.eu

Contact: Prof. Luca Viganò
Dipartimento di Informatica
Università degli Studi di Verona
Strada Le Grazie 15
I-37134 Verona, Italy
Mobile: +39 3204251233
Phone: +39 0458027070
Fax: +39 0458027068
E-mail: luca.vigano@univr.it
1.2 List of beneficiaries

<table>
<thead>
<tr>
<th>Beneficiary number</th>
<th>Beneficiary name</th>
<th>Beneficiary short name</th>
<th>Beneficiary type</th>
<th>Country</th>
<th>Date enter project</th>
<th>Date exit project</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (coordinator)</td>
<td>Università di Verona</td>
<td>UNIVR</td>
<td>academia</td>
<td>Italy</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>2</td>
<td>ETH Zurich</td>
<td>ETH Zurich</td>
<td>academia</td>
<td>Switzerland</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>3</td>
<td>Institut National de Recherche en Informatique et Automatique</td>
<td>INRIA</td>
<td>academia (research org.)</td>
<td>France</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>4</td>
<td>Institut de Recherche en Informatique de Toulouse</td>
<td>UPS-IRIT</td>
<td>academia (research org.)</td>
<td>France</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>5</td>
<td>Università di Genova</td>
<td>UGDIST</td>
<td>academia</td>
<td>Italy</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>6</td>
<td>IBM Research GmbH</td>
<td>IBM</td>
<td>industry/research</td>
<td>Switzerland</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>7</td>
<td>OpenTrust</td>
<td>OpenTrust</td>
<td>industry (SME)</td>
<td>France</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>8</td>
<td>Institute e-Austria Timișoara</td>
<td>IEAT</td>
<td>research org.</td>
<td>Romania</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>9</td>
<td>SAP AG</td>
<td>SAP</td>
<td>industry</td>
<td>Germany</td>
<td>month 1</td>
<td>month 36</td>
</tr>
<tr>
<td>10</td>
<td>Siemens Aktiengesellschaft</td>
<td>SIEMENS</td>
<td>industry</td>
<td>Germany</td>
<td>month 1</td>
<td>month 36</td>
</tr>
</tbody>
</table>

1.3 The overall goal of the AVANTSSAR project

Driven by rapidly changing requirements and business needs, IT systems and applications are undergoing a paradigm shift: components are replaced by services, distributed over the network, and composed and reconfigured dynamically in a demand-driven way into service-oriented architectures. Exposing services in future network infrastructures entails a wide range of trust and security issues. Solving them is extremely hard since making the service components trustworthy is not sufficient: composing services leads to new subtle and dangerous vulnerabilities due to interference between component services and policies, the shared communication layer, and application functionality. Thus, one needs validation of both the service components and their composition into secure service architectures.

The overall goal of the AVANTSSAR project is to develop such a rigorous technology supporting the formal specification and automatic validation of trust and security in service-oriented systems. The AVANTSSAR technology will provide the ability to formally model and automatically reason about services, their composition, their required security properties and associated policies, both at network and application level. This will include not only standard properties such as authentication and secrecy, but also authorisation, access control, trust delegation and obligations, identity management, etc. The AVANTSSAR technology will thus speed up the development of the next generation of service-oriented architectures, guarantee their correctness, and therefore increase the public acceptance of advanced, distributed ICT systems and applications based on them. In order to ensure the migration of the project results into industry and standardisation bodies, this technology will be automated as part of an integrated toolset, the AVANTSSAR Validation Platform, which will be tuned on case studies of industrial
relevance.

To this end, the project will accomplish the following tasks:

• Develop ASLan, the first formal modelling language that is fully dedicated to specifying trust and security aspects of services, their composition, as well as the properties that they are required to satisfy and the policies that they manipulate and abide by.

• Develop novel automated techniques to reason about runtime composition of services and their associated security policies into secure service-oriented architectures.

• Develop the AVANTSSAR Validation Platform comprised of automated tools for the validation of trust and security aspects of service-oriented architectures. The AVANTSSAR Validation Platform and its usage in Enterprise SOA are depicted in Figure 1, where we use TS as an abbreviation for Trust and Security.

• Develop a library of secure composed services and secure service-oriented architectures by applying our validation technology to proof-of-concept case studies taken from practice, in particular those provided by the industrial partners of the project.

The AVANTSSAR Validation Platform takes as input specifications of trust and security requirements — expressed in terms of policies — and models of services, including a specification of their security relevant behaviour as well the local policies they respect. These service specifications can be both statically configured or dynamically discovered. The main components of the platform are the following:

• The TS Orchestrator provides the means to compose the service models in a way presumed to respect the global policies. In case of dynamic composition of services, this orchestration is synthesised utilising TS Wrappers which add security functionality not provided by the initial set of services.

• The TS Validator automatically analyses the validation problem resulting from the TS Orchestrator output. Failed validation means the existence of vulnerabilities that need to be fixed; otherwise, the composition of the services is guaranteed to be secure, i.e. to respect the global policies.

Whenever the TS Validator detects a vulnerability on the composed service, a feedback loop to the TS Orchestrator is initiated. Several options exist
Figure 1: The AVANTSSAR Validation Platform and its usage towards Enterprise SOA (TS abbreviates Trust and Security).
to revise the TS Orchestrator results in order to fix the vulnerability: using a different composition pattern, revising the local policies, or introducing new services or policies to the orchestra. Any combination of these will be supported.

The AVANTSSAR Validation Platform operates on the logical level. Hence, the specifications of services and their orchestration provided to the platform (and resulting from the validation and synthesis activities) need to be transformed to and from the modelling artifacts and languages used at the application level. This transformation is non-trivial, since, in many cases, the modelling techniques available at the application level do not provide the concepts or expressiveness needed for automated validation of the security of services and their composition. (Otherwise, they could be used directly.) AVANTSSAR explicitly addresses this transformation through an Industry Migration workpackage that takes current industrial best practise languages and models into account, and systematically relates them to each other. Tools will be provided to assist designers in extending their models with the augmentations required for validation. This is key to successful exploitation of the AVANTSSAR results in real-world industrial settings, since the industry standards are used as a matter of fact, and for good reasons. The AVANTSSAR approach, thus, does not ask for disruptive changes, but its Industry Migration allows for a smooth integration in existing environments. This will be demonstrated by some of the project’s industrial partners.

1.4 Overall strategy of the work plan

The AVANTSSAR project can be subdivided into four main technical parts and a dissemination package, together with a workpackage WP1 devoted to project management. The dependencies (and input–output relations) between the workpackages are depicted in Figure 2.

Workpackage WP2 has as main goal the definition of the AVANTSSAR Specification Language (ASLan), which will allow users of the platform to formally model trust and security-related aspects of service-oriented architectures resulting from the run-time composition of services and their associated policies.

Workpackage WP3 will focus on the development of automated reasoning techniques for service architectures formally described and specified using the concepts and language of WP2.

Workpackage WP4 will integrate and implement the reasoning techniques and decision procedures developed in WP3 for systems modelled us-
ing the ASLan language. The result will be a uniform toolset, the AVANTSSAR Validation Platform, with support for both design and analysis. It will be able to automatically check whether a set of services can be securely combined, orchestrate their composition by providing a protecting security wrapper for the composed service, and validate the result.

Workpackage WP5 will define and formalise a set of industrial problem cases, against which the models, techniques, and tools developed in WP2, WP3, and WP4 will be assessed. This includes producing the AVANTSSAR Library, a set of formalised and validated secure services and service architectures, providing proof of concept that the developed technology scales to the envisaged applications.

Workpackage WP6 has as objective to facilitate the dissemination and migration of the project results into the scientific community and industry. Besides the dissemination activity, for which appropriate and standard communication media including a web site, forums, project workshops, and reports will be set up to disseminate the project results, a consid-
erable effort will be dedicated to the migration of the project outcomes to industry. In general, while the four technical workpackages address issues such as expressiveness, scalability and automation, WP6 will focus on making the results of the other workpackages accessible to, and readily exploitable by, industry designers and developers.
2 Project Presentation Slides

The following set of slides provides a quick presentation of the project, which has been given already at a number of meetings, in particular, at a meeting in Bruxelles to prepare the Bled conference on “The Future of the Internet” ([www.fi-bled.eu](http://www.fi-bled.eu)), at a meeting of the Sensoria project to which AVANTSSAR was invited ([www.sensoria-ist.eu](http://www.sensoria-ist.eu)), and also at a number of internal meetings held at different AVANTSSAR project sites.
Automated VAlidatioN
of
Trust and Security
of
Service-oriented ARchitectures

FP7-2007-ICT-1, ICT-1.1.4, Strep project no. 216471
(36 months duration, 590 PM, 3.8M€ budget)

Project motivation

- ICT paradigm shift: from components to services, composed and reconfigured dynamically in a demand-driven way
- Trustworthy service may interact with others causing novel trust and security problems
- Validation of composition of individual services into service-oriented architectures dramatically needed
The consortium

Industry
• IBM Zurich Research Labs
• OpenTrust Paris
• SAP Research France
• SIEMENS AG Munich

Expertise
• Service-oriented enterprise architectures
• Security solutions
• Standardization and industry migration

Academia
• Università di Verona
• ETH Zurich
• INRIA Lorraine
• UPS-IRIT Toulouse
• Università di Genova
• IEAT Timisoara

• Automated security validation
• Formal methods
• Security engineering

Main objectives and principles

Platform for formal specification and automated validation of trust and security of SOAs
– First formal language for specifying trust and security properties of services, their policies, and their composition into service-oriented architectures
– Automated toolset supporting the above
– Library of validated industrially-relevant case studies

Migration of platform to industry and standardization organizations
– Speed-up development of new service infrastructures
– Enhance their security and robustness
– Increase public acceptance of SOAs
Project results and innovation

Impact: industry migration

- Services need to be securely combined according to evolving trust and security requirements and policies
- A rigorous demonstration that a composed SOA meets the security requirements and enforces the application policy will
  - significantly increase customers’ confidence
  - enable them to fully exploit the benefits of service orientation
- **Integration of AVANTSSAR Platform in industrial development environment**

- **The AVANTSSAR Platform will advance the security of industrial vendors’ service offerings: validated, provable, traceable**
- AVANTSSAR will thus significantly strengthen the competitive advantage of the products of the industrial partners
Impact: industry migration

- Services need to be securely combined according to evolving trust and security requirements and policies
- A rigorous demonstration that a composed SOA meets the security requirements and enforces the application policy will
  - significantly increase customers’ confidence
  - enable them to fully exploit the benefits of service orientation
- Integration of AVANTSSAR Platform in industrial development environment
  - The AVANTSSAR Platform will advance the security of industrial vendors’ service offerings: validated, provable, traceable
  - AVANTSSAR will thus significantly strengthen the competitive advantage of the products of the industrial partners

E-business impact example (from project SERENITY): Loan Origination Process

- Customer
- Pre-processing clerk
- Credit Bureau
- Post-processing clerk
- Manager
E-business impact example (from project SERENITY):
Loan Origination Process

Customer

Pre-processing clerk

Credit Bureau

Post-processing clerk

Manager
E-business impact example (from project SERENITY): Loan Origination Process

Customer
- Request loan

Pre-processing clerk
- Customer identification

Credit Bureau
- Check credit worthiness

Post-processing clerk
- Check internal rating

Manager

No
No
No
E-business impact example (from project SERENITY):
Loan Origination Process

Customer
- Request loan

Pre-processing clerk
- Customer identification

Credit Bureau
- Check credit worthiness
  - Yes
  - No

Post-processing clerk
- Check internal rating
  - Yes
  - No

Manager
- Calculation of the loan
E-business impact example (from project SERENITY):
Loan Origination Process

Customer
- Request loan

Pre-processing clerk
- Customer identification

Credit Bureau
- Check credit worthiness
  - Yes: Manager
  - No: Post-processing clerk

Post-processing clerk
- Check internal rating
  - Yes: Calculation of the loan
    - Yes: Print the form
    - No: Manager
  - No: Manager

Manager
- Sign the form

Sign the form
### E-business impact example (from project SERENITY): Loan Origination Process

<table>
<thead>
<tr>
<th>Customer</th>
<th>Request loan</th>
<th>Sign the form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-processing clerk</td>
<td>Customer identification</td>
<td></td>
</tr>
<tr>
<td>Credit Bureau</td>
<td>Check credit worthiness</td>
<td></td>
</tr>
<tr>
<td>Post-processing clerk</td>
<td>Check internal rating</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td>Calculation of the loan</td>
<td></td>
</tr>
<tr>
<td>Open Account</td>
<td>Print the form</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer</th>
<th>Request loan</th>
<th>Sign the form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-processing clerk</td>
<td>Customer identification</td>
<td></td>
</tr>
<tr>
<td>Credit Bureau</td>
<td>Check credit worthiness</td>
<td></td>
</tr>
<tr>
<td>Post-processing clerk</td>
<td>Check internal rating</td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td>Calculation of the loan</td>
<td></td>
</tr>
<tr>
<td>Open Account</td>
<td>Print the form</td>
<td></td>
</tr>
</tbody>
</table>

- Yes: Calculation of the loan
- No: Open Account

---

**FP7-ICT-2007-1**
Project No. 216471
E-business impact example (from project SERENITY): Loan Origination Process

**Description:** scenario describes a customer asking for a loan

**Actors:** customer, bank, pre/post-processing clerk, manager, Credit Bureau, etc.

**Story:**
- The customer wants to buy a flat and asks for a loan
- The pre-processing clerk identifies the customer
- Several external and internal ratings need to be obtained by the post-processing clerk (Internal Credit Scoring and Credit Bureau)
- The price of the loan is calculated (amount, monthly rate, etc.)
- The contract is negotiated and signed by customer and manager

**Examples of Security requirements during Customer identification:**
- The information in the Customer Information File shall not be accessed and modified without customer authorization
- This customer authorization shall include a consent clause to advise the customer that some personal information shall be transmitted to a third thrust party (e.g Credit Bureau) for risk management purposes
- If the customer is an industrial customer, customer’s data shall be verified by a specialized clerk for enterprise account

Smart items impact example (from project SERENITY): health care

**Description:** health care scenario to monitor a patient after cardiac arrest.

**Actors:** sensor network, smart T-Shirt, e-health terminal, Health Care Center (including an Emergency Response Center (ERC), doctors, social workers, emergency team, etc), pharmacies, patients, Location Information Center (LIC), etc.

**Story:**
- Bob, 56 years old widowed man recently discharged from hospital after a cardiac arrest;
- Bob’s health to be monitored 24h a day: he carries monitoring devices that regularly measure his heart rate, blood pressure, etc and with a motion sensor providing passiveness alerts;
- These devices integrated in a smart T-shirt providing data to an e-health terminal that allows Bob to promptly communicate medical data to his doctor via the ERC;
- Bob has also subscribed an experimental programme that aims, through a sensor network, to enhance his home daily live and to provide additional data for better monitoring his health.

**Scenes:**
- scene 1: faintness alert
- scene 2: false alarm from Bob’s smart T-Shirt
- scene 3: emergency
### Smart items impact example (from project SERENITY): health care

**Bob feels giddy**

**Smart T-shirt**

**E-health terminal**

**Steps:**

1. Bob feels giddy and sends via his e-health terminal a request for assistance to ERC.

2. ERC receives the request and, since Bob’s doctor is in vacation, redirects it to Charlie.

3. Charlie analyses Bob’s medical data and history and sends to Bob an e-prescription.

4. Bob requests ERC for a medicine delivery.

5. ERC selects Alison to execute this task, sends a message to her, which she acknowledges, receiving then back the data for accomplishing this activity.

6. Alison goes to the pharmacy and after a successful credentials exchange, she gets the medicine from the pharmacist.

7. Alison delivers the medicine to Bob.

**Notes:** This request is completed with Bob’s medical data automatically retrieved by his e-health terminal by means of a query to his smart T-shirt.
Smart items impact example (from project SERENITY): health care

**Steps:**

1. Bob feels giddy and sends via his e-health terminal a request for assistance to ERC.
2. ERC receives the request and, since Bob’s doctor is in vacation, redirects it to Charlie.
3. Charlie analyses Bob’s medical data and sends to Bob an e-prescription.
4. Bob requests ERC for a medicine delivery.
5. ERC selects Alison to execute this task, sends a message to her, which she acknowledges, receiving then back the data for accomplishing this activity.
6. Alison goes to the pharmacy and after a successful credentials exchange, she gets the medicine from the pharmacist.
7. Alison delivers the medicine to Bob.

**Notes:**

The request would have been sent to Bob’s doctor, but he is in vacation and thus a doctor discovery process is activated. In the group of doctors able to substitute Bob’s doctor, Charlie is the first to answer.

Charlie retrieves Bob’s medical data and history by using his e-health terminal to query ERC. The e-prescription is sent from Charlie’s e-health terminal to Bob’s e-health terminal.
Smart items impact example (from project SERENITY): health care

Steps:
1. Bob feels giddy and sends via his e-health terminal a request for assistance to ERC.
2. ERC receives the request and, since Bob’s doctor is in vacation, redirects it to Charlie.
3. Charlie analyses Bob’s medical data and history and sends to Bob an e-prescription.
4. Bob requests ERC for a medicine delivery.
5. ERC selects Alison to execute this task, sends a message to her, which she acknowledges, receiving then back the data for accomplishing this activity.
6. Alison goes to the pharmacy and after a successful credentials exchange, she gets the medicine from the pharmacist.
7. Alison delivers the medicine to Bob.

Notes:
- Bob feels weak and instead of driving to the pharmacy to get the medicine, he prefers to be supported by the ERC for this task.
- Charlie retrieves Bob’s medical data and history by using his e-health terminal to query ERC. The e-prescription is sent from Charlie’s e-health terminal to Bob’s e-health terminal.
- Bob feels weak and instead of driving to the pharmacy to get the medicine, he prefers to be supported by the ERC for this task.
- as the others, Alison is equipped with an e-health terminal that she uses to communicate with the others health actors. In the data she receives from ERC there’ll be, properly protected, the e-prescription done for Bob.
Smart items impact example (from project SERENITY): health care

**Steps:**
1. Bob feels giddy and sends via his e-health terminal a request for assistance to ERC.
2. ERC receives the request and, since Bob’s doctor is in vacation, redirects it to Charlie.
3. Charlie analyses Bob’s medical data and history and sends to Bob an e-prescription.
4. Bob requests ERC for a medicine delivery.
5. ERC selects Alison to execute this task, sends a message to her, which she acknowledges, receiving then back the data for accomplishing this activity.
6. Alison goes to the pharmacy and after a successful credentials exchange, she gets the medicine from the pharmacist.
7. Alison delivers the medicine to Bob.

**Notes:**
- This request is completed with Bob’s medical data automatically retrieved by his e-health terminal by means of a query to his smart T-shirt.
- The request would have been sent to Bob’s doctor, but he is in vacation and thus a doctor discovery process is activated. In the group of doctors able to substitute Bob’s doctor, Charlie is the first to answer.
- Charlie retrieves Bob’s medical data and history by using his e-health terminal to query ERC. The e-prescription is sent from Charlie’s e-health terminal to Bob’s e-health terminal.
- Bob feels weak and instead of driving to the pharmacy to get the medicine, he prefers to be supported by the ERC for this task.
- The credentials exchange is between Alison’s e-health terminal and the pharmacist’s computer. Besides the validity of the e-prescription, Alison authorization to get the medicine in behalf of Bob needs to be checked.
- This last step involves an exchange of electronic credential between Bob and Alison. Their e-health terminals are used at this purpose.
3 Project Presentation Poster

The following poster has been displayed at the Bled conference on “The Future of the Internet” (www.fi-bled.eu) and will be used to present AVANTSSAR at future meetings.
**AVANTSSAR**

**Automated VAlidatioN of Trust and Security of Service-oriented ARChitectures**

FP7-ICT-2007-1, ICT-1.1.4, STReP project no. 216471

### Project motivation

- ICT paradigm shift: from components to services, composed and reconfigured dynamically in a demand-driven way
- Trustworthy service may interact with others causing new trust and security problems
- Validation of composition of individual services into service-oriented architectures (SOAs) dramatically needed

### Main objectives, principles, and innovation

- **Platform for formal specification and automated validation of trust and security of SOAs**
  - First formal language “ASLan” for specifying trust and security properties of services, their policies, and their composition into service-oriented architectures
  - Automated toolset supporting the validation of ASLan specifications
  - Library of validated ASLan specifications of industrially-relevant case studies

- **Migration of platform to industry and standardization organizations**
  - Speed up development of new service infrastructures
  - Enhance their security and robustness
  - Increase public acceptance of SOAs

The AVANTSSAR Platform will advance the security of industrial vendors’ service offerings in terms of their validation, provability, traceability

### The consortium

**Academia:** Università di Verona, ETH Zurich, INRIA Lorraine, UPS-IRIT Toulouse, Università di Genova, IEAT Timisoara

**Industry:** IBM Zurich Research Labs, OpenTrust Paris, SAP Research Sophia Antipolis, Siemens AG Munich

www.avantssar.eu
4 Project Website

The URL of the project is www.avantssar.eu (as well as www.avantssar.org, which redirects visitors to the main address).

The website is divided in a public area and in an area to which access is restricted to authorized users. The public area contains general information about the project, links to the project partners and the researchers working in the different sites, news about the project and events organized by the project partners, the public documents that have been generated by the project (publications and public deliverables), and a page of links to related projects or events.

The restricted area contains the confidential information and material that is intended for communication between the project partners (who also exchange information and material by means of an svn repository) and between the project partners and the European Commission.