



Automated VALidatioN of Trust and Security  
of Service-oriented ARchitectures

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

[www.avantssar.eu](http://www.avantssar.eu)

---

## Deliverable D1.2 Basic Dissemination and Use Plan

### Abstract

This document describes the basic plan for the actions and activities that will be taken to disseminate and use the knowledge and results obtained in the AVANTSSAR project. The Final Dissemination and Use Plan will be delivered on month 36 of the project.

### Deliverable details

Deliverable version: *v1.1*

Date of delivery: *30.06.2008*

Classification: *public*

Editors: *UNIVR*

Person-months required: *0.5*

Due on: *30.06.2008*

Total pages: *23*

### Project details

Start date: *January 01, 2008*

Project Coordinator: *Luca Viganò*

Partners: UNIVR, ETH Zurich, INRIA, UPS-IRIT, UGDIST, IBM,  
OpenTrust, IEAT, SAP, SIEMENS



## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Overview and General Approach</b>	<b>3</b>
2.1	Overview of expected results . . . . .	3
2.2	Management of knowledge and intellectual property . . . . .	4
2.3	Approach to Dissemination and Use . . . . .	6
2.4	Market projections . . . . .	8
<b>3</b>	<b>Description of the Dissemination Plan</b>	<b>10</b>
3.1	Web presence and information exchange . . . . .	10
3.2	Project Workshops and Conferences, Lectures, Tutorials . . . . .	10
3.3	Publications . . . . .	13
3.4	Local dissemination by industrial project partners . . . . .	14
3.4.1	IBM . . . . .	14
3.4.2	OpenTrust . . . . .	14
3.4.3	SAP . . . . .	15
3.4.4	SIEMENS . . . . .	16
3.5	Clustering and standardization . . . . .	16
3.5.1	Clustering . . . . .	16
3.5.2	Contributions to standards . . . . .	19
<b>4</b>	<b>Description of the Use Plan (by result)</b>	<b>21</b>
4.1	The AVANTSSAR Platform . . . . .	21
4.2	Specification Languages . . . . .	22
4.3	Automated reasoning techniques . . . . .	22
4.4	The AVANTSSAR Library of validated SOA problem cases . . . . .	22

# 1 Introduction

AVANTSSAR is an R&D STREP project funded by the European Commission under the FP7-ICT Theme Work Programme 2007-2008, Challenge 1, Objective 1.4: “Secure, dependable and trusted Infrastructures”. This document is the Basic Dissemination and Use Plan for AVANTSSAR, and is structured as follows:

- In section 2, “Overview and General Approach”, we give an overview of the expected results, along with our approach to dissemination and use, and some market projections.
- In section 3, “Description of the Dissemination Plan”, we describe the web-site we have set up, the conferences, events, and publications by means of which we will disseminate our results, and the clustering and standardization relevant to AVANTSSAR.
- In section 4, “Description of the Use Plan (by result)”, we describe the use plans for each of the main expected results.

The Final Dissemination and Use Plan will be delivered on month 36 of the project.

## 2 Overview and General Approach

### 2.1 Overview of expected results

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.

Deploying 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.

AVANTSSAR proposes a technology for the formal specification and Automated VALIDation of Trust and Security of Service-oriented ARchitectures. This technology will include an integrated toolset, the AVANTSSAR Validation Platform, which will be tuned on relevant industrial case studies. More specifically, the project will develop:

<i>Result</i>	<i>Type</i>	<i>D/U</i>	<i>Due at month</i>
ASLan	Technical report	U	30
Automated reasoning techniques	Technical report	U	34
AVANTSSAR Validation Platform	Software	D&U	36
AVANTSSAR Library	Electronic repository	D&U	36

Table 1: Overview of the main results (D=dissemination, U=use)

- *ASLan*, the first formal language for specifying trust and security properties of services, their associated policies, and their composition into service architectures.
- Automated techniques to reason about services, their dynamic composition, and their associated security policies into secure service architectures.
- The *AVANTSSAR Validation Platform*, an automated toolset for validating trust and security aspects of service-oriented architectures, depicted in Figure 1.
- A library of validated composed services and service architectures, proving that the AVANTSSAR technology scales to envisaged applications.

Migrating project results to industry and disseminating them to standardization organizations will speed up the development of new network and service infrastructures, enhance their security and robustness, and increase the public acceptance of emerging IT systems and applications based on them. The main envisioned results of AVANTSSAR are summarized in Table 1, together with their type and timing, as well as an indication of whether they are for dissemination and/or use.

## 2.2 Management of knowledge and intellectual property

All project partners have signed a Consortium Agreement before the start of the project, setting the principles of the consortium management and placing the relationship between the partners and their responsibilities on a legal basis for the duration of the work. In particular, the agreement includes specific arrangements concerning intellectual property rights to be

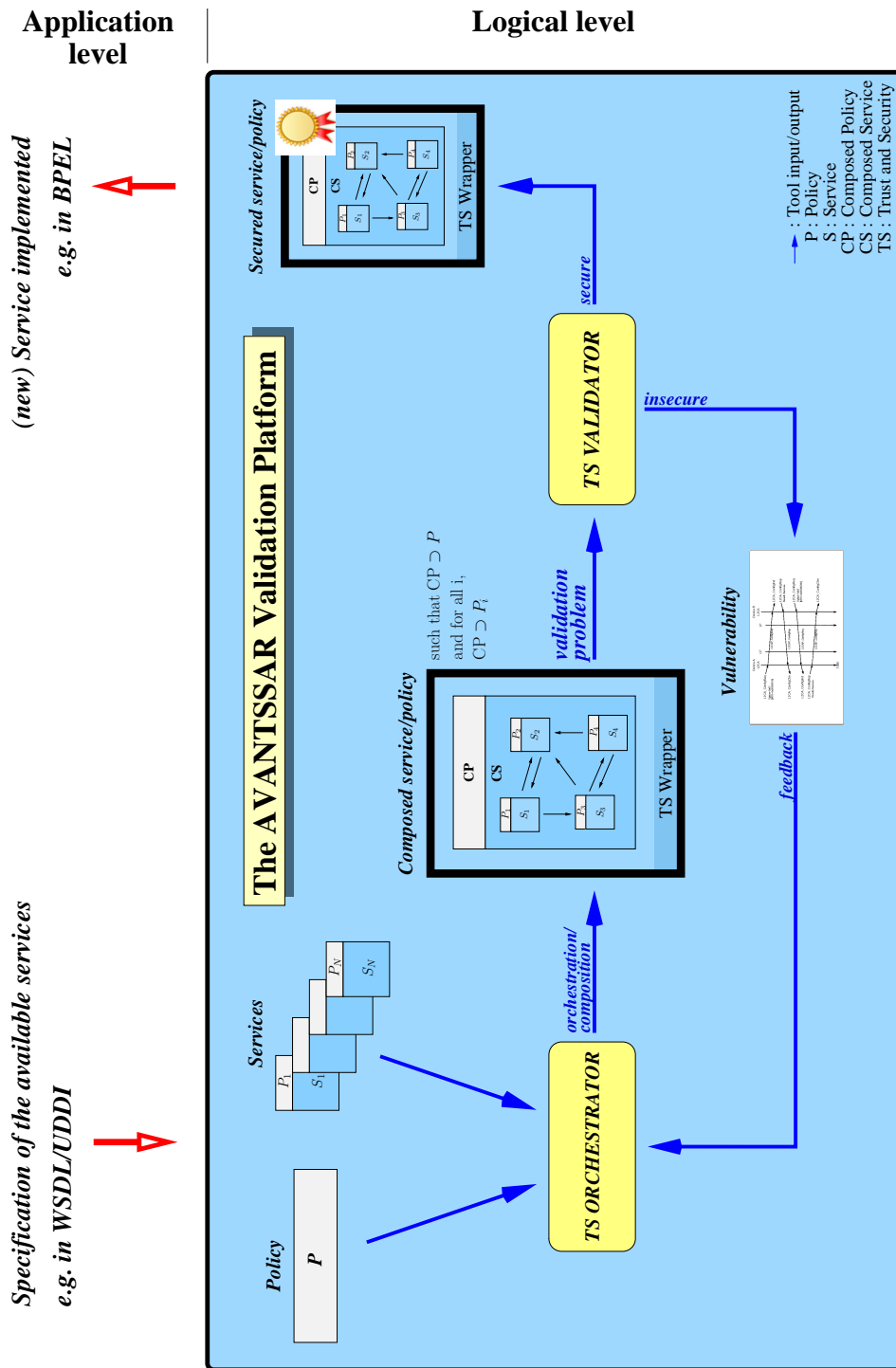


Figure 1: The AVANTSSAR Validation Platform and its usage towards Enterprise SOA (*TS* abbreviates *Trust and Security*).

applied among the participants and their affiliates, in compliance with the general arrangements stipulated in the contract. It thus specifies the rules for dissemination and use (confidentiality, ownership of results, patent rights, exploitation of results, protection and dissemination of knowledge), as well as financial and legal provisions.

### 2.3 Approach to Dissemination and Use

The AVANTSSAR project represents an unprecedented effort to apply automated validation methods to trust and security aspects of service-oriented architectures comprising of composed services, and we thus expect that it will generate a large interest in both academia and industry. Dissemination and use of foreground will have a high priority in this proposal and the WP 6 will be devoted to all the activities relevant to accomplishing this task.

We have thus planned appropriate measures to ensure an effective and timely dissemination of the project results to potential users, both at the European level and worldwide. The main targets of the dissemination activity will be industry, research institutions, and standardization bodies working on the design of Web Services and service-oriented architectures, focussing in particular on their trust and security aspects. Moreover, since the European Society as a whole will ultimately benefit from the results of the project (in terms of increased reliability and acceptance of, and confidence in, service-oriented architectures, in particular in e-health, e-government, e-market, etc.), special measures are planned to reach the public.

Dissemination to industry, research institutions and standardization bodies, as well as to European citizen, will be carried out by a variety of means:

- Talks at relevant international conferences, events and forums (both presenting the technical achievements and introducing at a high level the project's objectives and results).
- Publication of papers in proceedings of international conferences and events, as well as in international scientific journals.
- Organization of conferences and workshops on project-related topics, including "project workshops" where attendance of external experts and professionals is based on invitation.
- Organization of tutorials and thematic schools.
- Design and management of a publicly available web-site that includes descriptions of the main project results and allows the download of

the AVANTSSAR Validation Platform and of the library of validated composed services and service architectures.

- Press conferences and press releases describing the advancement and main results of the project, so to reach and make the public aware of both the short-term and long-term impact of the project results.
- SIEMENS and SAP are members of ForTIA (<http://www.fortia.org/>), the *Formal Techniques Industrial Association*, which is a subgroup of *Formal Methods Europe (FME)*. Since its goals include “to ensure that good tools and techniques are researched, developed and deployed”, ForTIA will have an active interest in applying and disseminating the formal methodology to be developed in AVANTSSAR.

The new techniques and methodologies, the formal models of the case studies, as well as the prototype tool for the automated validation of trust and security in composed services developed by the project will be of interest to researchers and professionals working on the design of new secure services. The AVANTSSAR consortium will aim at making available techniques, formal models of the case studies, and tools in order to provide support and to encourage designers to use the project’s results. We do not believe that automatic tools for the security validation of services will be attractive enough for a commercial market for reasons of potential market volume and appropriate pricing. On the other hand, all efforts should be made to increase the chance of AVANTSSAR being accepted as a de facto standard methodology and toolset within standardization bodies, thus opening a market for consulting and services relating to the security validation of services. We will implement the following measures in order to release our techniques, models, and tools outside the consortium and to stimulate the exploitation of the AVANTSSAR results by industry and standardization bodies:

- Development of the AVANTSSAR Validation Platform, i.e. a software suite for the automatic security validation of services. The release of the software, the documentation, and the formalization of the case studies will be considered: we aim at the public availability of an automatic tool supporting the security validation of services which would be the main vehicle for the exploitation of the result both by the partners involved in the project as well as by industries or standardization bodies. New versions of the AVANTSSAR Validation Platform will be released regularly and a mailing list for the users set up and supported by the consortium.

- Organization of educational activities. As remarked above, we will transfer the results of AVANTSSAR in educational activities within industry, universities, workshops, working groups or standardization organizations (e.g. AVANTSSAR workshops, theses, course materials, presentations at standardization committees, invited short courses at visited universities, etc). At least 3 such educational activities will be carried out, with the direct involvement of academic and industrial partners of the consortium.
- Organization of the “AVANTSSAR Technology Migration Workshop”, presumably in the context of the ForTIA industrial interest group on formal methods, mentioned above. This event is specifically targeted to service designers from industry and standardization bodies in which methods, techniques, tools, case studies, and success stories developed within the project will be publicly presented.

Additionally, the industrial partners in the consortium will use the results of the project (namely, the formal models of the services and the automated validation techniques and tools) in the design and development process of their products in order to reduce the security-related risk and, thus, contribute to the reduction of the total cost of ownership. The AVANTSSAR case studies will provide the test bed for potential integration of the AVANTSSAR results into the companies’ development environments and procedures.

## 2.4 Market projections

The Web Services technology has been analyzed to have very high potential, especially as the most prominent implementation basis for SOA (Service-Oriented Architectures). Many vendors, Microsoft in particular but also IBM, have heavily invested into Web Services platforms. Also SAP has committed itself to base its platform on SOA principles.

So far, Web Services do not dominate the IT infrastructure of enterprises, but this is to be explained by the lack of maturity in the Web Services standards; standards play an essential role, as the promises of SOA, i.e. flexibility and interoperability, can only be realized by using standards.

The WS-\* specification stack was initially proposed by Microsoft and IBM in 2002, and the main security specifications, i.e. WS-Security, WS-Trust, WS-SecureConversation and WS-SecurityPolicy, are now OASIS standards.

The main field where Web Services and the Web Services security standards are used today is the communication across enterprises, i.e. identity

federation, which is a growing area, specially suitable for the Web Services technology, where new investments are made, and where security is of course very important. Moreover, at the moment, a strong trend towards “SOA-fication” is observable across many industries including SIEMENS, SAP, and IBM.

The SIEMENS directory product, DirX, already offers Web services interfaces and implements most Web Services security standards. The main platform at SIEMENS Enterprise Networks, Open SOA, implements the SOA principles, and there are also plans to make the main platform at MED, Soarian, compatible with SOA. All the AVANTSSAR application scenarios provided by SIEMENS have immediate or at least near-term relevance for the SIEMENS business. The IT security department at SIEMENS Corporate Technology is currently involved in three projects that deal with secure software distribution and updates, in the areas of aviation, automotive, and medical infrastructure. SIEMENS Healthcare Infrastructure has started applying Web Service based solutions for the secure exchange of electronic patient/health records among hospitals. SIEMENS IT Solutions and Services is developing secure Web Services for e-government products conforming, among others, to the EU service directive.

With SAP Business ByDesign—the most complete on-demand business software solution specifically addressing a new market of prospective, fast-growing midsize customers—the technical advantages of SOA enter the level of business processes and allow SAP customers to exploit the full potential of new business trends without becoming IT experts. Quality and security play a fundamental role in the acceptance and usage of SAP Business ByDesign and similar software products in the marketplace of midsize companies. Being able to rigorously demonstrate that a given set of services composed in a particular way meets security requirements and enforces the application security policies is crucial to increase customers’ confidence and enable them to fully exploit the benefits of service orientation. Automating such validation is key, since it serves for reduced additional effort and smooth integration in the existing development environment. The AVANTSSAR results provide the necessary qualities and will contribute to advance the traceable security of both SAP’s and independent vendor’s service offerings beyond the current state-of-the-art. A successful migration of the AVANTSSAR platform in the SAP development environment would clearly add to the competitive advantage of SAP products in the marketplace.

In general, the validation of trust and security properties will become a fundamental part of the design process for Web Services. Also the confidence for using information technology for privacy-sensitive applications ranging from online shopping to health care can be improved by the vali-

dition of privacy-friendly technology such as IBM's anonymous credential system Identity Mixer.

## 3 Description of the Dissemination Plan

### 3.1 Web presence and information exchange

The website of the AVANTSSAR project is

[www.avantssar.eu](http://www.avantssar.eu)

and includes:

- A general introduction to the project: the objectives, the expected results, the milestones, the detailed description of the consortium and its coordinates within the Seventh Framework Programme.
- The list of events taking place in the context of the project: meetings, conferences, workshops, and their availability to the public.
- Publications originated from the project, both in the scientific community and in the general press.
- A number of relevant links: other projects, institutions and companies that are related to AVANTSSAR.
- An internal protected section, containing contact details, internal mailing lists, details about the meetings (slides, notes and so on) and other temporary technical information needed by the consortium.
- A protected section containing the deliverables and other documents for the European Commission.

Besides for the website, communication and information exchange among the members of the project is enforced via a carefully organized and maintained central repository and a number of dynamically created mailing lists.

### 3.2 Project Workshops and Conferences, Lectures, Tutorials

Three Project Workshops will be organized, in 2008, 2009, and 2010.

The first two workshops will be attended by all members of the AVANTSSAR project and we will invite as guests a small number of international researchers and professionals who are working on related problems.

The third workshop will be open to external participants (possibly with contributions selected by peer reviewing) and we aim to have published proceedings. Together with the third workshop, we also plan to organize a one-day “Dissemination Workshop” with invited speakers representing the main actors in IT security: industry, research, standardization bodies, government, and funding agencies. In order to maximize the dissemination of the project results, we plan to organize this event in the context of a major scientific event such as, e.g., a meeting of the IETF or an international conference on information security.

Additionally, the members of AVANTSSAR will play an active role in the organization of a number of scientific events, some of which are already scheduled:

- ARSPA is a series of workshops on *Automated Reasoning for Security Protocol Analysis* that was started during the AVISPA project (the predecessor of AVANTSSAR) and that will be carried on in the context of AVANTSSAR.
- FCS-ARSPA-WITS’08: the *Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security* was held in Pittsburgh, PA, USA, June 21-22, 2008, in affiliation with LICS 2008 and CSF 21. Luca Viganò of UNIVR was one of the co-chairs of the workshop. More information is available on the project’s website <http://profs.sci.univr.it/~vigano/fcs-arspa-wits08>.
- ARSPA-WITS’09: in 2009, ARSPA will again join forces with the WITS workshop, in the context of the ETAPS 2009 conference (22-29 March, 2009, York, UK). The co-chairs of ARSPA-WITS’09 will be Pierpaolo Degano (of the University of Pisa) and Luca Viganò of UNIVR.
- SAC’08 Security Track: the *23rd ACM Symposium on Applied Computing* is a multi-track symposium under the auspices of ACM. It was held in Fortaleza (Brazil) March 16-20, 2008. Giampaolo Bella of SAP chaired the Security Track. Details can be found at <http://www.dmi.unict.it/~giamp/sac/08cfp.html>.
- SAC’09 Security Track: the *24th ACM Symposium on Applied Computing* will be held in Honolulu (USA) March 8-12, 2009. Giampaolo Bella and Luca Compagna of SAP will chair the Security Track. Details can be found at <http://www.dmi.unict.it/~giamp/sac/09cfp.html>.

- LORIA Thematic Day on Web Service Verification (end of 2008/beginning 2009).
- ForTIA industry day at FM'08 (28 May 2008, Holiday Club Turku, Finland), which was co-chaired by Jorge Cuellar of SIEMENS.
- IeAT will consider organizing a security workshop jointly with the 2009 edition of the SYNASC International Symposium on Symbolic and Numeric Algorithms for Scientific Computing in Timisoara, possibly jointly with an AVANTSSAR project meeting. (IeAT has hosted two similar workshops in the past.)
- Invited talk titled “*Security, a Sisyphean task? A personal view.*” at the University of Genova, June 18, 2008, held by Jorge Cuellar of SIEMENS.
- Invited talk “*Software Model Checking: new challenges and opportunities for Automated Reasoning*” at the 1st Workshop on Practical Aspects of Automated Reasoning (PAAR-2008), August 10, 2008, Sidney, Australia, held by Alessandro Armando of UGDIST.
- Invited talk on automated verification of security-sensitive service-oriented architectures at the Workshop on Logic and Information Security, September 22-26, 2008, Leiden University, Holland, held by Alessandro Armando of UGDIST.
- Classes on network and systems security at the University of Verona, held every year by Luca Viganò of UNIVR.
- Classes on security protocol design and verification at the University of Genova, 2008, held by Alessandro Armando of UGDIST.
- Classes on “*Sécurité des systèmes informatiques: cryptographie et protection des données*” to 5<sup>th</sup> year students at the “*Institut National d’Informatique*” in Algiers, the Université Libanaise in Beirut and the Université Paul Sabatier in Toulouse, held every year by Philippe Balbani of UPS-IRIT.
- Class on access control to 5<sup>th</sup> year students at the Université du Mirail Toulouse 2, held by Yannick Chevalier of UPS-IRIT.
- Class on formal methods for security policies at the University of Los Andes, Bogotá, Columbia, May 2008, held by Jorge Cuellar of SIEMENS. The class will be repeated in 2009.

- Class on formal methods for Web Services at the University of Washington, Seattle, USA, Jul/Aug 2008, held by Jorge Cuellar of SIEMENS.

Moreover, we aim to present our work at international conferences and forums on computer security, software architectures, and automated reasoning.

### 3.3 Publications

We aim to publish the results obtained in AVANTSSAR in the proceedings of international events and in international journals on computer security, software architectures, and automated reasoning. The AVANTSSAR consortium has already achieved the following publications (available on the project's website):

- P. Balbiani, F. Cheikh, G. Feuillade. *Composition of interactive Web services based on controller synthesis*. In Proceedings of the 2<sup>nd</sup> International Workshop on Web Service Composition and Adaptation (WSCA-2008). IEEE Computer Society, to appear.
- P. Balbiani, F. Cheikh, G. Feuillade. *Algorithms and complexity of automata synthesis by asynchronous orchestration with applications to Web services composition*. In Proceedings of the 1<sup>st</sup> Interaction and Concurrency Experience (ICE'08). Electronic Notes in Theoretical Computer Science, to appear.
- P. Balbiani, Y. Chevalier, M. El Hourri. *A logical approach to dynamic role-based access control*. In Proceedings of the 13<sup>th</sup> International Conference on Artificial Intelligence: Methodology, Systems, Applications (AIMSA 2008). Springer-Verlag, to appear.
- D. Basin, C. Caleiro, J. Ramos, L. Viganò. *A Labeled Tableaux System for the Distributed Temporal Logic DTL*. In Proceedings of the 15<sup>th</sup> International Symposium on Temporal Representation and Reasoning (TIME'08), pages 101–109, IEEE Computer Society Press, 2008.
- Y. Chevalier, M. Anis Mekki, M. Rusinowitch. *Automatic Composition of Services with Security Policies*. In Proceedings of the 2<sup>nd</sup> International Workshop on Web Service Composition and Adaptation (WSCA-2008), held in conjunction with 6th IEEE International Conference on Services Computing (SCC-2008), Honolulu, USA, 2008.

- M. Maidl, D. von Oheimb, P. Hartmann, R. Robinson. *Formal Security Analysis of Electronic Software Distribution Systems*. In Proceedings of the 27<sup>th</sup> International Conference on Computer Safety, Reliability and Security (SAFECOMP), Springer, LNCS, 2008.

Several other papers describing work carried out in the context of the project are currently under reviewing.

### 3.4 Local dissemination by industrial project partners

#### 3.4.1 IBM

IBM will use the AVANTSSAR Validation Platform for the analysis of the anonymous credential system Identity Mixer developed by IBM, which requires the full range of features that the AVANTSSAR technology has to offer. Besides this, IBM will consider using AVANTSSAR for the validation of security aspects of other Web Services related applications.

#### 3.4.2 OpenTrust

The dissemination of the AVANTSSAR project results at OpenTrust will be done in two phases. Each phase targets a different audience.

**Phase 1: internal dissemination** The first phase consists in internal company dissemination targeting developers and managers, so to inform the OpenTrust team members who did not participate in the project about the results: talks will be given by OpenTrust contributors to present the collection of languages, tools and validations that are output by the project.

OpenTrust commercializes a variety of products that make intensive use of Web Services, mainly OpenTrust PKI and Crypt&Share, a software for secure file exchange via Internet. Learning sessions will be organized by contributors, specifically for product designers where more advanced aspects of the AVANTSSAR methodologies and technologies will be addressed. A couple of scenarios from their products will be modeled and validated. Moreover, project managers will get involved in order to define a new methodology that integrates AVANTSSAR validation into project management processes. A reference document will be agreed upon and used whenever new customer scenarios appear from business opportunities. An internal meeting will be organized to collect feedback about the available results and learning materials (presentations, tutorials, samples, ...).

**Phase 2: external dissemination** Feedback from Phase 1 will be used to prepare dissemination for external audience: clients and partners. OpenTrust often relies on partners in order to integrate its solutions into client information systems. Consequently, partners, as well as clients, need a deep knowledge of the security aspects of the products. An initiation to AVANTSSAR technologies will be proposed to them as a complement to product training sessions.

A tutorial will be available and further learning sessions will be organized when needed. This will help designing secure services and making safe use of the product features.

### 3.4.3 SAP

SAP Research is going to be the main actor in the industry migration activity that will be carried out in WP 6 according to the following plan:

1. SAP Research will interact with SAP development units to understand their methodologies and needs in matter of both (i) specification languages and modeling artifacts, and (ii) integration of the AVANTSSAR Validation Platform.
2. An industrially-suited specification language (ISSL) will emerge on top of ASLan (as developed in WP 2), taking into account the requirements provided by SAP development units in the previous phase.
3. An industrial prototypical instance of the AVANTSSAR Validation Platform will be constructed based on the prototype developed in WP 4 and considering the requirements emerging from the first phase.
4. The SAP development environment will be reproduced under the perimeter of SAP Research as experimental prototype environment on which SAP Research will test, tune, and assess the ISSL and the industrial prototypical instance of the AVANTSSAR Validation Platform against one of the SAP scenario.

With the ultimate goal of realizing such a migration plan, an intensive internal dissemination activity is currently underway towards other SAP Research Program groups and SAP's business group such as the Netweaver Security and Identity Management team, the Netweaver modeling team, the Application Platform cross-development team, the AP Security team and AP foundation.

### 3.4.4 SIEMENS

SIEMENS is going to use the AVANTSSAR techniques and tools in their current and future security analysis and consulting projects for customers, e.g. at Continental VDO, Boeing Phantom Works, and the Rhön-Klinikum AG. This includes security analysis at early system design stages in the context of tendering procedures for e-Health and e-Government applications like electronic health record management systems and national and EU-wide citizen and service portals.

## 3.5 Clustering and standardization

### 3.5.1 Clustering

This section indicates some projects and organizations relevant to the ongoing work (at world-wide, European or national level) and with which information exchange might be beneficial.

#### World

- SIEMENS presentations planned at:
  - OASIS technical committees on SOA,  
[http://www.oasis-open.org/committees/tc\\_cat.php?cat=soa](http://www.oasis-open.org/committees/tc_cat.php?cat=soa)
  - W3C working groups on Web Services,  
<http://www.w3.org/2002/ws/#groups>
- UNIVR presentations planned at the IFIP WG 1.7 *Theoretical Foundations of Security Analysis and Design*, [http://www.dsi.unive.it/IFIPWG1\\_7/](http://www.dsi.unive.it/IFIPWG1_7/). Luca Viganò of UNIVR has been recently nominated as a member of this working group.

#### EU

Project presentations are planned at events organized by the European Commission, such as The Future of The Internet Conference ([www.fi-bled.eu](http://www.fi-bled.eu)), which was held in Bled, Slovenia, March 31 – April 2, 2008, and at which the project was presented.

Members of the AVANTSSAR consortium participate in (or are in close contact with the initiators and members of) several related European projects, including:

- ARTIST2: FP6 Network of Excellence on Embedded Systems Design. Sep 2004 – Aug 2008, <http://www.artist-embedded.org/artist>.
- ARTISTDesign: FP7 Network of Excellence on Design of Embedded Systems. Jan 2008 – Dec 2011, <https://www.control.lth.se/project/ArtistDesign>.
- DEPLOY: Industrial deployment of system engineering methods providing high dependability and productivity. FP7 project, Feb 2008 – Jan 2012, <http://www.deploy-project.eu/index.html>.
- MASTER: Managing Assurance, Security and Trust for sERVICES. FP7 project, Feb 2008 – Jan 2011, <http://www.master-fp7.eu/index.php>.
- PRIME: Privacy and Identity Management for Europe. FP6 project, March 2004 – May 2008, <http://www.prime-project.eu>.
- PrimeLife: Bringing sustainable privacy and identity management to future networks and services. FP7 project, Mar 2008 – Feb 2011, <http://www.primelife.eu>.
- R4eGov: Towards e-Administration in the large. FP6 project, Mar 2006 – Feb 2009, <http://www.r4egov.eu>.
- SENSORIA: Software Engineering for Service-Oriented Overlay Computers, FP6 project, Sep 2005 – Aug 2009, <http://www.sensoria-ist.eu>. Luca Viganò of UNIVR gave an invited presentation of AVANTSSAR at a Sensoria meeting held in Munich, Germany, March 11–14, 2008.
- SERENITY: System Engineering for Security and Dependability. FP6 project, Jan 2006 – Dec 2008, <http://www.serenity-forum.org>.
- WASP: Wirelessly Accessible Sensor Populations. FP6 project, Sep 2006 – Feb 2010, <http://www.wasp-project.org>.

Some of the members of the AVANTSSAR team, including ETH Zurich, INRIA, SAP, SIEMENS, and UNIVR also participate, at different levels, in the activities of the European Research Consortium in Informatics and Mathematics (ERCIM). In particular, ERCIM has recently set up a specific Working Group on Security and Trust Management, which aims at steering the research of ERCIM institutions on a series of activities (e.g., research projects, workshops, dissemination of knowledge) for fostering the European

research and development on security, trust and privacy in ICT. These are among the main issues of current and future research efforts for “security in Europe” (cf., for example, <http://www.cordis.lu/security>). We thus expect that the results of AVANTSSAR will be beneficial for this ERCIM WG, which will in turn provide a major forum for the peer-evaluation and dissemination of our results.

### France

INRIA and UPS-IRIT participate in:

- ARA SSIA COPS: Composition Of Policies and Services, a 3-year national project (with LIM Marseille) funded by Agence Nationale de la Recherche, which started in December 2005. The aim is to build technologies enabling the security analysis of Web Services that take into account the potential flaws at communication level, at the access policy level or at the interface between communications and access policy.

### Germany

SIEMENS participates in:

- BITKOM AK (working group) SOA Technologies, [http://www.bitkom.org/de/themen\\_gremien/18151.aspx](http://www.bitkom.org/de/themen_gremien/18151.aspx)
- CAST workshops on SOA Security, <http://www.cast-forum.de/workshops/infos/103>
- TeleTrust project group SOA Security, <http://teletrust.de>

### Romania

- Practical Formal Verification Using Automated Reasoning and Model Checking. INTAS research grant 8144, Sep 2006 – Feb 2009, <http://www.risc.uni-linz.ac.at/projects/intas>
- CONQUERS: Continuous Quality Evaluation and Restructuring of Software. Romanian national research grant, Oct 2007 – Sep 2010.

### Switzerland

- ETH Zurich is involved in the project VerSePro (funded by the Swiss National Science Foundation SNSF) together with the Ecole Polytechnique Federale de Lausanne EPFL. This 4-year project, which started

in the autumn of 2005, aims at the development and verification of security and privacy protocols for wireless networks. We thus expect that it will be possible to re-use in AVANTSSAR some of the techniques developed in VerSePro and vice versa. Furthermore, ETH Zurich is involved in the project ComposeSec (funded by the Hasler Foundation). This 3-year project started in September 2007, and aims at analysing complex protocol suites or services built by combining networked components. The goal of this project is to develop effective compositional methods, with accompanying tool support, to tackle this problem. This includes foundational work on bridging the gap between currently used security protocol models and high-level analysis models of composed services.

### 3.5.2 Contributions to standards

There is considerable motivation in industry for standardizing the basic constituents of the infrastructure for service interoperability over the Internet since this avoids the development of proprietary, incompatible solutions and it is considered to be the best approach to make long-term decisions and to achieve long product cycles.

AVANTSSAR has the potential to provide the reference assessment technology for the validation of security services that have already been standardized or are undergoing standardization. This potential can be realized by providing an effective tool with wide coverage that features push-button automation, which should increase the acceptance and dissemination of the approach. AVANTSSAR significantly contributes to the strong European position in verification of security properties of security-critical systems, which in turn enables the European industry to provide high-quality products and solutions with rigorously assessed properties.

The contribution of AVANTSSAR to both the security verification community and the security services developers community, including key standardization bodies, will be supported by a broad spectrum of dissemination activities in the context of WP 6. Moreover, the results obtained by AVANTSSAR can be immediately exploited in industry. For instance, SIEMENS has a substantial interest in supporting its standardization work in IETF, OASIS, and other bodies by means of rigorously validating its proposals and thus increasing their acceptance. Previous experience (e.g. the UMTS authentication and key exchange protocol standardized by 3GPP, the H.530 authentication protocol for multimedia standardized at ITU, and the EAP authentication protocols standardization at the IETF) showed that verification can be the key to ensuring correctness and therefore acceptance

in standardization. The automation provided by the AVANTSSAR approach will substantially reduce the effort involved, enabling formal analysis to be carried out as a routine, every-day activity, thus leading to substantial increase in quality of standardized solutions.

The main ideas to transfer the results of AVANTSSAR to standardization will be (a) to propose individual secured services (time stamping, mail services, authentication services, notary services, etc., or their interfaces) resulting as solutions from our case studies to standardization, and (b) to propose extensions to one or several standard languages, via an XML namespace, identified by a AVANTSSAR-URI reference, to describe the industrially-suited specification languages ISSL or ASLan specific policies needed to automatically integrate Web Services with AVANTSSAR. Another possibility of linking and binding the Web Service to AVANTSSAR is via RDF or an Ontology or Rule language. The languages to be extended could be in particular WS-SX, WSBPEL, WS-CDL, WSDL, or WS-Agreement:

**WS-SX** (<http://www.oasis-open.org/committees/ws-sx>) has three standards: WS-SecureConversation, WS-SecurityPolicy, and WS-Trust, and is defining the interoperability of the three. For instance, a requestor R gets a security token from an identity Provider, subsequently uses the token to establish a secure conversation with a service S, and then R and S exchange messages in that secure conversation. This is done with one particular choice of tokens, security mechanisms, etc.

**WSBPEL and WS-CDL** The most important standardization activity related to the orchestration languages is undertaken by the OASIS Web Services Business Process Execution Language (WSBPEL) Technical Committee ([http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=wsbpel](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel)). The standardization of the Web Services Choreography Description Language (WS-CDL) is led by the Web Services Choreography Working Group (<http://www.w3.org/2002/ws/chor/>). The most interesting problem with BPEL and WS-CDL is how to express security requirements and security goals at this level and how to enforce (implement) them.

**WSDL** The standardization of a Services Description Language (WSDL), a core language tailored to describe Web services based on an abstract model of what the service offers, is being conducted by the Web Services Description Working Group <http://www.w3.org/2002/ws/desc/>. When describing how to access a service, it is also important to publish the policies that determine which security mechanisms the

requestor must apply. This is an open issue today. In the new WSDL-2.0 (January 2006) the issue is left out-of-scope, the only syntactical means is to use “secure-channel features”, which are simply internationalized URLs, IRIs, without any semantics attached to them. After that, the requestor must find the intersection between this published and his own. This logical step is still missing and there is no tool support for this.

**WS-Agreement** is a Web Services protocol for establishing agreement between two parties, such as between a service provider and consumer. In the case of security services, the service provider and the consumer must agree on trust assumptions, liability, revocation issues, etc. For example, suppose the service creates and provides keys that will be used for cryptographical purposes. Of course, those keys must have the expected entropy and they should not be guessable for an attacker. Moreover, the keys must be securely stored by the service provider. Those all are part of the trust agreement that the partners accept. Furthermore, the consequences in case that those assumptions are not met must also be subject to the agreement. If the service provider has used a bad random number generator for creating the keys, or he has not protected the keys, he must provide some liability to the consumer of the service. All these topics are open issues today. Further information about WS-Agreement, as defined by the Global Grid Forum (GGF) working group “Grid Resource Allocation Agreement Protocol (GRAAP)” is available via [graap-wg@ggf.org](mailto:graap-wg@ggf.org).

## 4 Description of the Use Plan (by result)

In this section, we describe the expected project results that have potential for exploitation, including those beyond the use of AVANTSSAR as a whole as described above.

### 4.1 The AVANTSSAR Platform

The main result of the project is the AVANTSSAR Validation Platform. This result is not independent of the rest as it will be impossible to use the tools comprising the platform without the specification language or the deduction techniques. Thus, the AVANTSSAR Platform will provide SOA designers with an expressive formal language (with a formal semantics) for expressing their products and with powerful tools to verify them. Moreover,

the AVANTSSAR library will provide them with a good basis for developing new services by providing many examples and allowing the reuse of well-tested modules.

On the other hand, the user may be not interested in the techniques themselves or in the syntax and semantics of the specification language, but in using our tools to validate their SOAs.

The initial set of users of the AVANTSSAR Platform will be the SOA designers of companies and institutes of the project participants, integrating them into their development process. This usage will pave the way to the migration of our technology into standardization organizations so that both the scientific and the industrial communities will readily benefit from the advances achieved by the project.

## 4.2 Specification Languages

In order to facilitate the penetration of formal validation techniques in the SOA industry, we plan to promote the ASLan (and the companion language ISSL) as candidate for a standardized formal notation for SOAs. Such a precise notation will allow for easy validation and reuse of modules and services by industry. This promotion will be supported by tutorials given at conferences, industrial meetings, thematic schools, and presentations and courses at engineering schools.

## 4.3 Automated reasoning techniques

We will develop automated reasoning techniques supporting the automatic verification of ASLan specifications of SOAs. By automating the reasoning about security-relevant aspects of services and associated policies, these techniques will serve as the basis for the automated validation technology that will be developed by the project. Moreover, we expect that several of the techniques will be general enough to be applied also in other validation environments.

## 4.4 The AVANTSSAR Library of validated SOA problem cases

We will follow a proof of concept approach by providing a test suite of relevant SOA problem cases which we will use to evaluate the concepts, methodologies, techniques, and tools developed by the project. We will thus guide and assess the development of the AVANTSSAR Validation Platform with a

number of challenge problem cases emerging from a variety of real-world application scenarios based on the service-oriented paradigm and selected from the areas of interest of the industrial partners.

This set of problems, specified in the ASLan, will be also available to the scientific community: the library will be proposed to the scientific community as a suite of benchmark problems for automated analysis of trust and security aspects of SOAs that can be readily used to assess and compare the performance of rival validation approaches.