The vision of Assert4SOA project is to enable automatic processing of security certifications for complex service-oriented applications.

Current trends in the IT industry suggest that software systems in the future will be very different from their counterparts today, due to greater adoption of Service-Oriented Architectures (SOAs) and the wider spread of the deployment of Software-as-a-Service (SaaS). These trends point to large-scale, commodity ICT infrastructures hosting applications that are dynamically built from loosely-coupled, well-separated services. Being able to guarantee key non-functional properties like security, privacy, and reliability will be of critical importance in the future.
Certification of software properties promises to be a major way to provide such guarantee. Current certification schemes, however, are either insufficient or not applicable at all to the requirements of automated run-time security assessment. Today's certification schemes simply do not provide, from an end-user perspective, a viable way to assess the trustworthiness of a composite applications in the context where (and at the time when) it will be actually executed.
The major challenges faced by the project include:

a) Methodologies – mainly based on certification processes – need to be developed for assessing conventional static systems can hardly handle the dynamicity and variety of SOA based systems;
b) New artefacts are needed to support and automate the assessment of the trustworthiness of a stand-alone service, and no means exist to assess the trustworthiness of composite applications;
c) Mechanisms are needed to express and confront claimed security properties.

Assert4SOA has been filling up this gap by producing novel techniques and tools – fully integrated within the SOA lifecycle – for **expressing, assessing and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced.**
More specifically, in order to address the challenges listed above and realize its vision, Assert4SOA has achieved three main **objectives**:

1) providing methods and tools to support certification of SOA based software by providing **abstract models** for these systems that capture their characteristics and the security properties they satisfy;
2) providing notations for **expressing certification claims** in the SOA lifecycle and mechanisms for handling them;
3) providing **mechanisms and tools for reasoning about ASSERTs** (Advanced Security Service cERTificates) in order to assess the trustworthiness of service based systems at runtime.

ASSERTs are **issued by trusted authorities** that contain **machine-readable** specification of security properties and other **information relevant for assessing the trustworthiness of a service** (e.g., *proofs* supporting certificate claims). ASSERTs are strongly bound to service endpoints, in order to ensure their own trustworthiness. They enable service consumers to make sure their application has a certified level of assurance supporting the desired security properties during service orchestration.

1.1 Technical Agenda

To achieve these challenging objectives in the three-year lifetime of the project, the temporal structure of Assert4SOA has been defined as follows:

Requirements and High Level Design Principles (milestone 1, year 1)

In the first year of the project, the focus was primarily set on collecting requirements from a selected set of use-cases (chosen with the help of the industrial partners), and on providing the support to express and manage certified properties, encompassing the definition of models and languages as well as a high-level design of the architecture.

Feasibility Prototype and Advanced Concepts (milestone 2, year 2)

In the second year, Assert4SOA is aimed at moving towards the concrete implementation of the Assert4SOA framework. This prototype takes into account the comments from a first meeting with recognized experts of certification (Advisory Board), and initiates the integration of software components developed by different partners of Assert4SOA. It consists of an integrated prototype of the framework, and several standalone demonstrators showcasing the viability and the potential of the Assert4SOA approach.

Integrated Platform and Final Validation (milestone 3, year 3)

The final year aims to assess the completion of the objectives of Assert4SOA. The framework integrates the different software components and the validation of the Assert4SOA concepts will be done by using our methodology and tools to a significant and relevant use case integrating externalised B2B services in the area of Software as a Service.

1.2 Progress

ASSERT4SOA final year was mostly focused on finalizing the prototype implementation of ASSERT4SOA framework and validating the approach on different use cases, as well as progressing on the standardization.

The consortium defined the most advanced concepts of ASSERT4SOA (language, ontology, composition) and worked on the integration of the solutions, developed within the different activities, in a common framework. In more detail, we developed:

- **Conceptual instruments** including a consolidated version of the ASSERTs language, a common scheme for the three kinds of certificates, a refined version of the ASSERT4SOA query language, schemes for composition of certificates and ASSERT4SOA ontology
- **Software components and prototypes.** We developed the components of ASSERT4SOA and a common integration framework, as well as demonstrators for the more advanced concepts.

ASSERT4SOA also defined **a common, business motivated scenario** based on a service marketplace), which was the basis for the validation of the framework.
Finalizing these activities, the project reached all its key objectives:

(1) Concerning *modelling support for certification*: the project delivered and validated **a formal ontology,** which is the basis for the representation of security properties relevant to services and of their relations, allowing reasoning and interoperability. Furthermore, ASSERT4SOA defined **specific models for the three families of service certificates**, respectively based on testing and on formal modelling and ontology, producing examples for all of them.

(2) Concerning *schemes for expressing certificates*, ASSERT4SOA finalized **the schemes for expressing certificates**, (now at v2.1) converging to a modular structure composed by a *core* part (where the security property is described independently of the evaluation used to prove it) and an *evaluation-specific part*, where the evidences/proofs of the validity of the property are described (in terms of ASSERT-M, ASSERT-O, and ASSERT-E). In addition, ASSERT profiles have been delivered to support the user in defining ASSERTS according to specific schemes (e.g., Common Criteria). ASSERT4SOA also developed a tool to support the writing and management of certificates: **ASSERT Management Tool (AMT**).

(3) Concerning *support for reasoning about certified properties*. The **assert-aware discovery system was developed**. Notably the **modular matchmaking system,** including algorithms and software components to match and order ASSERTs at the level of property description, ontology-based certificate, evidence-based certificates, and model-based certificate. Furthermore, ASSERT4SOA developed a conceptual approach for building **secure service compositions** using patterns and for using them during the discovery process. The results have been integrated in a common framework and demonstrated on two prototypes, addressing different scenarios: **Assert-enabled service marketplace** and **Assert-aware BPEL design tool.**

The ASSERT4SOA prototypes constituted a major step to show the feasibility of ASSERT4SOA approach, and they played a major role in the validation phase.

.

The framework prototypes are a concrete instantiation of the architecture design, developed in the initial phase of the project, and they are targeted to two different scenarios: **ASSERT-enabled service marketplace** and **ASSERT-aware BPEL design tool.** The rationale of having two prototypes is that we want to address different communities and levels of sophistication.

Indeed, given the increasing industrial relevance of the marketplace metaphor, we introduced the concept of an **ASSERT-enabled service marketplace.** Services offered on such a marketplace are Assert-certified, and can be browsed and selected based on their Assert-certified security properties. This scenario targets business users, and it is characterized by a quick-to-market vision. A first version of the prototype has been presented to a SAP DKOM 2013 in Paris, a major internal event of SAP developer community. It has also constituted the basis for validation, targeting two business expert groups from industrial project partners: Engineering and SAP software developer and consultants.

The second scenario aims to demonstrate the more advanced concepts of ASSERT4SOA, including service discovery.

An additional prototype for creation and management of ASSERTs (AMT tool) has been developed mostly addressing the certification authority community

These three prototypes were used for the validation. The validation was performed according to a proven validation methodology, i.e. via expert focus groups, covering the different stakeholder communities of ASSERT4SOA, such as certification authorities, application developers, IT specialists. Our experts evaluated the framework from different angles: business relevance, usability, quality and adoption. In a nutshell, the validation outcome was characterized by a strong appreciation of the approach, grounded on the recognition of the relevance of certification and the need of more flexible certificate consumption schemes. We also presented the results in form of research papers to major scientific events, to collect feedbacks from the research community.

Dissemination activities also progressed substantially in the last year. Two Advisory Board meetings (comprising relevant experts in certification) were held, and the AB members' valuable feedback has been taken into account. Notably, in this forum, experts from privacy certification

suggested to extend ASSERT4SOA to more privacy-specific use cases. Accordingly, ASSERT4SOA consortium proposed new models for privacy certification for services.
The consortium successfully presented its results at a number of key events; had accepted papers in some major conferences (International Common Criteria conference, ICWS 2012, ICWS 2013, Services 2012, and CLOUD 2012)), and had published articles in some journals (ACM Transactions on the Web, Springer Computing Journal, The Computer Journal).
The link with other EU projects through the SecCord initiative was particularly significant. Notably, ASSERT4SOA has co-organized the **Cluster Workshop on "Assurance for the Cloud" @ CSP EU Forum 2013,** (a follow-up of 2012 event: Cluster Workshop on Security Contracts @ CSP EU Forum 2012**)**. The workshop had as outcome the agreement from several EU projects, to provide a contribution to standardization. A joint document was later submitted to ETSI TG3 and communicated to DG Connect. In addition, the concept of certification was introduced in the draft for the forthcoming ISO/IEC 27018 standard on *Code of practice for data protection controls for public cloud computing services*.
A workshop of Security and Privacy, Assurance and Certification (SPEAC) proposed by our project was run in the framework of the IEEE SERVICES conference, a major international venue for services research and industrial experiences exchange. SPEAC has collected more than 20 submissions, including several contributions from other FP 7 projects, such as TCloud and CUMULUS. A total of 8 papers were accepted, and presented at SPEAC on June 27th 2013.

Project website: http://www.assert4soa.eu
Project Coordinator: Michele Bezzi - Michele.Bezzi@sap.com
Scientific and Technical Coordinator: Ernesto Damiani - Ernesto.Damiani@unimi.it