

# Newsletter

## Editorial

by Veronika Sirková

Welcome to the first edition of the MASTER newsletter! We have designed this having in mind not only the partners of the MASTER consortium but also the broader community, and so we will include the work of the project itself as well as issues that are related to :

- assurance, security and trust issues in centralized, distributed and outsourced information systems,
- security controls and measurements, regulatory compliance in service-oriented environments,
- and audit of information security management systems.

The newsletter will always host a feature article. For this edition we have chosen the introduction of MASTER itself. In every issue you will also find the interview with some of the representatives of the MASTER consortium or IT security experts, consultants and auditors. Our first guest is Pedro Soria Rodriguez from Atos Origin, coordinator of MASTER project.

## The MASTER Project

by Veronika Sirková

Today, organizations must comply with multiple regulations, international policies, and best practices. Business are becoming more complex and international and the complexity and scope of various compliance efforts has increased significantly. However, companies are sometimes faced with conflicting requirements or with difficult technical challenges when new business models, such as outsourcing, are adopted. A common element to all compliance requirements is the need for strong and effective security controls over various enterprise business processes. Information security is, therefore, a crucial foundation of compliance: without proper security controls, the various compliance processes cannot be effectively deployed.

MASTER (Managing Assurance, Security and Trust for Services) is a project researching languages and tools to express and manage different compliance requirements and processes, such that these can be effectively managed within an organization. From the view point of regulatory compliance MASTER brings added value in two main respects. Firstly, it provides an approach

to implementation and maintenance of auditable provisions to achieve and assure compliance with a set of regulatory requirements. Secondly, it provides a particular implementation of this approach specifically to service oriented systems.

MASTER is a collaborative research project run by consortium of 14 European industrial or academic organizations and co-funded by the European Commission under the 7th Framework Programme of the European Union.

The MASTER project is planned, to address the compliance management issues in relation to assurance, trust and security in three phase:

- the single trust domain,
- the multiple trust domain, and
- the iterated outsourcing domain.

These are relevant when thinking about SOA (Service Oriented Architecture) based business processes, as the dynamics of SOA allows for streamlines of services composition, which may cross different domains of trust, or different domains of regulatory application. (continues on page 2)

## Interview with Pedro Soria Rodriguez

by Ivana Sabatova

MASTER is a large-scale integrating project funded by EU Seventh Framework Programme where 14 partners from 12 EU countries and 2 non-EU countries are participating. The crucial factor of success is perfect project coordination since the preparation up to the assuring of project outcomes sustainability. That's why we invited Mr. Pedro Soria-Rodriguez the project coordinator for the #1 of MASTER newsletter.

What is the most important aspect of MASTER that distinguishes this one from the other FP7 projects concerned with information security?

MASTER is an important project because it is going to fill a gap in the consulting and

auditing business to help companies and auditors to have a better understanding of the security situation of their business and service infrastructures. MASTER is going to map their high level business requirements to the low level IT security requirements, and to provide the methodologies and tools to monitor and assess their conformance to security policy and regulatory requirements.

What was the original idea that led to MASTER project proposal and who namely came with it?

MASTER emerged from an idea by Volkmar Lotz of SAP and Fabio Massacci of University of Trento. In cooperation with Atos Origin, this idea was developed into an FP7 project proposal. (continues on page 2)



MASTER kick-off meeting

## The MASTER Project

*(continues from page 1)*

The project results and their applicability in the real world will be demonstrated in two case studies - healthcare sector represented by Hospital San Raffaele and finance sector represented by insurance company CESCE. The MASTER methodology and the set of MASTER technologies are meant to address the problem of compliance in environments subject to different types of regulations, specifically targeting compliance to information security norms and policies. With this in mind, the project has identified the stakeholders of MASTER as auditors (internal and external to an organization), Chief Information and Security Officers of organizations, and those in charge of administration of control processes.

Today, MASTER is in the middle. For the first year of the project, we followed a concurrent engineering approach (on concepts, architecture, and methodology), prototyping (infrastructure building), and the provision of the test bed in terms of scenario instantiation were all going on in parallel.

During those first 12 months, research work for the single-domain scenarios were performed, resulting in initial prototypes. This work was driven by the requirements of the case studies, which were finally selected and specified in the first year.

MASTER has proposed a methodology and architecture solution to the compliance problem that supports the Deming Cycle (Plan-Do-Check-Act). Different components of MASTER have been taking care of each

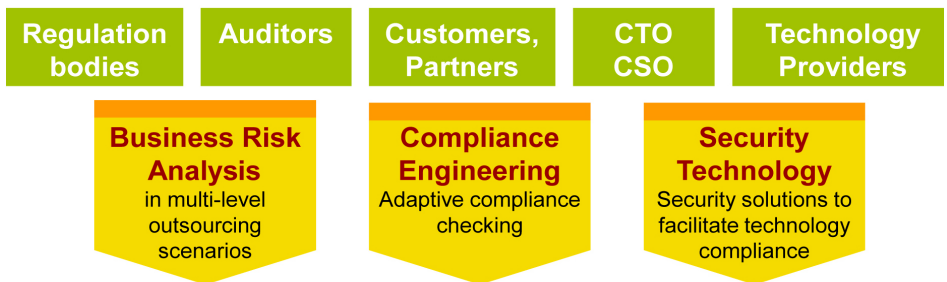
of those four phases of the cycle: a design component which helps organizations to plan the rollout of control processes in their business processes, an enforcement component which ensures the application of control process, a monitoring component which checks for the correct operation of controls, and a reactive component which acts in situations of failure or non-compliance. On top of these, MASTER provides an assessment component which oversees the complete process.

Now, we concentrate on the research work for the multi-domain scenarios and the finalization of the prototypes for the single-domain scenarios, using the final concepts for this scope which have been elaborated at the end of the first year.

*Project motivation*

### Challenges:

- **Highly dynamic service-oriented architectures**
- **Outsourcing and distributed management constitute the norm**
- **Increasing complexity in security and trust requirements from regulations and business standards**



## Interview with Pedro Soria Rodriguez

*(continues from page 1)*

The project will end in the beginning of 2011. Do you have an idea how to ensure that the project outcomes and ideas will further be spread?

MASTER is one of strategic projects of NESSI, the Networked European Software and Services Initiative. We closely cooperate with NESSI which allows us to spread the project outcomes to this broad and representative European community and also it will ensure that MASTER ideas will be further utilized in the future, through the NESSI

Open Framework (NEFOX). MASTER brings significant innovations towards resolution of trust and security compliance within emerging service oriented ICT environments.

*How do you plan to target the users of MASTER project outcomes?*

Beside other dissemination activities like website, this newsletter, publication of project deliverables and a number of other publications, we have been participating and presenting MASTER project at

relevant industry and research events internationally. In 2010 MASTER will organize a conference involving target business actors to whom MASTER is relevant. Recently we have been negotiating the partnership with the 7th Annual CISO Executive Summit 2010 which seems to be an ideal opportunity to merge with.

*Thank you for your time.*

## The first year deliverables

by Veronika Sirková

In the first year of the project we concentrate on the single trust domain scenarios and on initial prototypes. Our research work was driven by the requirements of the health care and financial case studies which were specified in this phase of the project. This article introduces public project deliverables of the Activities A1, A2, A3 and A4.

**D1.1.1** Stakeholder Requirements Analysis introduces MASTER and the market needs it serves.

**D1.2.1** MASTER Scenarios describes two case studies chosen for the project in detail, by taking into account both the stakeholder requirements and the regulatory requirements.

**D1.1.3.** Risk Analysis Modelling comprises overview of research on risk analysis in MASTER.

**D2.1.1** Protection and Assessment Model for the Single Trust Domain contains the formalisation of the notions of business and control processes, compliance, and indicators, and thus provides the rest of the project with precisely defined concepts. The main achievements of **D2.2.1** Language Framework and Language Integration for Single Trust Domain were the successful integration of languages suitable for expressing control objectives, and for monitoring, enforcement, and assessment rules, as well as the creation of a suitable semantic interoperability model. This enables a control process to be defined as a set of policies that each different technical activity can execute.

**D2.3.1** Technical Architecture and APIs for Single Trust Domain focused on the creation of a consolidated technical architecture based on services that enabled each of the infrastructures developed in the project to interoperate. The deliverable also provided technical architectural descriptions of the monitoring, enforcement, and assessment infrastructures to show the suitability of that architecture.

**D3.1.1** MASTER Methodology v.1 provides general principles and high-level procedures for designing and implementing controls for the single trust domain case. The Methodology is intended to be compatible with the main IT standards and frameworks so that it will easily fit into the governance, risk and compliance culture of end-user organisations, auditors and certification authorities. The methodology is founded on the basic principles of Plan-Do-Check-Act of the Deming cycle that are commonly adopted with major IT frameworks (e.g. COBIT, ISO/

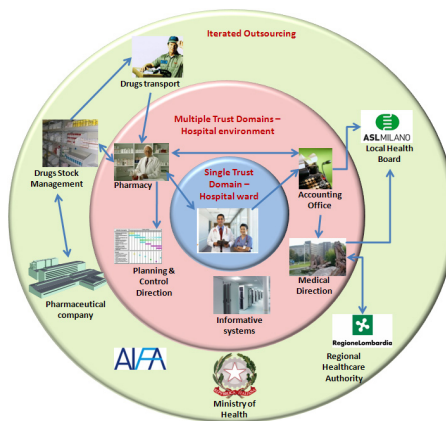
IEC 27001).

**D4.1.1** Requirements Analysis/First Signalling Prototype collects the requirements of the observation infrastructure from the other activities within MASTER and expresses them as requirements on the signalling and monitoring infrastructure, respectively. This deliverable applies these specifications on a simplified version of the CESCE use case and integrates them with implementations of signalling for infrastructure components, such as a BPEL engine and an Enterprise Service Bus.

MASTER public deliverables of the first project year are available on [www.master-fp7.eu](http://www.master-fp7.eu).

(To be continued in the next edition...)

### Healthcare overall scenario



## Events

MASTER is following an active dissemination strategy to reach its various stakeholders. In next three months MASTER has planned:

### WISTP'09

(<http://www.wistp.org>)

MASTER will organize a session "Management of Assurance & Security Metrics in Service Orchestration". The session will take place on September 3, 2009 in Brussels, Belgium during the WISTP'09 conference.

### WICSA/ECSA 2009

(<http://www.wicsa.net>)

MASTER will participate in Joint Working Conference on Software Architecture 2009 & European Conference on Software Architecture 2009 which will take place on September 14, 2009 in Cambridge, United Kingdom. MASTER will present paper "An Evidence Model to Enable Constraint-Based Runtime Monitoring in an SOA".

### ICSEA 2009

(<http://www.laria.org/conferences2009/ICSEA09.html>)

MASTER will be presented at The Fourth International Conference on Software Engineering Advances. The conference will take place on September 20 – 25, 2009 in Porto, Portugal.

### ISACA CZ

(<http://www.isaca.cz>)

MASTER will be presented at the conference "ITG - Business Innovation" organized by ISACA Czech Republic Chapter. The conference will take place on October 14 – 15, 2009 in the Czech Republic.

## References

Alexander Pretschner (Fraunhofer-Institute for Experimental Software Engineering) gave an invited talk on "Distributed Usage Control" at the KEPT 2009 conference in Cluj (Romania), on July 3, 2009. In his talk he also featured MASTER.

The paper "Employing Key Indicators to Provide a Dynamic Risk Picture with a Notion of Confidence" by Atle Refsdal and Ketil Stølen (SINTEF) was presented under the Risk Assessment Session within the IFIPTM

2009 conference taking place in West Lafayette (USA) on June 15-19, 2009.

The paper "Dynamic Enforcement of Abstract Separation of Duty Constraints" authored by David Basin (ETH), Samuel J. Burri (IBM) and Günter Karjoth (IBM) is going to be presented within the 14th European Symposium on Research in Computer Security (ESORICS '09). September 21–25, 2009, Saint Malo (France).

## MASTER contributes to NEXOF-RA

### NEXOF-RA:

Reference Architecture for NEXOF project is the first step in the process of building NEXOF (NESSI Open Framework) the generic open platform for creating and delivering applications enabling the creation of service based ecosystems where service providers and third parties easily collaborate.

The overall goal of NEXOF-RA is such independence that NESSI Open Framework can be implemented into a broad range of application domains supporting any size of business by all user communities using different technologies. For that framework NEXOF-RA will deliver a coherent set of globally applicable technologies intended to provide Europe with digital service to improve flexibility, interoperability and quality. In addition, NEXOF-RA will try to establish strategies and policies to speed up the dynamics of the services eco-system as well as to foster safety, security and well being of citizens by means of new societal applications. Collaboration between MASTER and NEXOF-RA lays mainly in MASTER contribution to Open Architecture Process in the security field.

An example of the collaboration between MASTER and NEXOF-RA is recently published Position Paper on dynamic security of SOA reviews one specific aspect of dynamic security, namely automated responses to attacks (hostile activities aimed at exploiting software vulnerabilities) and intrusions (successful attacks). Authors of the paper are MASTER partners and their entry to the problematics discusses the evolution of dynamic execution environments increasingly requires security policies that are also dynamic in nature to address events such as process migration, changes in personnel, shifts in alliances, and detected intrusion that cannot be well anticipated or addressed by static policies. This paper, considers one aspect of dynamic security, namely adaptive functionality that reacts to changes in the security environment. This aspect falls into the third category of contributions ("Dynamic Security Architecture") sought in Section 4.6 of the NEXOF-RA Invitation to Contribute.

## MASTER will be hosted by WISTP'09

by *Veronika Sirková*

The WISTP'09 (Workshop in Information Security Theory and Practices) that will take place on September 1 – 4, 2009 in Brussels (Belgium) is to bring together researchers and practitioners and encourage discussion on issues related to the security of the next generation networks, computer systems and especially embedded systems and the privacy of users immersed in such systems.

As MASTER scope of research is very relevant to the respective issues, MASTER will organize a session with the title "Management of Assurance & Security Metrics in Service Orchestration" within this workshop. The session will be structured around two main topics, with an introduction of the work of MASTER in the field, and invited talks, to motivate discussion from the audience, with the goal of validating and enriching the work of MASTER in these topics. Bruno Crispo from the University of

Trento and David Sinclair from the Dublin City University will be represented MASTER in two sessions: Information Assurance and Trust Management, and Security measurements. The session on Information Assurance and Trust Management will cover proposals from MASTER on models, technology, and tools to define policies, goals and performance indicators from a security, trust, and assurance perspective while the session on Security measurements will be dedicated to the proposal on security and assurance metrics from MASTER: Trustworthiness of control processes and effectiveness of control processes and to the validation of the proposal from MASTER. Invited talks will be given by Bernhard M. Hämmerli (CEO Acris GmbH), Rudolf Schreiner (CTO, ObjectSecurity Ltd) and Reijo Savola (VTT). For detailed agenda please visit [www.master-fp7.eu](http://www.master-fp7.eu). We are looking forward to seeing you on September 3, 2009.

## The 3rd MASTER General Assembly

by *Veronika Sirková*

The third MASTER General Assembly took place in Oslo (Norway) from June 30 to July 2, 2009 and was hosted by SINTEF. Besides reporting about activities and achievements in the first year of the project, the meeting was dedicated to coordination among components and to the planning of prototypes that are due by the end of the second year of the project.

During the first year we mainly focused our research on the single trust domain and performed a deep analysis of the necessary tools and concepts to setup the MASTER solution. Our effort resulted in initial prototypes of the observation infrastructure and concepts to deal with the problematic issues raised by the requirements of the case studies which were finally selected and specified during this year.

In the following year, we have been finalizing a solution for single trust domains by

producing the final version of the prototypes based on a refinement of the concepts provided by the first year of research. In parallel, MASTER will investigate the multi trust domain aspects and develop the different concepts that will have to deal with the challenges of an open system.

The event also offered an excellent opportunity to present the testbed for the particular use case scenarios which will be used for further testing and verification of the developed technology. All partners were introduced to the testbed, so that all technical activities in the project are aware of how to "plug-in" the MASTER components in the testbed, and for the technical activities to comment on the testbed. At the end of the meeting an interesting discussion on dissemination of MASTER results was initiated.

The next General Assembly will be held in January 19 – 21, 2010.



Project is co-financed by the European Commission under the Seventh Framework Programme  
FP7 - 216917

**Periodicity:** quarterly

**Editorial board:** Jan Fanta (ANECT), David Sinclair (LERO), Pedro Soria Rodriguez (ATOS), Bruno Crispo (UNITN)

**Chief Editor:** Veronika Sirková (ANECT)

**Edited by MASTER Consortium:**

Atos Origin, SAP, Università di Trento, Engineering Ingegneria, Informatica S.p.A., British Telecom, ETH, University of Stuttgart Lero, ANECT, Deloitte, IBM, Cesce, Fondazione San Raffaele, Stiftelsen Sintef  
[www.master-fp7.eu](http://www.master-fp7.eu)