MASTER: Management of Compliance in Service-based enterprises for Security and Trust

Beatriz Gallego-Nicasio[1], Aljosa Pasic[1], Pedro Soria-Rodriguez[1],

[1] Atos Origin, Albarracin 25, 28037 Madrid, Spain
{beatriz.gallego-nicasio, aljosa.pasic, pedro.soria}@atosorigin.com

Abstract. Organizations are subject to a number of regulations, internal policies and best practices and standards, and in the context of the Future Internet, Enterprise Systems will look for increased collaboration to make use of dynamically composed services. Compliance to regulations and policies becomes an important problem from the security and trust standpoint, to ensure secure and trustworthy collaboration among enterprises. MASTER provides a engine for cross-enterprise and cross-domain collaboration compliance management.

Keywords: Compliance, trust, security, collaboration, SOA, Future Internet.

1 Introduction

Organizations are subject to a number of regulations, internal policies and best practices and standards, and in the context of the Future Internet, Enterprise Systems will look for increased collaboration to make use of dynamically composed services. Compliance to regulations and policies becomes an important problem from the security and trust standpoint, to ensure secure and trustworthy collaboration among enterprises.

MASTER is a compliance governance engine devised with the goal of developing models, concepts and technology to facilitate the management of regulatory compliance in Future Enterprise environments where collaboration will be the norm, and security needs to be assured by means of compliant processes.

The MASTER solution for the compliance problem follows a Deming cycle-like paradigm with Plan-Do-Check-Act phases. Different components of MASTER take care of each of those four phases: A design component helps organizations plan the rollout of control processes in their business processes, an enforcement component ensures the application of control process, a monitoring component checks for the correct operation of controls, and a reactive component acts in situations of failure or non-compliance. On top of these, MASTER provides an assessment component to oversee the complete process.

The goals of MASTER are realized mainly in a conceptual model of the different artifacts involved in the process of monitoring, assessing and enforcing compliance: control processes, risk analysis, and metrics. MASTER has defined Key Assurance

and Key Security indicators (KAI and KSI), which help assess the conformity of a system to a particular regulation or policy (in a way, the "degree of compliance", albeit this concept is not strictly correct), and the correctness of the control processes in place to implement regulatory compliance.

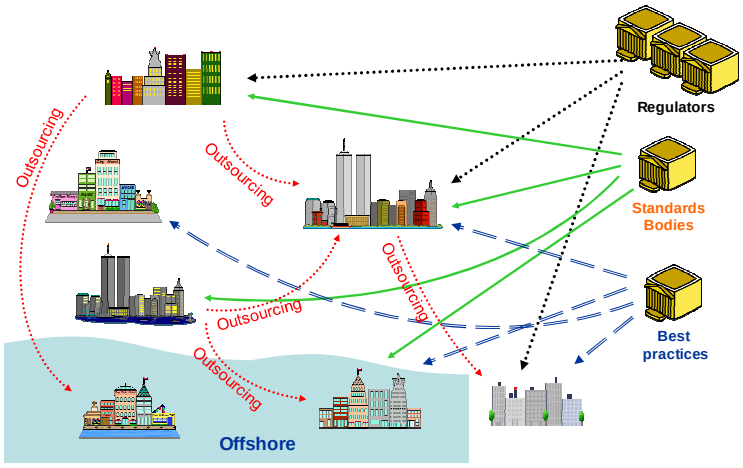

Figure 1 – Compliance interdependencies among Enterprises

Figure 1 presents the typical environment of collaboration and outsourcing that presents compliance challenges. MASTER is positioned within each organization with respect to the related security tools, processes and stakeholders. MASTER monitors and enforces regulatory and security control activities and control processes at the organizational and Business Process levels, tapping into the communications among enterprises to ensure that one organization's regulatory compliance requirements are met across the service chain composed of services provided by other enterprises.

Recently the first "high-level integrated governance solutions" have appeared in the market, often based on previous work in security compliance checking, monitoring infrastructures or risk assessment tools. However, dynamic Enterprise Collaboration creates challenges to regulatory compliance that have yet to be resolved. The MASTER platform targets these challenges of the Future Internet and future Enterprise Systems, and delivers a platform that helps ensure secure and trustworthy collaboration among enterprises.

2 The MASTER solution

The MASTER design framework allows stakeholders and analysts to create a model of their business processes, system and resources, and based on laws, regulations and corporate policies, to produce a control process model. This control process model contains all the information to configure MASTER infrastructure in a way that ensures both business and control objectives are satisfied.

In today's Entrerprise Systems, and with the emergence of cloud computing, classic outsourcing practices have evolved to become dynamic and iterative, and the traditional security and compliance problems such as lack of control and visibility, aggravate. In iterative outsourcing, a client outsources parts of its information system to an outsourcing provider, which, in turn, uses third-party providers to deliver its own services. The client has only contractual relationship with the service provider, but no other contractual relationship with the third-parties providers. The problematic is similar for dynamic outsourcing, but in this case, the contractual relationships change more quickly and frequently. The possibility to purchase services from the cloud and make use of them in minutes demands contractual relationships to be established almost automatically.

Run-time compliance checking is performed by MASTER based on the ideas of visibility and control. Essentially, a *monitoring infrastructure* makes sure the controls are correctly operated and, in case of deviations, reactive and preventive mechanisms are triggered. In iterative outsourcing scenarios, the capability to access information owned by service providers and the degree of control over external domains' business process executions is limited.

Not knowing the details of the service provider's processes is a problem for the client because it is uncertain of the events that are emitted by the service provider. Some important unknowns are: Have all relevant events been emitted? Is the data in the events accurate? The client cannot know because the service provider will in general not let the client install appropriate controls in the services provider's infrastructure. Thus, there is a need for balance between the clients' requirement to be compliant with regulations even in outsourcing situations, and the service provider's confidentiality and the validity of access control policies.

In MASTER, the control process model adapts to the new requirements being customizable, allowing companies to negotiate certain parameters along with the actual service level agreement, at negotiation-time. Some of these parameters are for instance the specific evidence a service provider must supply the client, and some constraints over the process execution that service provider must satisfy, in order to maintain conformance. For this purpose, MASTER introduces two new concepts which, in conjunction, enable establishment of cross-domain trust relationships for iterative and dynamic outsourcing.

Protection and Regulatory Models (PRMs) are a new concept of domain-specific design patterns introduced by MASTER which encode the protection goals, such as regulations or security best practices. This encoding makes it possible to state precisely, in a modular way, what it means to comply with some protection goals. The name Protection and Regulatory Model reflects that the control objectives may stem from regulations (such as HIPAA) or from some security consideration (such as a client request to protect a particular asset). More specifically, a PRM is a set of parameterised fragments of control processes and each PRM is linked to a generalized control objective. Each control process fragment is defined by a set of allowed event traces. PRMs map security compliance objectives to control processes and architectures that achieve them in defined business and technical contexts. PRMs address security and compliance objectives that occur frequently in practice and encapsulate design knowledge and best practice allowing this knowledge to be reused.

Protection-Level Agreements (PLAs) represent a key tool for expressing protection objectives and related indicators for a business process that is run, at least partly, in a different trust domain. The terms written into the PLA need to take into account the direct impact of this regulation on the outsourced sub-process, and also the need to demonstrate that the overall process remains compliant. PLAs include PRMs as external points of reference (and thus avoid the need to incorporate standard conditions or terminology in a PLA) and provide "boilerplate" text that can be customised. If these PRMs are standardised by a regulatory body, both client and provider can be confident that they are negotiating everything that is relevant for compliance.

Negotiation

Parties to the negotiation would initially agree on a PRM if it is not already dictated by convention within some community or industry. For example, hospitals in the U.S. are subject to HIPAA, so PLAs in health care would probably be using PRMs related to HIPAA. The parameters in the template define a space of possible PLAs. Negotiation is then an exploration of that space of possible agreements in order to find at least one region of mutually acceptability. Of course, each party in the negotiation will try to maximise its own benefit according to some measure of utility.

The need to automate the negotiation of outsourcing relationships and Protection Level Agreements (PLA) rises as the cost of manual negotiations is high in dynamic outsourcing. However, there is a fundamental aspect that makes the automation of the process of selection of providers and negotiation of contracts difficult: trust.

In MASTER, the concept of automatic trust negotiation pioneered by Winsborough et al. [1] and Winslett at al. [2], is considered for dynamic selection of outsourcing service providers and also for iterated outsourcing. The MASTER Trust Management Model incorporates the concepts of direct trust, trust recommendations, and reputation. Our trust model uses the support of Subjective Logic (SL) [3] to quantify trust measurements taking explicitly into account uncertainty and incomplete knowledge.

3 Future work

MASTER introduces new concepts to specify security and compliance requirements in inter-enterprise contracts and service provisioning, along with a platform for the design, monitoring and assessment of compliance controls.

The system works in the service domain, monitoring service invocation calls to determine the effectiveness and correctness of controls. This poses a potential performance problem to be further investigated, since such service invocations themselves may be often encrypted. While some techniques have been explored in MASTER to deal with encrypted traces and service calls, this is one topic that needs further investigation and development.

The concepts of PRM and PLA need to be further studied, in particular to align them with new practices and state of the art in Enterprise Collaboration,

Acknowledgments. The work published in this article has partially received funding from the European Community's 7th Framework Programme Information Society Technologies Objective under the MASTER project[4] contract FP7-216917. The MASTER project started in February 2008 led by Atos Origin, with technical coordination by SAP and scientific coordination by University of Trento, and the participation of Engineering, British Telecom, ETH, University of Stuttgart, Dublin City University, ANECT, Deloitte, IBM, CESCE, Hospital San Raffaele, SINTEF and Fraunhofer.

References

1. A. Jøsang. Subjective logic book (draft). Available at: http://persons.unik.no/ josang/sl/, 2010;
2. W.H. Winsborough, K.E. Seamons, V.E. Jones. *Automated Trust Negotiation*. In, Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 88-102, 2000.
3. M. Winslett, T. Yu, K.E. Seamons, A. Hess, J. Jacobson, R. Jarvis, B. Smith, and L. Yu. *Negotiating Trust on the Web*. IEEE Internet Computing, 6(6):30-37, 2002.
4. The MASTER project, http://www.master-fp7.eu