Chapter 4
Aspects of General Security & Trust

David Brossard, Theo Dimitrakos, Angelo Gaeta, and Stéphane Mouton

Abstract Organisations increasingly engage in business collaborations with different partners in different locations. Such enterprises want to capitalise on and offer their existing internal capabilities as services to its customers. Service-oriented architectures let them do so. SOA by definition is loosely coupled, highly granular, and often widely distributed and multi-step. They can combine internal and external services. However, exposing sensitive services through an SOA gives rise to serious security concerns. In particular, it is important to rethink identity and access management. Neither aspect is a new IT management challenge but SOA amplifies them with scale and complexity. The management of user identities, their credentials and other attributes, as well as controlling their access to the business services need to be defined, managed, controlled, and enforced. Identity silos must be bridged.

4.1 Introduction

The activities of the General Security area have led to the identification of Technical Requirements, Common Capabilities, Design Patterns and Software components to address issues of trust & security of users & applications in a distributed environment, typically regarding the privacy, confidentiality, and integrity of message exchanges between different users & services.

Key challenges come from the evolution of the way businesses interact nowadays: the work environment has become more pervasive with a mobile workforce, outsourced data centres, different engagements with customers and distributed sites. Systems are no longer monolithic: they integrate different services and clients from potentially many partners; each one with different security rules, identity stores, interfaces and regulations. Message exchanges no longer take place within the enterprise but across uncontrolled public networks. This stresses the need to secure end-to-end transactions between business partners and the customer. Companies will have to comply with their own directives and regulations as well as their partner organisations’ rules and legal constraints: compliance must be monitored. In order
to enable rich & flexible scenarios, the security mechanisms put in place must support, not hinder them and must be flexible and adaptive. Different enterprises, services and customers imply multiple authorities and complex relationships regarding the ownership of resources and information across different business contexts and organisational borders. Security policies must be issued by multiple administrators and enforced over a common infrastructure. There is also a need for well-orchestrated, end-to-end Operations management that provides controlled visibility, governance of network and IT state, timely assessment of the impact of security policy violations and the availability of resources. Hence, there is an increasing interest in security observers & monitors.

One can also refer to the challenges elicited in the Virtual Organisation thematic area (see Chap. 3) to complete those already mentioned in the previous paragraph.

Five components have been developed by the General Security area over the course of the project to address these issues.

In particular, the Security Token Service (SOI-STS) (see Sect. 4.5.2) serves as an identity broker & federation manager that manages (a) an enterprise’s participation in federations; (b) identity bridging between intra- and inter-enterprise identity technologies, claims, and authentication techniques; and (c) the lifecycle of identities and security attributes of users and services within that given enterprise. By federating identity brokers, a group of collaborators may create manageable circles of trust, each of them corresponding to a structurally rich trust network. The SOI-STS enables multiple administrators to control their own view of a circle-of-trust and authorized users & services. By issuing identity tokens, the SOI-STS also provides cryptographic material that can be used in secure e2e communications.

The Authorization Service (see Sect. 4.5.3) is a policy-based authorization service which takes in access control requests, evaluates them against internal policies, and returns its decision to the requestor. It grants distributed access control and combines several access control models (attribute-based, role-based, and rule-based) to produce an authorization framework suitable for highly distributed, dynamic environments. The SOI-AuthZ-PDP supports delegation which in turns enables a multiple administrative model.

The Secure Messaging Gateway (SOI-SMG) (see Sect. 4.5.4) is a policy enforcement point and an XML Security Gateway which is an appliance or software that enforces XML and Web service security policies. The SOI-SMG allows the enforcement of message and service-level policies with little or no programming. Combined with the SOI-STS or on its own, the SOI-SMG is able to analyze message flows, encrypt/decrypt, sign/validate signatures and again guarantee secure enterprise to enterprise communication. Because it is policy-based and its policy location mechanism is flexible, the SOI-SMG can allow for rich and diverse scenarios and deployments. Commercial alternatives also come with rich monitoring tools. Some of the key benefits of the SOI-SMG are that it decreases cycle time by removing security development burden from developers and coherently applying security policies across an entire enterprise.

The Security Observer (SO) (see Sect. 4.5.5) is a component that aims at monitoring security properties in a Grid environment and notifying subscribed entities when