

# SOA3: an architecture for service oriented authentication, authorization and accounting in distributed environment

*Wednesday, 19 September 2012 14:50 (20 minutes)*

## Description of the work

The user list is stored in an LDAP directory: every record contains userId, password and a set of generic attributes. Every user can be associated to one or more roles and one or more groups. SOA3 User Management Service provides REST CRUD operations for managing stored identities, roles or groups. SOA3 Authentication Service is composed by two modules:

username/password Module, which matches incoming usernames/passwords with the information stored on the LDAP directory

SAML Access Module which grants the accesses parsing SAML assertions: this module acts as a SAML Service Provider providing SAML based Identity Federation.

The Authentication Service also includes a SAML Identity Provider and Attribute Authority: when the access is granted, a SAML Authentication Assertion is returned containing a set of attributes associated to the user. The associations to group and roles are considered attributes in this context. This Assertion can be used both for Identity Federation and to propagate the attributes in the domain for authorization purposes.

The Authorization Service implements Attribute Based Access Control model with policies written in XACML. The service checks if a request must be permitted or denied basing on the attributes of the requester: the attributes are transported as SAML assertions associated to the request. The assertions can be directly associated, e.g. adding an assertion to the SOAP security header, or indirectly, adding only the reference to be resolved by SAML Artifact Resolution Profile.

The Accounting service is built around the Usage Tracker service whose goal is to keep track of resource usage by receiving and archiving usage records. It provides CRUD operations on usage records. Core accounting components are agnostic on the type of the resources and their properties by adopting an extensible data model. Specializations of this generic model have, however, been realized to ease the management of resource types actually in use.

## Wider impact of this work

The work is a complete, standard based security architecture. It has been designed to be used in distributed environment. The possibility to introduce the security as an infrastructure service provides a great added value on modularity and manageability.

A strong importance has been given to the performance aspect: for example LDAP directory has been chosen for this reason.

## Printable Summary

Service Oriented Authentication, Authorization and Accounting (SOA3) provides the three main functionalities of a security system according to the Security as a Service model. All the services are exposed by RESTful interfaces providing high adaptability to different context, especially distributed environments and Cloud environments.

The architecture is composed by:

- \* an Authentication Service, including an User Management module and a SAML ID-Federation Module
- \* a XACML based Authorization Module
- \* an Accounting Module

**Primary author:** FORMISANO, Ciro (Engineering Ingegneria Informatica)

**Co-authors:** TRAVAGLINO, Ermanno (Engineering Ingegneria Informatica); BALRAJ, Kanchanna (Engineering Ingegneria Informatica Spa); Mr FABRIANI, Paolo (Engineering Ingegneria Informatica S.p.A.)

**Presenter:** FORMISANO, Ciro (Engineering Ingegneria Informatica)

**Session Classification:** AAI Workshop

**Track Classification:** Resource Infrastructure services (Peter Solagna: track leader)