Access Control Service Oriented Architecture Security

Yoon Jae Kim, yj1dreamer AT gmail.com (A project report written under the guidance of Prof. Raj Jain)

Download 

Abstract

Service Oriented Architecture (SOA) is one of the most popular concepts to implement computing systems. However it faces many challenges to security and many standards and frameworks come out to support it. We focus especially on the access control system using SOA and represent what are the SAML and XACML and how they are applied for Portal and Web Services.

Keywords

Service Oriented Architecture, SOA, SOA Security, Web Service, Web Service Security, SAML, Security Assertion Markup Language, XACML, eXtensible Access Control Markup Language, access control

Table of Contents

1. Introduction to Services Oriented Architecture Security

One of the most popular IT trends is Service Oriented Architecture (SOA), which is defined as follows:

Service Oriented Architecture (SOA) is a design pattern which is composed of loosely coupled, discoverable, reusable, inter-operable platform agnostic services in which each of these services follow a well defined standard. Each of these services can be bound or unbound at any time and as needed. [Jamil08]

However, as defined, SOA has a loosely-coupled feature, which makes SOA open to the challenges of security. It means that SOA must meet several requirements. The main requirements are as follows[Candolin07]: service discovery, service authentication, user authentication, access control, confidentiality, integrity, availability, and privacy. To ensure security in a loosely-coupled SOA environment, the open standards communities that created Web services developed a number of security standards for Web services which is one of the most active and widely adopted implementation of SOA. Figure 1 depicts a notional reference model for Web services security standards. This reference model maps the different standards to the different functional layers of a typical Web service implementation.

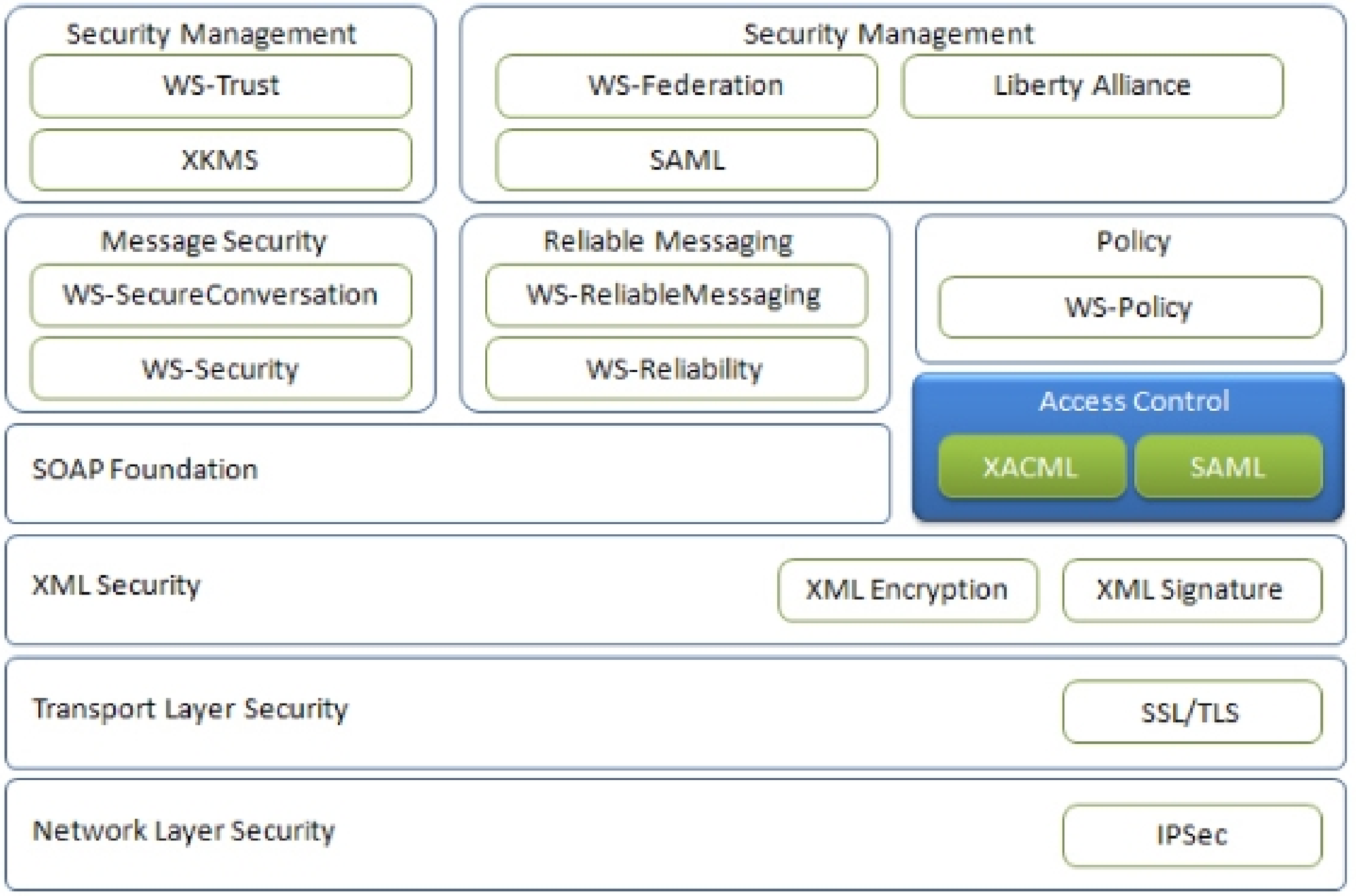

Figure 1. The Web Services Security Stack[Singhal07]

As described above, in the Web Services Security Stack the Security Assertion Markup Language (SAML) and the eXtensible Access Control Markup Language (XACML) are the standard for access control which means that when the service is requested by a user the service must enforce the specified security policy related to access control. We focus on access control in the Web Services security and represent what SAML and XACML are, how they work and where they are able to be applied together.

---

2. SAML (Security Assertion Markup Language)

SAML is an XML standard for exchanging authentication and authorization data between security domains. SAML has the feature like platform independent and is mainly applied to Single Sign-On (SSO).

2.1 What Is SAML?[Madsen05]

As many web sites are created and a lot of application systems are developed, federation is the prominent movement in identity management. Federation is defined as the establishment of business agreements, cryptographic trust, and user identifiers across security and policy domains to provide seamless cross-domain business interactions. As Web service based on XML turns up and provides integration between business entities by loose coupling at the application and messaging layer, federation can do so without the relation to the other's authentication and authorization infrastructure. To make this loose coupling possible at the identity management layer the standardized mechanisms and formats for exchanging security information is necessary and that is SAML.

SAML, created by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS), is a *an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.* [Madsen05]
SAML is a flexible and extensible protocol designed to be used - and customized if necessary - by other standards.

2.2 SAML Architecture[Ragouzis08]

SAML consists of six components as follows: assertions, protocols, bindings, profiles, metadata, authentication context. The relationship between these components is similar to building-blocks and when they are put together they allow a number of use cases to be supported such as web single sign-on use case and identity federation use case. The components mainly enable to transfer secure information like identity, authentication, and authorization information between trusted entities.

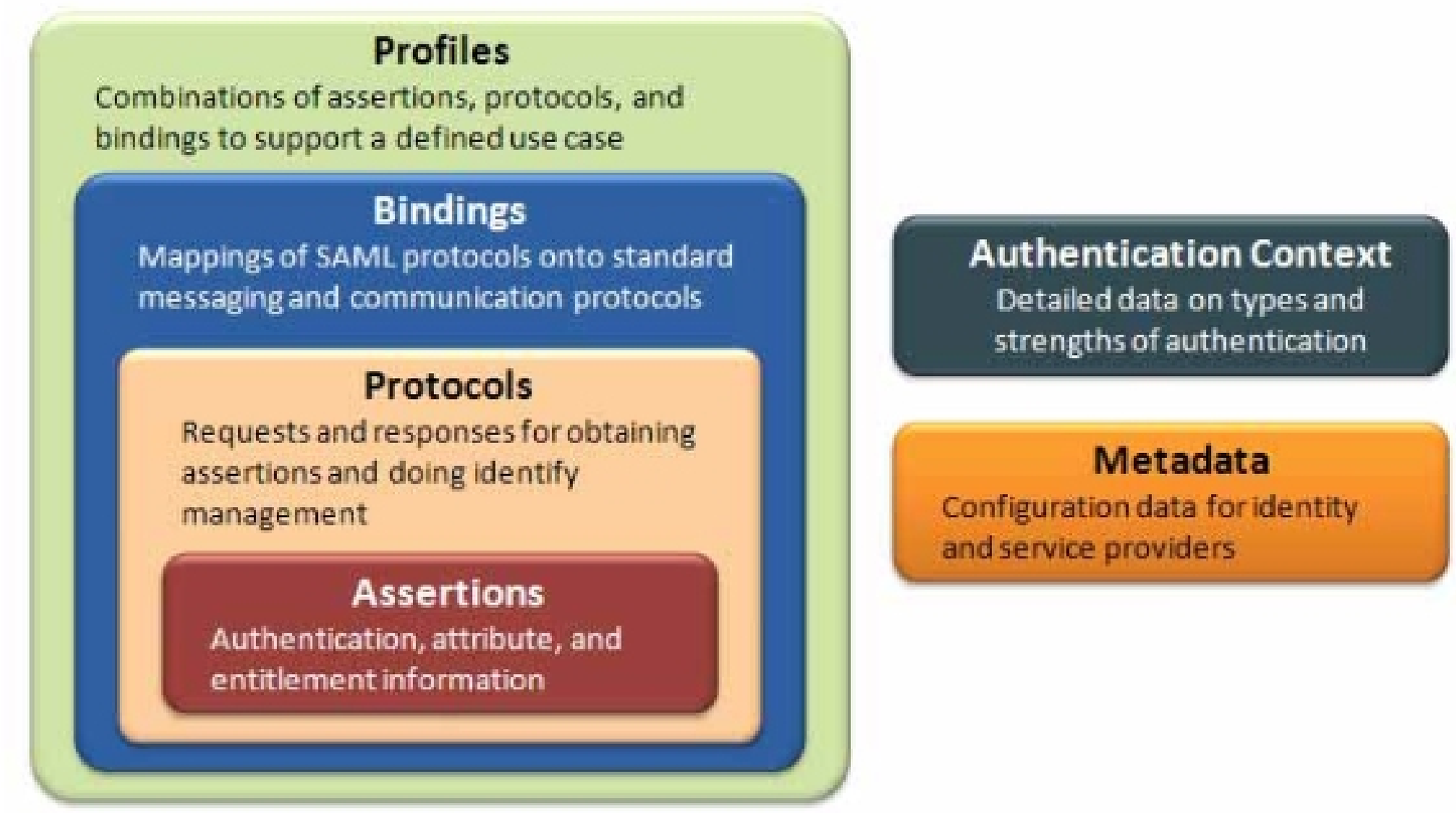

Figure 2. the relationship between basic SAML Concepts

- SAML assertions contain identifying information made by a SAML authority. In SAML, there are three assertions: authentication, attribute, and authorization. Authentication assertion validates that the