Chapter VIII
Using SAML and XACML for Web Service Security and Privacy¹

Tuncay Namli
Middle East Technical University, Turkey

Asuman Dogac
Middle East Technical University, Turkey

ABSTRACT
Web service technology changes the way of conducting business by opening their services to the whole business world over the networks. This property of Web services makes the security and privacy issues more important because the access to the services becomes easier. Many Web service standards are emerging to make Web services secure and privacy protected. This chapter discusses two of them; SAML (OASIS, 2005) and XACML (OASIS, 2005). SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. In other words, SAML handles the user authentication and also carries attribute information for authorization (access control). XACML is the complementary standard of OASIS to make the access control decisions. This work is realized within the scope of the IST 027074 SAPHIRE Project which is an intelligent health care monitoring and decision support system.

INTRODUCTION
Web service technology changes the way of conducting business by opening their services to the whole business world over the networks. This property of Web services makes the security and privacy issues more important because the access to the services becomes easier. Furthermore, the privacy and security issues are indispensable for Web service technology in order to make them acceptable in more sensitive business transactions.

In this chapter, we discuss two security and privacy related standards for Web services, namely, SAML (OASIS, 2005) and XACML (OASIS, 2005). SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information (OASIS, 2006, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security). In other words, SAML handles the user authentication and also carries attribute information for authorization (access control). XACML is the complementary standard of OASIS to make the access control decisions. For example, once the identity of a physician is confirmed by the system using SAML, whether this physician in the role he plays has the right to access the particular data of a particular patient can be decided by using XACML mechanisms.

Generally, the clients of the Web services are the software, not the direct users in B2B systems. Therefore, usually access control decisions may not be needed and only the authentication of the requestor software is enough. However, there are cases where authorization of the user becomes important. In this chapter, we give a real life Web service example from the health care domain where a medical institute serves access to medical documents. Because a patient’s medical data is sensitive information, the Web service needs an authentication mechanism to authenticate the user. Furthermore, an authorization decision is necessary to decide if the user is allowed to access to the Web service and the resource that it has requested.

This chapter describes the use of SAML and XACML technologies to provide for the security and privacy of Web services. This work is realized within the scope of the IST 027074 SAPHIRE Project, which is an intelligent health care monitoring and decision support system. SAPHIRE System is a platform integrating the wireless medical sensor data with hospital information systems. The patient monitoring is achieved by using agent technology where the “agent behaviour” is based on computerized clinical practice guidelines. The patient medical history stored in medical information systems is accessed through semantically enriched Web services. In this way, not only the observations received from wireless medical sensors, but also the patient medical history, is used in the reasoning process. The security and the privacy architectures described in this chapter are developed for the SAPHIRE system.

The chapter is organized as follows; In Section 3, OASIS standard XACML, the policy language, the processing environment, and the request/response context are described. Section 4 describes the Web Service profile of XACML. Section 5 and Section 6 provide the details of the XACML’s SAML profile. This profile describes how to use SAML to carry XACML instances and Role Based Access Control (RBAC) profile of XACML. Section 7 describes the SAML token profile for Web Service Security and subject confirmation methods. Finally, Section 8 presents a comprehensive real life example from the medical domain which uses all the given profiles described in this chapter.

**ACCESS CONTROL AND SINGLE SIGN-ON**

In order to provide a strong access control mechanism, a system should deal with several class types. For example, the system should be able to deal with the properties of participating entities.