

Standards for XML and Web Services Security

Martin Naedele, ABB Corporate Research

XML schemas convey the data syntax and semantics for various application domains, such as business-to-business transactions, medical records, and production status reports. However, these schemas seldom address security issues, which can lead to a worst-case scenario of systems and protocols with no security at all. At best, it confines security to transport-level mechanisms like secure sockets layer (SSL).

On the other hand, the omission of security provisions from domain schemas opens the way for generic security specifications based on XML document and grammar extensions. These specifications are orthogonal to domain schemas but integrate with them to support a variety of security objectives, such as confidentiality, integrity, and access control.

In 2002, several specifications progressed toward providing a comprehensive standards framework for secure XML-based applications. Figure 1 shows some of the most important specifications, the issues they address, and their dependencies.

XML signatures (XML DSig)

Digital signatures serve as persistent proof of a document's data integrity as



Several standards are establishing a framework for integrating security into domain-specific XML-based applications.

well as nonrepudiable evidence of who created it. The XML Signature Syntax and Processing specification describes an XML syntax for representing the associations between cryptographic signatures and XML documents or other electronic resources. The specification also includes procedures for computing and verifying XML signatures.

An XML digital signature differs from other protocols for message signing, such as PGP (www.pgpi.org/), in its support for signing only specific portions of the XML tree rather than the complete document. This is relevant, for example, in workflow scenarios.

In addition, the XML signature specification defines mechanisms for countersigning and for transformations—so-called canonicalizations—to ensure that two instances of the same text produce the same digest for signing even if their representations differ slightly—for example, in typographic white space.

XML encryption (XML Enc)

The XML Encryption Syntax and Processing specification defines an XML vocabulary and processing rules for protecting confidentiality of XML documents—in whole or in part—and of non-XML data as well. The encrypted content and additional processing information for the recipient are represented in well-formed XML, so that the result can be further processed using XML tools.

In contrast to other commonly used technologies for confidentiality such as SSL or virtual private networks, XML encryption also applies to document parts and to documents in persistent storage.

Security Assertion Markup Language

SAML is an XML-based framework for request/response exchanges of authentication and authorization information. Such exchanges occur, for example, between interacting applications that do not share the same underlying authentication and authorization infrastructure. The differences may be organizational (different, unconnected Windows domains) or platform-based (Windows versus Java). In any case, SAML can be used to realize single sign-on (SSO) between different systems and platforms.

SAML statements are called *assertions*. They are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different information items referring to authentication (identity), authorization decisions, and attributes such as credentials or group member-

ship designators. SAML assertions describe the results of authentication actions that occurred previously.

The use of SAML assumes and requires trust between the participants, but the SAML protocol does not include provisions to establish or guarantee this trust. SAML is not concerned with guaranteeing confidentiality, integrity, or nonrepudiability of the assertions in transit. For these purposes, it refers to XML Enc and XML DSig or to other mechanisms provided by the underlying communication protocol and platform.

Extensible Access Control Markup Language

XACML is an XML specification for expressing fine-grained information-access policies in XML documents or any other electronic resource.

At configuration time, XACML expresses and communicates the rules and policies that an access-control mechanism uses to derive an access decision for a set of subjects and attributes. By comparison, at runtime SAML formulates assertions about subjects, their attributes, and their access rights. For digital rights management or workflow processing use cases, an application or medium can transmit XACML rules together with the content to which access is being regulated. If necessary, mechanisms outside XACML must but be used to enforce the integrity of access rules and confidentiality of content.

The XACML specification defines ways to encode rules, bundle rules to policies, and define selection and combination algorithms in cases where multiple rules and policies apply.

Access control lists in XACML are 4-tuples—subject, target object, permitted action, provision. The *subject* can include user IDs, groups, or role names. The *target object* allows granularity down to a single XML document element. The *permitted action* primitive can be either read, write, create, or delete. This represents a major XACML limitation because it does not

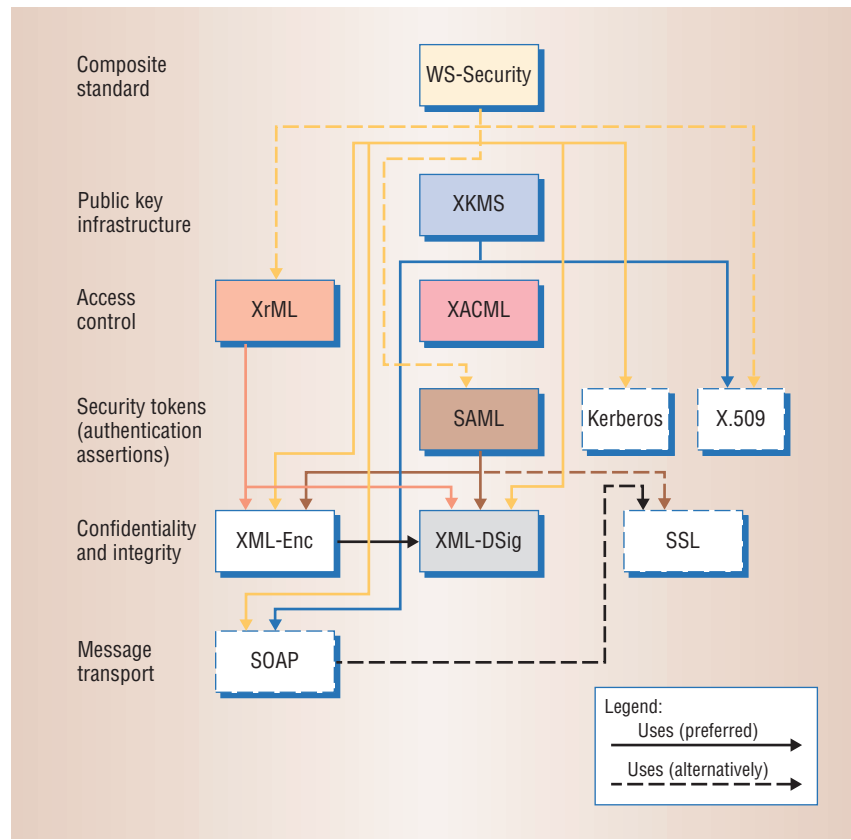


Figure 1. XML and Web services security standards and their dependencies. Standards discussed in this column appear in boxes with solid outlines; related standards appear in boxes with dashed outlines. Issues the standards address are listed on the left.

accommodate domain-specific permission types. A *provision* is an action that must execute upon a rule's activation (for both deny and grant rules). Such actions may include initiating log-in, requesting additional credentials, and sending an alert. The XACML specification defines a language for formulating such provisions.

Extensible Rights Markup Language

XrML is a general-purpose, XML-based specification for expressing rights and conditions, such as expiration times, associated with digital resources and services.

XrML focuses on digital rights management, but it overlaps with XACML. XACML is the more comprehensive and flexible specification. XrML is easier to use but not suited to complex

access policy or rule sets. XrML is resource agnostic, whereas XACML provides explicit means to involve resource characteristics in the access decision.

XrML does not address authentication and protection of the rights expressions. Like XACML, it leaves those matters to encryption and digital signature protocols like XML DSig and XML Enc.

XML Key Management Specification

XKMS defines a Web service interface for a public key infrastructure to manage keys for use with protocols like XML DSig and XML Enc.

Based on XML, the simple object access protocol (SOAP), and Web Services Description Language, XKMS contains two subprotocols: XML Key

Table 1. XML security specifications, sponsoring organizations, and status.

Specification	Organization	Status
XML DSig	Joint Working Group of the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C); www.w3.org/signature/	W3C recommendation, February 2002 (www.w3.org/TR/xmlenc-core/) and IETF draft standard RFC 3275, March 2002 (www.ietf.org/rfc/rfc3275.txt). Exclusive XML Canonicalization 1.0 transform specification, W3C recommendation, July 2002 (www.w3.org/TR/xml.exc-c14n/)
XML Enc	W3C XML Encryption Working Group; www.w3.org/encryption/2001/	W3C recommendation since December 2002; www.w3.org/TR/xml-enc-core/
SAML 1.0	XML-based Security Services Technical Committee (TC) of the Organization for the Advancement of Structured Information Standards (OASIS); www.oasis-open.org/committees/security/	OASIS standard since November 2002; www.oasis.open.org/committees/security/docs/cs-sstc-core-01.pdf
XACML 1.0	OASIS Extensible Access Control Markup Language TC; www.oasis-open.org/committees/xacml/	OASIS standard since February 2003; ../repository/cs-xacml-specification-01-1.pdf
XrML 2.1	OASIS Rights Language TC www.oasis-open.org/committees/rights/	Initial submission by ContentGuard in May 2002; ../documents/xrml.200205.zip ; www.xrml.org
XKMS 2.0	W3C XML Key Management Working Group; www.w3.org/2001/XKMS	W3C Note, working toward last-call working draft
WS Security 1.0	OASIS Web Services Security TC; www.oasis-open.org/committees/wss/	Initial submission in June 2002, addendum in August 2002; OASIS working draft v8 in December 2002; www.verisign.com/wss/wss.pdf , www.verisign.com/wss/ws-Security-Addendum.pdf

Information Service Specification and XML Key Registration Service Specification. X-KISS locates and retrieves public keys from a key server to be used in, for example, encryption or signature verification. An application can also use X-KISS to verify that a certain key has not been revoked. X-KRSS defines service interfaces for registering, revoking, and recovering escrowed keys from a key server.

Web services security

The WS-Security specification defines new SOAP extensions (message headers) to provide per-message authentication, as well as end-to-end message confidentiality using XML Enc and end-to-end message integrity using XML DSig in a Web services environment. WS-Security also defines the use of time stamps to prevent message replay.

Application developers and protocol designers can combine the specification elements in different ways to realize various security protocols. WS-

Security is independent of HTTP and HTTP-S for transport. The WS-Security mechanism for inclusion of security tokens (authenticators) supports Username, Kerberos, X.509, SAML, and XrML.

In April 2002, IBM and Microsoft issued a roadmap (www-106.ibm.com/developerworks/webservices/library/ws-secmap/) proposing additional specifications to address a variety of other issues associated with Web services security. These include WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation, and WS-Authorization. In February 2003, the Component-Based Development and Integration Forum (www.cbdiforum.com), an independent think-tank, reported the first successful WS-Security interoperability demonstration between Microsoft and IBM environments.

As Table 1 shows, several of these XML security initiatives reached major milestones in 2002. The

Gartner Group, a market research consultancy, estimates that it may take until 2004 before these specifications provide a complete standards foundation for XML security. Nevertheless, the existing set establishes a good framework for developers who need to integrate security functionality into their XML-based applications. ■

Martin Naedele is a research engineer with the Information Technology Dept. of ABB Corporate Research in Switzerland. Contact him at martin.naedele@ch.abb.com.

**Editor: William A. Arbaugh,
Dept. of Computer Science,
University of Maryland at College Park;
waa@cs.umd.edu**