Created: February 19, 2004.

# OASIS SAML Interoperability Event Demonstrates Single Sign-On at RSA Conference.

OASIS has announced that several vendors will team with the U.S. General Service Administration E-Gov E-Authentication Initiative at the RSA Conference 2004 to demonstrate interoperability of the Security Assertion Markup Language (SAML). Vendor participants include Computer Associates, DataPower Technology, Entrust, Hewlett-Packard, Oblix, OpenNetwork, RSA Security, Sun Microsystems, and others.

SAML Version 1.1 is an OASIS authentication and authorization standard based upon an XML framework for exchanging security information. "This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. A typical example of a subject is a person, identified by his or her email address in a particular Internet DNS domain. One major design goal for SAML is Single Sign-On (SSO), the ability of a user to authenticate in one domain and use resources in other domains without re-authenticating."

The unique teaming of the U.U. General Service Administration with eleven vendors in this RSA event "showcases interoperability across three separate scenarios, simulating interaction between a government or enterprise portal and sites from typical content or service providers. For the first time ever, members of the OASIS Security Services Technical Committee will demonstrate both types of SAML version 1.1 Single Sign-On, along with additional scenarios that highlight SAML's flexibility. The event is sponsored by the U.S. GSA E-Gov E-Authentication Initiative, which is committed to delivering open standards-based authentication solutions to U.S. government agencies."

In connection with the OASIS SAML 1.1 Interoperability Showcase, members of the Security Services TC have published a *Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1* as a committee working draft.

**About SAML Version 1.1**

> *Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1*. TC Working Draft 01. 16-February-2004. Document identifier: 'sstc-saml-tech-overview-1.1-draft-01' Edited by John Hughes (Entegrity Solutions) and Eve Maler (Sun Microsystems). 17 pages.
>
> Technical Overview Abstract: "The Security Assertion Markup Language (SAML) standard defines a framework for exchanging

security information between online business partners. It was developed by the Security Services Technical Committee (SSTC) of the standards organization OASIS (the Organization for the Advancement of Structured Information Standards). This document provides a technical description of SAML V1.1."

SAML Version 1.1 "focuses on improving interoperability and specification clarity through experience with Version 1.0, and in particular on tightening up the relationship of SAML with XML Signature. In general, minor revisions of SAML can be expected to be backwards compatible. This version is very slightly incompatible with SAML Version 1.0 in the area of XML Signature in order to take advantage of new knowledge about XML Signature processing..." TC FAQ document]

**SAML Version 1.1 Committee Specification Documents**

- *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1*. Edited by Eve Maler (Sun Microsystems), Prateek Mishra (Netegrity), and Rob Philpott (RSA Security). OASIS Committee Specification. 27-May-2003. Document identifier: sstc-saml-core-1.1-cs-01. 53 pages. This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocol that conveys this information. XML schemas:
  - XML Assertion Schema (.xsd), see also the display version.
  - XML Protocol Schema (.xsd), see also the display version.
- *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1*. Edited by Eve Maler (Sun Microsystems), Prateek Mishra (Netegrity), and Rob Philpott (RSA Security). OASIS Committee Specification. 27-May-2003. Document identifier: sstc-saml-bindings-1.1-cs-01. 31 pages. This specification defines protocol bindings and profiles for the use of SAML assertions and request-response messages in communications protocols and frameworks.
- *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1*. Edited by Eve Maler (Sun Microsystems) and Rob Philpott (RSA Security). OASIS Committee Specification. 27-May-2003. Document identifier: sstc-saml-sec-consider-1.1-cs-01. 26 pages. This specification describes and analyzes the security and privacy properties of SAML.

- *Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) V1.1*. Edited by Eve Maler (Sun Microsystems), Prateek Mishra (Netegrity), and Rob Philpott (RSA Security). OASIS Committee Specification. 27-May-2003. Document identifier: sstc-saml-conform-1.1-cs-01. 22 pages. This specification describes the program and technical requirements for SAML conformance.
- *Glossary for the OASIS Security Assertion Markup Language (SAML) V1.1*. Edited by Eve Maler (Sun Microsystems) and Rob Philpott (RSA Security). OASIS Committee Specification. 27-May-2003. Document identifier: sstc-saml-glossary-1.1-cs-01. 13 pages. This specification defines terms used throughout the OASIS Security Assertion Markup Language (SAML) specifications and related documents.

**About SAML Version 2.0**

SAML Version 2.0: Work on SAML v2.0 began in the Summer of 2003 and is projected to be complete sometime in 2004. The goals of the Version 2.0 effort are:

- "Addressing issues and enhancement requests that have arisen from experience with real-world SAML implementations and with standards architectures that use SAML, such as the OASIS WSS and XACML work.
- Adding support for features that were deferred from previous versions of SAML for schedule reasons, such as session support, the exchange of metadata to ensure more interoperable interactions, and collection of credentials.
- Converging on a unified technology approach for identity federation by integrating the specifications contributed to the TC by the Liberty Alliance..."

The SAML 2.0 effort intends to deliver on the following goals: (1) Address issues and enhancement requests that have arisen from experience with real-world SAML implementations and with other security architectures that use SAML; (2) Adding support for features that were deferred from previous versions of SAML. (3) Develop an approach for unifying various identity federation models found in real-world SAML implementations and SAML-based security architectures.

SAML Version 2.0 work item examples: (1) Session Support: Global signout and similar would be considered simple sessions.

Complex sessions would include things like global timeout. Boeing has provided input on their requirements around this. (2) Peristent pseudonyms for principals: This should also include privacy and anonymity features à la Shibboleth and Liberty. This should include the notion of an anonymous name identifier. (3) SSO with Attribute Exchange: This can be used to achieve a kind of federation without using an account-linking model. (4) Metadata and Exchange Protocol: This work has already begun; it should include SAML feature discovery through a WSDL file. SAML metadata might want to include a way to discover supported types of authentication protocols. (5) SSO Profile Enhancements: Richer SSO profiles, including (signed) requests from destination sites, control over authentication, passivity, extensibility, and source site discovery..." [from the TC FAQ and Scope documents]

SAML Version 2.0 Working Drafts as of 2004-02-19:

- "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. TC Working Draft version 05. 17-February-2004. With Assertion Schema and Protocol Schema. "This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocols that conveys this information."
- "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0." Working Draft, 2-January-2004. "This specification defines protocol bindings and profiles for the use of SAML assertions and request-response messages in communications protocols and frameworks."
- "Metadata for SAML 2.0 Web Browser SSO Profiles." Working Draft 00. 15-September-2003. With XML Schema. "The SAML Web Browser SSO Profiles require agreements between source and destination sites about information such as URLs, source and destination IDs, certificates and keys, and so forth. Metadata definitions are useful for describing this information in a standardized way. This document defines metadata that describe the elements and attributes required to use the SAML Web Browser SSO Profiles. Since the Liberty Alliance Web SSO Profiles are directly based on the SAML Web SSO Profiles, the metadata defined in this document borrows extensively from the metadata definitions in the draft Liberty Alliance 1.2 specifications..."
- "Metadata Discovery Protocols for SAML 2.0 Web Browser SSO Profiles." Working Draft 00. 01-October-2003. "The SAML Web Browser SSO Profiles require agreements between source and destination sites about supported protocols, service end points, supported profiles, source and destination IDs, certificates, cryptographic keys, and so forth. Metadata definitions are useful for describing this information in a standardized way. Moreover, it is desirable for assertion producers and consumers to have standard ways for discovering metadata about each other. This document

describes a proposal for Metadata Discovery Protocol. The proposal described in this document borrows extensively from the metadata discovery protocol defined in the draft Liberty Alliance 1.2 specifications..."

- "Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0." Working Draft 01. 5-January-2004.

**About the U.S. E-Authentication E-Gov Initiative**

"The E-Authentication E-Gov initiative is setting the standards for the identity proofing of individuals and businesses. E-Authentication will focus on meeting the authentication business needs of E-Gov initiatives by building the necessary infrastructure to support common processes and systems for governmentwide use. E-Authentication's mission is to enable trust -- an inherent part of every online exchange between citizens and the government.

Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. E-Authentication makes that trust possible. E-Authentication is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used. The initiative will focus on meeting the authentication business needs of the E-Gov initiatives, building the necessary infrastructure to support common, unified processes and systems for government-wide use. This will help build the trust that must be an inherent part of every online exchange between citizens and the Government..."

Authentication defines the level of trust or trustworthiness of the parties involved in a transaction — it is the process of determining the certainty that someone really is who they claim to be... E-Authentication provides a uniform set of policies and technologies developed to ensure appropriate authentication of users for all electronic transactions with the Government, allowing agencies to focus on their core lines of business. By using E-Authentication, agencies save human and financial resources that would otherwise be tied up creating redundant authentication solutions. An electronic credential binds an individual to a technology such as PINS, PKI certificates and smartcards, creating an electronic identity. The types of electronic credentials E-Authentication will accept are PINS, passwords and PKI-based credentials. The level of authentication of an electronic credential is the degree of confidence in the binding of the identity to the credential issued. The processes and controls employed in the operation of the credential service provider (CSP) and the methods used to protect the subscriber's information determine the assurance level. Some business transactions need to know exactly who you are while

others don't. Since the E-Authentication Initiative supports all E-Gov transactions, it must support multiple levels of assurance. [from the Home Page and FAQ document]

**Interoperability Lab Report**

Rob Philpott of RSA Security Inc. provided a brief report on the Successful SAML V1.1 Interop Lab at RSA2004 Conference. Excerpt:

"... some news regarding the SAML interoperability lab we held during the RSA2004 conference. The lab was hosted by RSA and sponsored by the General Services Administration (GSA) of the US government and by Sun Microsystems, who provided 19' LCD monitors for everyone to use... We had eleven vendors participating in the interop. We also had Enspier Technologies participating under contract to GSA. The vendors that participated in the event were Computer Associates, DataPower Technology, Entegrity Solutions, Entrust, Hewlett-Packard, Oblix, OpenNetwork, Ping Identity, RSA Security, Sun Microsystems, and Trustgenix. There were two key goals for the interop. First, we wanted to demonstrate SAML 1.1 interoperability for both Web SSO profiles and for general queries. The other main goal was to show an interoperable implementation of the GSA eGov program's eAuthentication architecture that builds on top of SAML. Also, given that the major change for SAML 1.1 dealt with improving XML DSIG interoperability, we certainly wanted to demonstrate this in the process... All vendors except DataPower implemented the Web SSO use cases, providing both the SAML 1.1 Web SSO Profile and eAuthentication demo scenarios. All of these vendors supported the Browser/Artifact Profile and all but two supported the Browser/POST Profile. Enspier provided a portal that implemented the additional exchanges defined by the eGov program's eAuthentication architecture. Each vendor implemented the AP and RP sides of these exchanges during the lab. The portal was also enhanced to support the generic SAML demo as well. The SAML query use case was demonstrated by DataPower who implemented a simple web services-based demo utilizing SAML 1.1 Attribute Queries to the RSA Attribute Authority... The interop testing proved that the SSTC's goal of producing a quality SAML V1.1 specification that improved interoperability was convincingly achieved. We found no defects in the V1.1 standard..."

**Principal references:**

- Announcement 2004-02-25: "OASIS SAML Interoperability Lab Demonstrates Single Sign-On for GSA E-Gov's E-Authentication Initiative. Computer Associates, DataPower Technology, Entrust, Hewlett-Packard, Oblix, OpenNetwork, RSA Security, Sun Microsystems, and Others Showcase Authentication and Authorization Standard at RSA Conference."
- Interop Announcement 2004-02-19: "OASIS SAML Interoperability Lab To Demonstrate Single Sign-On."
- Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1
- OASIS Security Services TC website
- SAML Version 2.0 Scope and Work Items. February 17, 2004.
- "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. TC Working Draft version 05. 17-February-2004.
- U.S. E-Authentication Initiative web site
- E-Authentication FAQ document
- "Getting to Green with E-Authentication: Technical Approach." Chris Louden Enspier. February 3, 2004.
- U.S. General Services Administration (GSA) web site
- RSA Conference 2004. 13th Annual RSA Event. February 23-27, 2004. Moscone Center, San Francisco, CA, USA.
- "Successful SAML V1.1 Interop Lab at RSA2004 Conference."
- Earlier SAML news:
    - OASIS TC Approves Version 1.1 Specifications for Security Assertion Markup Language (SAML)."
    - Sun ONE Identity Server 6.0 Supports Liberty Alliance and SAML Specifications."
    - Security Assertion Markup Language (SAML) Version 1.0 an OASIS Open Standard."
    - Burton Group's Catalyst Conference Features SAML Interoperability Event."
- "Security Assertion Markup Language (SAML)" - Main reference page.