Working Group Charter: Basic Security Profile

Basic Security Profile (secprofile)

Document Version: 1.8

Creation Date: 7 March 2003
Revision Date: 19 July 2005

Document Editor:
Paul Cotton, Microsoft Corporation

This Working Group will produce an extension profile called the Basic Security Profile.

Table of Contents

1. Goals and Mission

The Basic Security Profile Working Group will develop an interoperability profile dealing with transport security, SOAP messaging security, and other Basic Profile-oriented security considerations of Web services.

The group will develop and select a set of usage scenarios and their component message exchange patterns (MEPs) to guide the profiling work. The Basic Security Profile group will use the WS-I Security Plan Framework document, particularly its collection of usage scenarios and use cases, and the WS-I Work Plan for Web Services Security Interoperability as input to its work.

2. Working Group Chair and Membership

Chair: Paul Cotton, Microsoft Corporation

The Chair is appointed by the WS-I Board. The membership will be determined as a part of the WS-I community activity.

3. Working Group Composition and Responsibilities

Participants should include, but not be limited to, those engaged in Web service security development, software architects, and experts in the security domain. Some participants should come from the currently existing working groups in order to build on existing experience.

4. Scope of Effort

This Working Group will focus on the development of the Basic Security Profile and on the development of ancillary material that serves to ground the development of this profile. The Basic Security Profile is intended to be layered on the Basic Profile as an “extension

profile," as that term is defined in the Profile Versioning and Composition Editor's Draft of 28 January 2003. The profile will cover interoperability of both transport-layer security and SOAP messaging security, as well as other security considerations implicated by the Basic Profile.

The group will develop and select a set of usage scenarios and their component message exchange patterns (MEPs) to guide the profiling work. It will also develop business use cases as necessary to motivate the profile's applicability to real-world problems, but is not responsible for a cohesive set of use cases, which will be the responsibility of a Sample Applications Working Group that will be tasked with security-profile-conforming application development. The Basic Security Profile group will work closely with the Sample Applications group to this end.

The Basic Security Profile will be based on the following specifications as used in the context of the Basic Profile and the Security Scenarios:

- Transport security (HTTP over TLS ("HTTPS") [RFC 2818])

  This specification is built on HTTP V1.1. Note that the Basic Profile already states some requirements on the use of this specification and others referenced from it.

- SOAP attachment security (RFC 2392 and OASIS Web Services Security WSS SOAP Messages with Attachments (SWA) Profile V1.1 [WSSTC])

  The profiling of this set of specifications is based on the attachment technologies selected by Basic Profile V1.1 and Attachment Profile V1.0.

- SOAP message security (OASIS Web Services Security V1.0 [WSSTC])

  The security tokens to be profiled are username, X.509. SAML, and REL.

- SOAP message security (OASIS Web Services Security V1.1 [WSSTC])

  The Kerberos security token will be profiled based on WSS V1.1.

Other technologies already appearing in the Basic Profile, such as HTTP and SOAP, may also need to be further profiled in the Basic Security Profile depending on the scenarios selected.

Each security technology in the scope of this work is at the root of a tree of normative dependencies on other technologies. For example, the OASIS Web Services Security specifications depend on XML Signature, which in turn depends on XPath. The interoperability profiling of referenced technologies should be constrained only to the portion explicitly used by the initially profiled technology. For example, arbitrary use of XPath not otherwise provided for in the "root" specifications is not in scope for profiling.

The group should solicit early public feedback for at least its Security Scenarios document (see Section 5) for the purpose of vetting security considerations. Interoperability of security technologies does not in and of itself ensure security, and the act of combining new technologies and protocols is especially susceptible to security threats. It is thus essential for the Basic Security Profile Working Group to take steps to avoid introducing new security threats.

5. Required Deliverables

The required deliverables of this Working Group are as follows:

- **Security Scenarios**: This document defines the requirements for and scope of the Basic Security Profile. It contains a selected set of usage scenarios and their component

MEPs, along with any business use cases required to motivate their selection. [Completed: May, 2005]

- **Basic Security Profile**: This document profiles the specifications used to provide security for the selected Web services scenarios, by providing clarifications and restrictions designed to promote interoperability of those technologies.

The WS-I Security Plan Framework document should be used as input to the development of these deliverables, but the completion of the framework is not a required deliverable.

6. Duration of Working Group and Schedule of Work

This Working Group has until twelve months after the OASIS Web Services Security specifications reach Committee Specification status to produce Candidate Approval Drafts of its deliverables. The Working Group will then remain active through the "Adoption of Material" process as per Article VII, Section 6 of the WS-I Bylaws. The Board may, at its discretion, extend the Working Group's term to accommodate rework associated with proposed changes from Working Group members, the Board, and the WS-I Membership.

Following is the recommended schedule of work:

1. By Sep 2005, make available to WS-I members a Basic Security Profile 1.0 Working Group Approval Draft based on the Security Scenarios and OASIS Web Services Security V1.0 [WSSTC] and the username, X.509, SAML, and REL token profiles. BSP 1.0 will also profile SWA and the Kerberos token profile from Web Services Security V1.1 [WSSTC] .
2. By Dec 2005, make available to WS-I members a Basic Security Profile 1.1 Working Group Approval Drafts based on OASIS Web Services Security V1.1 [WSSTC].

7. Critical Dependencies with Other Groups

The Basic Security Profile Working Group will work closely with a Sample Applications Working Group tasked with covering security matters to ensure that its Security Scenarios and resulting Basic Security Profile can be implemented.

The Basic Security Profile Working Group needs to ensure that its profile reflects the needs of a Test Tools Working Group tasked with covering security matters in testing applications of the Basic Security Profile.

The Basic Security Profile Working Group has a dependency on the OASIS Web Services Security Technical Committee's schedule for producing Committee Specifications, as reflected in Section 6.