D. Merrill, University of Virginia

Recommendations for an OGSA™ Basic SOAP Security Profile

Status of This Memo

This memo provides information to the Grid community on common security requirements for securing OGSA services at the SOAP message level. Distribution is unlimited.

Abstract

This memo reviews the coverage and suitability of three Grid-specific secure communications profiles: the *OGSA Basic Security Profile 1.0 – Core*, the *OGSA Security Profile 1.0 – Secure Channel*, and the *HPC Basic Profile, Version 0.3.* We conclude that there is a gap in the OGSA security architecture profile coverage and that the set of OGSA Basic Security Profiles would benefit from the integration of a new profile that addresses the inclusion of security tokens (and mechanisms for authenticating them) at the SOAP message-level. The integration of this proposed *OGSA Basic SOAP Security Profile* (OGSA BSP-SOAP) would involve a minor re-alignment of the existing OGSA BSP profiles and would derive significantly from the SOAP messaging security considerations in the WS-I Basic Security Profile.

Contents

1 Introduction

Normative profiles are useful tools for understanding and defining the interaction amongst existing Web services specifications in order to achieve interoperability. They are particularly important within the context of secure communication, as common treatment of Web services security specifications (e.g., SSL/TLS, WS-Security and related token profiles, XML-Encryption, XML-Signature, etc.) is crucial for real-world interoperability. In the domain of basic Web services, the WS-I Basic Security Profile 1.0 defines an interoperability profile addressing transport and SOAP messaging security considerations.

To address secure and interoperable interaction within the scope of distributed system management and grid computing, the OGSA-WG has defined two OGSA security profiles: the *OGSA Basic Security Profile 1.0 – Core* and the *OGSA Security Profile 1.0 – Secure Channel*. In the related, but more specific domain of compute-grids, the OGSA-HPCP-WG has defined the *HPC Basic Profile, Version 0.3*, which profiles security requirements for HPC-BP-compliant implementations. In this memo, we briefly review and comment on these profiles and make recommendations for a secure SOAP profile that addresses our concerns.

2 Current Grid Security Profiles

2.1 OGSA Basic Security Profile 1.0 – Core

The *OGSA Basic Security Profile 1.0 – Core* concerns the matter of binding key and key-usage information to a WS-Addressing endpoint reference. More specifically, the profile specifies how to bind any WS-Security security token reference within the metadata section of an endpoint reference.

The profile does not unambiguously indicate how an implementation that consumes such embedded security token references is expected to use those references. For example, consider the following scenarios:

i. Is the key information relevant for transport-level security? For example, a client might compare an X509 certificate token embedded within an endpoint reference with the one provided by the remote endpoint during an SSL/TLS secure transport handshake in order to verify that the remote party is the same as indicated by the endpoint reference.

ii. Does the key usage indicate any *server-side* confidentiality requirements? If so, how does a client know which subset of the SOAP message elements (e.g., the entire body, particular elements within the body, header elements, etc.) to perform XML encryption on?

iii. Is this a hint that the client can optionally use this embedded key information to perform XML encryption of message elements for which the *client requires* confidentiality?

iv. In the (likely) event that the token reference is an X.509 certificate (chain), what is the identity that can be authenticated using that end-entity certificate? In a scenario in which stateful endpoints (e.g., WS-Resources within Web services containers) are given individual cryptographic identities (i.e., issuing certificates for resources with their WS-Naming endpoint identifiers embedded within the certificate), an *individual resource* can be authenticated to a client (via a hierarchy of trust and XML encryption/response signature), regardless of how it migrates amongst containers.

By providing guidance for embedding security tokens (particularly X.509 certificates and certificate chains) within endpoint references, this profile takes a significant step towards facilitating SOAP message level security. It is important that we co-locate (and profile) all of the information necessary for communication with an endpoint resource: not just the address URL and reference parameters, but also any key material, transport and message-security actions required by the endpoint resource, cryptographic identity of the

endpoint/resource, etc. By taking this approach (as opposed to, say, extending WSDL to present some subset of this information), the architecture can securely accommodate more advanced features such as secure migration and rebinding.

2.2 OGSA Security Profile 1.0 – Secure Channel

The *OGSA Security Profile 1.0 – Secure Channel* concerns the matter of securing transport-level communication between networked endpoints. Generally speaking, it is a straightforward, direct adaptation of the WS-I BSP's transport-level considerations to the grid domain.

Unfortunately, the Secure Channel Profile may not be *sufficient* to address the security considerations set forth in the OGSA use-cases and functional requirements:

i. In some OGSA implementations (e.g., many based upon the WSRF profile), multiple stateful endpoint resources are hosted within one Web services container. Secure communication performed at the transport-level as per the Secure Channel Profile can only authenticate the container; the client is precluded from being able to authenticate individual resources (let alone authenticate migratable resources).

ii. Although SOAP messages are traditionally exchanged directly between two connected endpoints over the TCP-based HTTP transport protocol, other transport protocols (e.g., JMS, email, proprietary UDP, etc.) are equally viable, as well as support for message-passing intermediaries. Under these alternative scenarios, transport-level security would not be an effective means for securing communication; a profile for secure communication at the SOAP message level would be more appropriate.

iii. Cryptographic delegation of identity is a desirable feature for grid architectures. Although not addressed by the Secure Channel profile, any such delegation of identity becomes more difficult when secure communication is handled at the transport level: the SSL/TLS handshake may need to be extended to incorporate a delegation action, such as the signing of a proxy certificate. (Other issues, such as channel-reuse, would also complicate such delegation.) It seems likely that mechanisms for the delegation of identity/rights/attributes/etc. would be better suited to the SOAP message level.

iv. The Secure Channel Profile makes (at least) one distinguished extension to the WS-I BSP: it requires *mutually*-authenticated (via X.509 certificates) transport level communication. This consideration is made explicitly with the goals of authorization and auditing in mind. Certainly it is true that most clients will want to be assured of the identity of the endpoints that they interact with. Similarly, there are many scenarios in which server-side authorization decisions are likely to be based upon authenticated client identities (especially for resources with identity auditing requirements). However, there are attractive alternative server-side authorization scenarios that are precluded when clients are forced to authenticate with identity certificates: i.e., role/attribute-based authorization, pseudo-anonymous authorization (e.g., Shibboleth-style), etc. In these alternative scenarios, a profile on transport-level security that allowed optional server-side-only authentication in conjunction with a profile for authenticating identity/role/attribute credentials (e.g., X.509 certificates, SAML assertions, etc.) at the SOAP message level would be more appropriate.

2.3 HPC Basic Profile, Version 0.3

The *HPC Basic Profile, Version 0.3* describes the application of a particular set of specifications to realize the basic use-cases for HPC systems. In order to achieve the security requirements set forth in the HPC use-cases, this profile addresses secure communication by specifying two alternative mechanisms:

i. Mutually authenticated TLS/SSL transport communication compliant with the OGSA BSP-SC profile discussed in section 1.2 of this document. Again, the mutual-authentication requirement is made explicitly with the goal of authorization in mind.

ii. Server-side-only authenticated TLS/SSL transport communication in conjunction with username-password authentication at the SOAP message level (as per the WS-S UsernameToken Profile). This alternative is partially compliant with the OGSA BSP-SC profile: the requirement for mutual authentication is removed.

Although the HPC-BP phrases its mechanisms as "message security", we would clarify that most of the secure communication (i.e., confidentiality, integrity) specified is performed at the transport-level rather than at the (SOAP) message-level.

It is notable that the authors of the *HPC Basic Profile, Version 0.3* were compelled to introduce new security profile considerations; ideally the profile would only need to cite specific OGSA security profiles. The inclusion of mechanism (*ii*) is clearly an indication of a gap in the profile coverage within the OGSA security architecture. The introduction of a SOAP message-level credential (viz. username-token) in this profile indicates that there is motivation to provide credentials (albeit non-authenticatable) that are orthogonal to the cryptographic mechanisms used for integrity and confidentiality. A better arrangement would be to profile the authentication of SOAP message-level credentials within the scope of the OGSA security architecture.

3 Recommendations

We would promote the creation of a new OGSA basic security profile that addresses the use of SOAP message-level credentials and message-level mechanisms for authenticating them (as well as message-level integrity and confidentiality): *OGSA Basic SOAP Security Profile* (OGSA BSP-SOAP).

The current OGSA BSP-Core profile is a necessary stepping stone towards achieving secure communication at the SOAP message-level, and would be folded into the new OGSA BSP-SOAP profile. Additionally, we would like to see the following endpoint reference security considerations profiled:

i. The optional indication of server-side confidentiality requirements within the endpoint reference, such as what elements within the messages need to be encrypted with the specified key(s). This could see interesting use-cases in which multiple keys are provided to encrypt different sections of a message destined for a broker-type service that should not be privy to all of the elements it processes.

ii. The optional indication of what token-profile (if any) is required for authorization. For example, the specification of the X.509 or the holder-of-key SAML token profiles would indicate that messages need to be signed. (Note: we are not looking to go down the slippery slope of specifying *which* credentials a resource requires. These types of authorization hints would be out of scope, as they do not impact the message-level security actions. We can foresee clients supplying multiple types of potentially-delegatable credentials at their own discretion.)

iii. An optional sub-profile for embedding WS-Naming EPIs into X.509 certificates so that individual resources are given cryptographic identity. (This is crucial for the secure migration of resources amongst host containers.) Endpoint references containing this type of security token must be WS-Naming compliant, and the EPI contained within the endpoint reference would need to match that contained within the X.509 certificate

The other contribution of the OGSA BSP-SOAP would be a straightforward application of the WS-I BSP's SOAP messaging security considerations to the grid domain. We suggest that the OGSA BSP-SOAP include a small extension to the WS-Addressing specification's Message Addressing Properties to include a note of any *client-required* message-level security actions required for the response message (similar to consideration *i* above). We would strongly recommend that compliant implementations support at a minimum the normative WS-S X.509 security token profiles. Actual authorization mechanisms for making use of these message credentials would be out of scope for the document.

Additionally, we would alter the OGSA BSP-SC profile to reflect an approach similar to the current HPC-BP: support two alternative mechanisms:

i. Mutually authenticated TLS/SSL as per the current OGSA BSP-SC
ii. Server-side-only authenticated TLS/SSL in conjunction with the proposed *OGSA Basic SOAP Security Profile.*