Discussion Document

Outline of OASIS DSS profile for WSS: SOAP Message Security signatures

Frederick Hirsch, Nokia

7 Feb 2004

1. SCOPE OF PROFILE

The purpose of this profile is to support the generation and veriifcation of SOAP Message Security digital signatures placed in SOAP security headers. Such signatures are defined in the OASIS WSS specifications.

Note that this is distinct from arbitrary application ds:Signatures in a SOAP body.

The following is out of scope for this profile:

- Policy communication in the protocol, although a policy-wise server approach may be integrated with this profile.
- Encryption
- Security header wsu:Timestamp processing

The scope of the profile will include some token profiles initially and then others, indicating a need for an extensible approach.

2. PROPOSED APPROACH

SOAP Message Security signatures are ds:Signatures with some special ds:KeyInfo and ds:Reference processing properties (named here "WSS Signatures" for convenience).

Specifically, ds:KeyInfo is either recommended (or potentially required through a WS-I profile) to use a SecurityTokenReference (STR) to obtain the key information from security token. SecurityTokenReference and security token are defined in the WSS: SOAP Message Security specification and WSS token profiles.

A STR-Transform is also defined so that a ds:Reference to a security token reference does not hash the STR, but what is referenced by the STR.

Generating WSS Signatures implies the proper generation of security tokens, a security token reference within KeyInfo and a ds:Signature.

Thus Signature request includes:

a) selection of KeyInfo mechanism, particularly STR
b) Input of security token(s) or specification of desired token to be generated
c) Signature reference definition and other signature options
d) option to include STR Transform for ds:Reference to STR

WSS Signature verification requires the ds:Signature and related security tokens to be passed to the server for verification.

a) pass entire soap message, security header block, or signature and appropriate tokens (?)
b) STR-Transform application to ds:References to STRs where required
c) Appropriate STR and token processing to obtain verification key information in some cases

Additional signature constraints, as noted in WSS SOAP Message Security as well as potentially a WS-I profile should be reflected in the profile.

Creation of signatures will be based on DSS signing protocol, verification on the DSS verification protocol.