For and Against SAML Bearer Token in ebMS3

# Background

ebMS3 is a messaging protocol layered on top of a number of the WS-\* web services standards. It carry payload and control information in SOAP envelopes and employs standard such as WS-Security and WS-Reliable Messaging to secure and ensure delivery of messages both directly and through multi-hop scenarios.

The core standard permits the use of any WS-Security compliant mechanism to be used to secure messages, but only elaborates on X.509 and Username/Password in detail. Recently the ebMS Technical Committee has published a Committee Specification providing additional detail on how messages may be secured using ebMS3.

An alternate approach for the incorporation of SAML is to use X.509 Authentication and include a SAML Bearer token as an authorisation token (refer to 7.10 in ebMS3 Core) on top of X.509 Authentication is known to have been implemented by one vendor.

# X.509 Scenario

In a standard X.509 scenario, the SOAP header contains a digital signature referencing a specific X.509 credential which can be used to verify the signature.



Where the X.509 Certificate contains identity attributes, a public key, and information which establishes its authenticity and currency.



# SAML Scenario

In a standard SAML scenario, the SOAP header contains a digital signature referencing a specific SAML Assertion which can be used to verify the signature. The SAML Assertion is a relatively short lived credential that is obtained by authenticating to a Security Token Service trusted by the Sender and Receiver. Note that where a secret key is used, only the designated recipient will be able to unwrap it to perform a validation.



Where the SAML Certificate contains identity attributes, a public key or secret key, and information which establishes its authenticity and currency.



# SAML Authorised X.509 Scenario

In this scenario, the SOAP header contains a digital signature referencing a specific X.509 Certificate which can be used to verify the signature. The SAML Assertion has been obtained by authenticating to a Security Token Service trusted by the Sender and Receiver using the same X.509 Certificate.

The SAML token should contain an attribute that can be used to link the SAML token to the X.509 Certificate such as fingerprint or copy of public key.

Note that the key in the SAML token is not used and may be omitted.



# Comparison of Scenarios

## SAML Tokens vs X.509 Certificates in Brief

SAML tokens are relatively short lived credentials that are issued dynamically in exchange for proving ownership of a long lived credential. SAML tokens generally contain up to date information with respect to the identity and authority attributes available to the issuer.

SAML tokens due to their limited lifetimes (typically somewhere from 5 minutes to a day depending on application) deliver point in time information which expires. There is no process for cancelling a SAML token prior to expiry although a relying party can make its own decision on required freshness by inspecting the time of issue.

X.509 Certificates are long lived credential, typically in the 1 to 4 year range. Certificates can be issued in an open structure in which case identification information is certified by an issuing authority and can be widely relied on. Certificates can also be self-signed in which case they are only as good as the means by which they are provided to the entity relying on them (a physical exchange between know representatives for example).

Because of their long life certificates tend not to contained information that may change as they have to be re-issued if any that information is relied on. Examples include email addresses and authorities.

Because X.509 Certificates are long lived, certificates other than those that are self-signed, require a revocation mechanism. Each issuer publishes black lists of certificates that are no longer valid (due to loss, compromise, …).

Whenever a certificate is used, it should be validated for authenticity and the black list (known as a Certificate Revocation List or CRL) checked. Note that CRLs are only updated periodically, typically in the range of 30 minutes to 24 hours. The Online Certificate Status Protocol (OCSP) may be used if more up to date checks are required, but the databases from which OCSP responders draw their information may be updated from CRLs so may not be any more current. This is dependent on the issuer.

## Advantages of a SAML based WS-Security Solution

This solution:

* is fully supported by WS-Security Standards and well documented;
* is supported by implementations of common web services stacks (ie. .NET and some Java stacks.)
* provides for non-repudiation (three party non-repudiation when asymmetric keys used)
* provides for use of credentials other than X.509 certificates

## Advantages of a SAML Authorised X.509 based WS-Security Solution

This solution:

* may be easier to implement with some web services stacks.
* Provides two party non-repudiation (chain of identity does not transit the token issuer, only the chain of authority).

## Concerns with a SAML Authorised X.509 based WS-Security Solution

* There is no standard way of linking the X.509 Certificate to the SAML Assertion. In a multi-hop scenario, the Assertion could be copied by any of the intermediaries. Some sort of linkage is recommended so the intermediaries cannot create their own messages with that assertion. Such a scheme would be easy to implement, but there should be a standard way of accomplishing this linkage.
The linkage is not strictly required, but without it, the solution is not as secure as with the linkage.
* The SAML token is capable of providing identity and authority. Using an X.509 credential to provide an additional layer of identity may be adding complexity where it is not warranted.

# Conclusion

SAML Bearer Tokens as authorisation tokens in ebMS3 provide an adequate solution with the following caveats:

* The solution requires a link between the SAML token and the X.509 certificate to provide strong security. While there are several options for doing this, there is no standard way of achieving this.