XML Security Standards

Current and Emerging Specifications attempting to provide standardization of XML security infrastructure

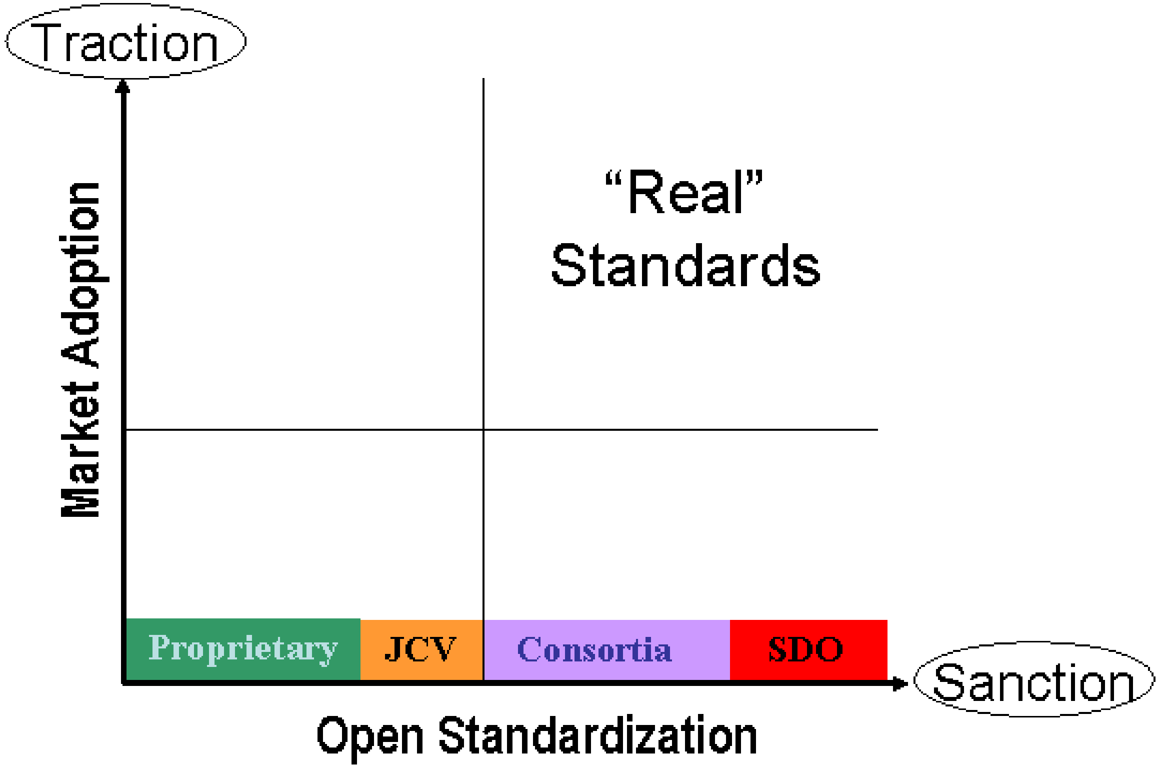
Jorgen Thelin
Chief Scientist
Cape Clear Software Inc.

Specifications and Standards

- There are lots of specifications flying around concerning Web Services
- Not all specifications are, or will be, “real” standards
- The hard part is working out which specifications will “win” and become part of the standard infrastructure
- Vendors and Architects need to plot an “intercept trajectory” for emerging standards

“Real” Standards

Standards Classification Matrix



When is a Specification not a Standard?

- Real standards are:
  - Published by a “recognized” standards development organization – eg. W3C, OASIS
  - Created through a process that allows public comment and feedback
  - Agreed and approved by a committee or group consisting of wide and diverse membership
  - Published at a final or definitive status, such as "W3C Recommendation"
  - Publicly available for reference - most usually by publication on the Internet.
  - Achieving both traction (usage) and sanction (backing)
- Everything else is just a specification **hoping** to become a standard!

Security Standards Overview

- There are several specifications for various aspects of XML and Web Services Security
- The standardization process is still at a very early stage in the evolution
- The front runner specifications are:
  - XML Digital Signatures
  - XML Encryption
  - SAML
  - WS-Security
  - WS-Trust
  - WS-Policy
  - WS-Secure Conversation
  - WS-Security Policy

XML Digital Signatures

- **Source:** W3C
- **Status:** Final

- **Purpose:**
  - Specifies a process for digitally signing data and representing the result in XML
  - Define the processing rules and syntax for XML digital signatures

- **Notes:**
  - A serialised form in XML is defined for the signature
  - The signatures can be applied to information in any form, not just XML-formatted information
  - The specification specifically excludes encryption.

XML Encryption

- **Source:** W3C
- **Status:** Final

- **Purpose:**
  - Specifies a process for encrypting data and representing the result in XML such that it is only discernable to the intended recipients and opaque to all others

- **Notes:**
  - The information that is encrypted can be arbitrary data (including an XML document), an XML element, or XML element content
  - The result is an XML Encryption element that contains or identifies the cipher data
  - The standard is generally accepted in the industry, although not yet in widespread use

SAML

- **Source:** OASIS
- **Status:** Final

- **Purpose:**
  - Uses XML to encode authentication and authorization information in “assertions”

- **Notes:**
  - Defines a standardized XML format for credential and security assertion data
  - The authentication and authorization information can be moved around systems within or between organizations
  - SAML is platform-independent and language-independent
  - A key objective of SAML is to allow organizations to exchange date regardless of the security system they use

WS-Security

- **Owner:** Microsoft/IBM/Verisign – Now OASIS WSS-TC
- **Status:** WIP for OASIS standardization process

- **Purpose:**
  - Provides a model for many levels of security needed for web services.
  - A general-purpose mechanism to associate security-tokens with messages
  - Describes how to encode binary security tokens in messages using SOAP Headers
  - Includes enhancements to SOAP to provide quality of protection mechanisms

- **Notes:**
  - Builds on top of XML Digital Signatures and XML Encryption specifications
  - WS-Security Addendum adds
    - Facility for timestamp and TTL headers
    - Provides greater protection when passing around passwords and security certificates

- **More Info:**
  - http://www-106.ibm.com/developerworks/library/ws-secure/
  - http://www-106.ibm.com/developerworks/library/ws-secureadd.html

  - WS-Security AppNotes - provide guidance to implementers of the WS-Security specification:
  - http://www-106.ibm.com/developerworks/webservices/library/ws-secapp/

WS-Security - Security Token Types

- The WS-Security specification set defines the following tokens:
  - Unsigned security tokens
    - Username
  - Signed security tokens
    - X.509 certificates (binary)
    - Kerberos tickets (binary)
  - XML security tokens
    - Any XML token, such as SAML
    - Usually self verifying / signed

WS-Security Profile for XML-based Tokens

- **Owner:** Microsoft/IBM/Verisign – Now OASIS WSS
- **Status:** WIP for OASIS standardization process
- **Purpose:**
  - Describes a general framework to enable XML-based security tokens to be used with WS-Security
- **Notes:**
  - Two profiles that use this general framework are provided for:
    - Security Assertion Markup Language (SAML)
    - eXtensible rights Markup Language (XrML).
- **More Info:**
  - http://www-106.ibm.com/developerworks/library/ws-sectoken.html

WS-Trust

- **Owner:** Microsoft/IBM/Verisign/RSA
- **Status:** Initial public draft release – Soliciting comments

- **Purpose:**
  - Uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for the issuance, exchange and validation of security tokens.

- **Notes:**
  - WS-Trust also enables the issuance and dissemination of credentials within different trust domains.

- **More Info:**
  - http://www-106.ibm.com/developerworks/webservices/library/ws-trust/

WS-Policy

- **Owner:** BEA/Microsoft/IBM/SAP
- **Status:** Initial public draft release – Soliciting comments

- **Purpose:**
  - **WS-Policy Framework**
    - Defines a general purpose model and corresponding syntax to describe and communicate Web services policies
    - Allows Service consumers can discover the information they need to know to be able to access services from a Service Provider
    - http://www-106.ibm.com/developerworks/webservices/library/ws-polfram/
  - **WS-Policy Attachments**
    - Provides a general-purpose mechanism for associating policy assertions with subjects (services).
    - Provides two approaches for making assertions:
      - policy assertions defined as part of the definition of the subject
      - policy assertions defined independently of and associated through an external binding to the subject
    - http://www-106.ibm.com/developerworks/webservices/library/ws-polatt/
  - **WS-Policy Assertions**
    - Specifies a set of common message policy assertions that can be specified within a policy
    - http://www-106.ibm.com/developerworks/webservices/library/ws-polas/

WS-Secure Conversation

- **Owner:** Microsoft/IBM/Verisign/RSA
- **Status:** Initial public draft release – Soliciting comments

- **Purpose:**
  - Defines mechanisms for establishing and sharing security contexts, and deriving keys from security contexts, to enable a secure conversation

- **Notes:**
  - Built on top of the WS-Security and WS-Policy models to provide secure communication between services
  - WS-Security focuses on the message authentication model but not a security context, and thus is subject to several forms of security attacks which this specification deals with

- **More Info:**
  - http://www-106.ibm.com/developerworks/webservices/library/ws-secon/

WS-Security Policy

- **Owner:** Microsoft/IBM/Verisign/RSA
- **Status:** Initial public draft release – Soliciting comments
- **Purpose:**
  - Defines a model and syntax to describe and communicate security policy assertions within a larger Policy Framework
  - Covers assertions for security tokens, data integrity, confidentiality, visibility, security headers and the age of a message.
- **More Info:**
  - http://www-106.ibm.com/developerworks/webservices/library/ws-secpol/

The Extensibility / Composability of XML

- XML is designed to be inherently extensible
- XML allows composable data structures by supporting nested content
  - Extra data can be
- Namespaces allow unique identification of data content
- Composability does not require any registration with a central authority, just a unique namespace

Combining Standards / Specifications

- Due to the extensibility features of XML and SOAP, all XML and Security Specifications can generally be combined independently of each other

- For example, add SOAP Headers for:
  - WS-Security X509 Token header to assert identity
  - WS-Policy header to signify:
    - Text encoding requirements
    - Supported languages

- On occasions, ordering of combinations can be significant
  - For example, do you "encrypt" then "digitally sign", or "digitally sign" then "encrypt"

WS-I Basic Security Profile

- From the charter for the new WS-I Basic Security Profile work group:
  - The BSP-WG will develop an interoperability profile dealing with transport security, SOAP message security, and other Basic Profile-oriented security considerations of Web Services
- Although this will not cover all aspects of the emerging XML Security specifications, it will certainly solidify the base levels.

Conclusion

- Only partial agreement on the "real standards" at the moment
  - Rival XML security specifications are still emerging
  - XML security standards have not yet been widely adopted
- New XML security standards are not yet proven (so probably contain "holes")
- WS-I Basic Security Profile will deliver a standardized XML security infrastructure