Web Services Security: SAML Token Profile

- presentation to OASIS Security Services TC
- at RSA in Burlington
- by Ron Monzillo
- Sept. 9, 2003
WS-Security Signature Model

- Security Token
  - Collection of (authority certified) claims

- Signature
  - Establishes signer identity, content integrity
  - Dependent on key binding claim

- Security Token Reference
  - Identifies security tokens to satisfy key binding dependencies
  - May encapsulate security token

- Data Reference
  - Identifies input to digest algorithm
Referencing SAML Assertions

• Key Identifier (remote, local implied)
  — ValueType = saml:Assertion
  — wsse:KeyIdentifier
    • saml:AssertionId
    • saml:Binding
    • saml:Location

• Direct or URI reference (not currently used)
  — remote and local references
  — Dependance on wsu:id (or xsd:id) attribute
    • otherwise overlap with key Identifier

• key name (not used)
  — depends on unique key name for assertion
(off-msg) Assertion Referenced From Header

SOAP envelope

WS-Security Header

Security Token Reference
KeyIdentifier
AssertionID

SOAP body
Holder of Key – Assertion Referenced From KeyInfo

SOAP envelope
WS-Security Header
- Signature
  - KeyInfo
    - Security Token Reference
      - SignedInfo
        - Data Reference
          - SignatureValue

SAML Assertion
- statement
  - Key Binding

SOAP body
Sender Vouches – Assertion Referenced From SignedInfo (note use of “Embedded”)

SOAP envelope

WS-Security Header

- Signature
  - KeyInfo
  - Security Token Reference
    - Attesting Entity’s Security Token
    - Key Binding
  - SignedInfo
    - Data Reference
    - Data Reference
      - transform
  - SignatureValue

Security Token Reference

SAML Assertion

Claims
SAML protocol issues/questions

- Can an intermediate (via Sender vouches) reuse an assertion containing “artifact confirmed” statements?
- Can one request an assertion with statements featuring a particular confirmation method? key confirmation requirment?
- Can a statement with a sender-vouches confirmation method contain a confirmation key?
- Can the entity attesting for a holder-of-key statement be different from the subject of the statement?
WS-Security Encryption Model

- **Reference List**
  - Identifies encrypted content

- **Encrypted Data**
  - Encapsulates encrypted content
  - May depend on key binding claim to identify encryption key

- **Encrypted Key**
  - Conveys encrypted key and Reference List
  - Dependent on key binding claim
XML Encryption Bound to SOAP (Using Reference List)

SOAP envelope
- WS-Security Header
  - Reference List
  - Data Reference
  - Security Token
  - Key Binding

SOAP body
- Encrypted Data
  - KeyInfo
    - Security Token Reference
  - Cipher Data
  - Message Content

Diagram showing the relationship between SOAP envelope and SOAP body with various security components.
XML Encryption Bound to SOAP (using Encrypted Key)

SOAP envelope
WS-Security Header
- Encrypted Key
  - KeyInfo
    - Security Token Reference
      - Reference List
        - Data Reference
          - Cipher Data
            - Key

Message Content
- Encrypted Data
  - Cipher Data
    - Security Token Reference
      - Security Token
        - Claims
  - Security Token Reference