XML Key Management Requirements

W3C XML Key Management Working Group Meeting – Dec 9th, 2001

Frederick Hirsch (Zolera Systems)

Mike Just (Entrust)

Agenda

- Goals and Status
- Draft overview
- Resolved issues
- Open issues
- Next steps

Goals

- Produce W3C Working Draft that captures XML key management requirements
  - 1st work group deliverable in charter
  - Last Call, January 2001
- Expose issues early, achieve consensus
  - Principles, scope and requirements
  - Ensure coordination with other groups

Status

- 1st draft posted Nov 8th

  Source of requirements:
  - XML Key Mgmt Activity Proposal & Charter
  - July Workshop Position Papers & Presentations
  - XKMS version 1.1 (draft 4)
  - XML Trust Center and mailing lists
- 2nd (and latest) draft posted Nov 23rd
  - Incorporates feedback from list and teleconference
- No further feedback on list

Draft Overview: Principles

- Provide Universality and Usability
  - Support simple clients
  - Be transport protocol agnostic but define SOAP/XMLP bindings
  - Be PKI-technology agnostic but ensure compatibility with recognized technologies
  - Be XML-based
  - Provide extensible messaging
  - Clearly define client and server behaviour

Draft Overview:Principles…

- Be Secure
  - Define transaction confidentiality and integrity options
  - Address trust issues
  - Design against known attacks (e.g. replay, substitution)
- Define key management requirements
- Define key information service requirements

Draft Overview: Out of Scope

- Non-repudiation
- Expressing PKI structures in XML
- Authentication & Authorization assertions
- Defining Web Services protocol security
- Anonymous access and service
- Inter-domain trust, cross-certification
- Knowledge representation
- Trusted time issues
- Design of cryptographic algorithms

Draft Overview: Services

- Key Registration Service
  - A service for managing public key assertions
    - Single and bulk key registration
    - Revocation, recovery, re-issuance
- Key Information Service
  - A service for obtaining information about public key assertions
    - KeyInfo Retrieval - Tier 0 <ds: RetrievalMethod> processing)
    - KeyInfo Resolution (Tier 1 - Locate processing)
    - KeyInfo Verification (Tier 2 - Validate processing)

Draft Overview: Requirements - Registration Service

- Support public key registration, revocation, and re-issuance
- Support private key retrieval from server
  - Roaming applications
  - Key recovery
- Define private key POP mechanism for both signing and encryption keys
- Define mechanism for out-of-band client authentication (e.g. with key derived from shared passphrase)

Draft Overview: Requirements – Bulk Registration Service

- Support asynchronous registration
- Support registration of multiple keys in a single request
- Support query of pending request status
- Support template-mode requests with server generated keys

Draft Overview: Requirements - Information Service

- Support for public key location given a <ds:KeyInfo> element
- Support for public key validation including
  - The binding of values to the key,
  - The status of the public key.
- Support for responses with variable validity period

Draft Overview: Requirements - Server Interaction

- HTTP Binding
  - URL specifies service and policy
- Messaging
  - Web based, incl namespace and XML schema
  - XML DigSig for signed requests/responses
  - XML Encryption for private key protection
  - Consistent Request/Response formats
    - Support nonce, deferred authentication, opaque data
- Transport Bindings
  - Transport agnostic (SOAP binding must be defined)

Resolved Issues

- Trust model/policy
  - URL conveys policy
  - No service negotiation, to enable simple client
- Security options to be highlighted, but mandatory choices deferred to protocol specs
- Privacy
  - Server may use standard P3P techniques to define and communicate registration privacy policy

Resolved Issues…

- Request/Response security
  - TransactionId as nonce
  - URL returned in response context
  - XML Signature of XKMS response supported in XKMS messaging
- No dependency on WS-Security

Open Issues

- Pending status (asynchronous registration)
- Optional items
- Consistency with SAML messages versus changes from v1.1
- Trust model/policy
  - Support for multiple PKI roots
  - Requestor role passed to server?
  - Is URI fine?
- Limits to SOAP linkage (Faults/integrity)

Open Issues…

- Request/Response security
  - How to support "deferred authentication"
    - Request digest returned in response? Digest of <Query>?
- Roaming
  - Should it be mentioned in this version? If so, how is it "specified" in XKMS?
- Other open issues?

Next steps

- Validate requirements with recent XKMS activities
- Coordinate with external activities
- Review Requirements draft
- Last Call for Requirements

Next Steps: Validate with recent XKMS activities

- Review XKMS 2.0 draft
- Review Bulk Registration draft
- Examine experience with XKMS test implementations

Next Steps: External Activity Coordination

- W3C XML Protocol (including SOAP)
- W3C Signature and Encryption
- Oasis Trust Center, especially SAML
- W3C Internationalization Interest Group
- W3C Architecture board
- W3C XML Core workgroup

Next Steps: Requirements

- Review requirements
  - Do they meet your key management needs?
  - Are they aligned with other activities?
  - Are there any gaps?
  - Are they consistent with XKMS experience?
  - Are they consistent with XKMS and Bulk Registration drafts?
- Send comments to the editors and mailing list by Jan 11th
- Last Call draft completed by Jan 25, 2002

XML Key Management Requirements Info

- XML Key Management WG

  http://www.w3.org/2001/XKMS/
  - Latest Requirements draft
  - Mail list instructions
- XKMS list archive

  http://lists.w3.org/Archives/Public/www-xkms-ws/

  (temporary mail list) www-xkms-ws@w3c.org
- Editor contact

  mike.just@entrust.com, fjh@alum.mit.edu