Possible Principles and Requirements

Frederick Hirsch, Nokia
12 July 2008
Contents

• Principles
• Requirements
  – Algorithms
  – Web Environment
  – Use Environment
  – Performance
  – Security
  – Signature Functionality
  – Coordination
  – Other
• Possible Approaches Noted
• Next Steps
Principles

• Be Consistent with the Web Architecture (1)
  – http://www.w3.org/TR/webarch/
• Be XML and XML Namespace compatible (1)
• XML Signatures are 1st class objects (1)
• Design for security and mitigating attacks (1)
• Enable extensibility where necessary but simplicity and reduced optionality by default (N)
• Re-use existing standards where possible (1)
• Don’t break backward compatibility unnecessarily (N)
  – Manage versioning and interoperability
  – Clearly call out compatibility issues and get feedback
• Acknowledge processing models with different software components/layers.

(1) 1st Edition Principles (N) Additional principles
Requirements: Algorithms

• Address maintenance of required/optional algorithms
  – Define profiles or suites a la TLS?
  – Registry?
• Review, simplify, unify XML canonicalization
  – Reference processing when needed vs. signature processing
  – Inclusive, Exclusive, Minimal etc
  – Desired properties: Idempotent canonicalization, ?
• Adjust required algorithms given changes in patents
  – DSAwithSHA1 required vs. RSAwithSHA1 recommended
• New algorithm classes and algorithms
  – Randomization, RSA-PSS, RMX
  – NSA Cryptosuite B
• Key Handling
  – X509Data update (v3 trust path, OCSP)
  – “Bare” keys
Requirements: Web Environment

• XML 1.1 [http://www.w3.org/TR/xml11/](http://www.w3.org/TR/xml11/)
• XPath 2.0 [http://www.w3.org/TR/xpath20/](http://www.w3.org/TR/xpath20/)
• EXI [http://www.w3.org/XML/EXI/](http://www.w3.org/XML/EXI/)
• xml:id [http://www.w3.org/TR/xml-id/](http://www.w3.org/TR/xml-id/)
• Schema validity when inserting signature and/or encryption into XML content
• Web 2.0/Browser environment
  – Integration with scripting languages (Perl, Python, Ruby, PHP etc)
• Semantic Web/RDF/Metadata
Requirements: Use Environment

- **XADES, DSS**
  - [http://www.w3.org/TR/XAdES/](http://www.w3.org/TR/XAdES/)

- **Web Services**

- **Identity Management**

- **Enable production of composite documents**
Requirements: Performance

- Reference Processing
  - Limitations
- Transforms
  - Limitations
- Processing layers
- Streaming
  - Two-pass
  - One-pass processing/avoiding DOM
- Infoset?
Requirements: Security

- Address wrapping attacks
- Simplify/modify/profile transform processing
- SHA-1
- Mitigate denial of service and other attacks
  - Limit XSLT, Transforms, Timeouts/limits, Resource resolution (References vs. KeyInfo), Operation order
  - Relying party get Reference material as has been signed
  - SignedInfo canonicalization issues (comments)
- Other practices
  - Pre-normalize entities before signing?
- Document Best Practices/Security Considerations
Requirements: Signature Functionality

• Enable signing/verification of any Web addressable content
• Enable variety of signature applications and use cases.
  – Sign/verify part or totality of XML document
  – Enable multiple signatures over static content given varied keys, algorithms, transforms etc
  – Support counter-signatures
  – Enable protected/unprotected signature properties
  – Enable variety of packaging
  – Detached, enveloped, enveloping signatures
  – Overlapping signatures and encryptions
• Handle xml:ids without XML schema processing
• Support arbitrary trust semantics
  – Multiple keys
• Address efficiency and usability
Requirements: Coordination

- W3C XML Coordination
- W3C XML Core [http://www.w3.org/2005/02/xml-core-wg-charter.html](http://www.w3.org/2005/02/xml-core-wg-charter.html)
- W3C Web Applications WG [http://www.w3.org/2008/webapps/](http://www.w3.org/2008/webapps/)
- ETSI Electronic Signatures
  - DSS-X, SSTC, WS-FED/WS-SX, XACML, Legal XML
Requirements: Other

• Reduce ambiguities
  – RetrievalMethod
Ideas: Possible Approaches

- Extensible mandatory Core and profiles
  - Simple mandatory profile
  - Increase core compatibility with XML Signature, 2nd Edition
- Algorithm suites
- General XML Canonicalization not required except for XML Reference processing
Next steps

• Review use cases and additional possible requirements
• Review principles and requirements list
Thank you.