

What's new with XML Signature

Frederick Hirsch

4 March 2008

XML Signature

- W3C Recommendation February 2002
 - Enables representation of Signature and meta data in XML
 - Designed to enable flexible signing of XML content
 - May also sign binary and non-XML content
 - Flexible
 - Signatures over content in same XML document, or other content
 - Inclusion of signature within XML content or separate
 - Transforms of content before hashing to sign
 - Choice of KeyInfo mechanisms, choice of algorithms
 - Signature properties

Canonicalization 1.1

- XML Canonicalization 1.0
 - W3C Recommendation 15 March 2001
 - Required algorithm for XML Signature inclusive canonicalization
- Exclusive XML Canonicalization
 - W3C Recommendation July 2002
 - Support canonicalization of portions for XML document, excluding inheritance of attributes from ancestors XML elements not in the subset.
- XML Canonicalization 1.1
 - W3C Proposed Recommendation, January 2008
 - Update to enable use of additional attributes in XML namespace with different inheritance properties, including xml:id and xml:base
 - Some additional clarifications

XML Signature, 2nd Edition

1. Require support for Canonicalization 1.1 algorithm, recommend its use for inclusive canonicalization.
2. Incorporate document errata
3. Provide clarifications, but no conformance affecting changes (other than #1)

XML Signature, 2nd Edition Status

- In process to become a W3C recommendation.
- Will also undergo IETF review in order to produce update to RFC 3275.
- Working group has produced a draft intended to become a W3C Proposed Edited Recommendation

XML Security Specifications Maintenance WG

- Chartered in 2007, operating in early 2008.
 - Chair - Frederick Hirsch.
 - W3C Team - Thomas Roessler
- Producing XML Signature, 2nd Edition
- Interop tested C14N11 and XML Signature
- Held public workshop regarding future directions.
 - <http://www.w3.org/2007/xmlsec/ws/report.html>
- Provided input to W3C team for charter for possible subsequent working group.

Possible Future Work

- Requirements for XML Signature canonicalization, reference and transform processing, algorithms, performance and XML environment.
- Specifications for Canonicalization and XML Signature.
- Algorithms for XML Encryption
- Maintenance of some other XML Security specifications.