

Update: XML Signature and friends

IETF 69 Chicago

Thomas Roessler
tlr@w3.org

Canonical XML 1.1

- Sort out xml: namespace related problems in C14N 1.0
- W3C XML Core Working Group
- W3C Candidate Recommendation as of 21 June
- <http://www.w3.org/TR/xml-c14n11/>
- Interoperability meeting: 27 September, Mountain View, Calif

XML Signature Syntax and Processing, 2nd ed

- Errata tracking
- Fold in C14N 1.1
- W3C XML Security Specifications Maintenance WG
- Work mostly finished
- Expect publication as Proposed Edited Recommendation once C14N 1.1 is in PR
- <http://www.w3.org/2007/xmlsec/Drafts/xmlsig-core/>

XML Signature, 2nd ed

- DName encoding rules
 - switch reference from RFC 2535 to RFC 4514
 - clarify conformance model for augmented rules
- XPointer normative reference
 - xmldsig-core normatively references a failed 2001 Candidate Rec for XPointer, ooops...
 - rephrase current behavior in terms of actually adopted standards
 - no conformance-affecting changes
- Updated URI spec: beware of different same-document reference definitions

Decryption Transform for XML Signature

- Changes mostly analogous to C14N1.1 / xmldsig-core
- Very little use and implementation out there
 - if you use this spec, corner me during the week
- Current plan:
 - Last Call WD really soon now
 - Candidate Rec after a few weeks
 - See if anybody wakes up

What Next? Workshop!

- W3C Workshop on Next Steps for XML Signature and XML Encryption
- 25/26 September, Mountain View, Calif
- Position papers are mandatory for participation
 - 1-5 pages
 - due date: 14 August
- <http://www.w3.org/2007/xmlsec/ws/>

Expected topics, among others

- dark corners of xmldsig-core, and other experiences / lessons learned in the last 5 years
- use cases that aren't usefully addressed?
- interoperability and robustness issues
- efficiency
- Efficient XML Interchange
- XML 1.1
- ...

Expected Workshop output

- Workshop report
 - we'll aim to have it in early November
- Ideally:
 - community consensus on future directions
 - chartering directions for one or more working groups?

Summary

- Workshop
 - 25/26 September, Mountain View, Calif.
 - <http://www.w3.org/2007/xmlsec/ws>
 - Position papers due 2007-08-14
- C14N1.1
 - Candidate Rec through end of September
- xmldsig-core
 - Editor's draft at:
<http://www.w3.org/2007/xmlsec/drafts/xmldsig-core/>
 - PER and Internet-Draft depend on C14N1.1

Questions?

tlr@w3.org

I'm around through lunch-time on
Friday.