Issues with XML-Signature Syntax and Processing
and
Rectifying Approaches

Jeff Hodges, Scott Cantor

XMLdsig Workshop
Mtv View
25-Sep-2007

Not about performance, per se

- Position paper was grouped under the title of “performance”, but performance not the chief issue
- Widespread hesitancy to implement specifications (e.g. SAML) that depend on XML in general, XML Signature specifically
- Need to address reluctance by developers using non-traditional, typically dynamic, languages (e.g. “scripting”)
  - C wrappers not a complete answer

So “SimpleSign” to the rescue

- We crafted a simpler SAML “binding” that makes message & assertion signature optional, and if signed, the XML is “simply” signed as a blob.
- Greatly simplifies rudimentary SAML support in scripting (or any) languages.
- Does not address SAML use cases in which signed assertions are a requirement.

We're not the only ones to note this

- Overall, essentially dovetails with those position papers advocating for meeting requirements for “streaming” (and there's Gutmann's treatise)
- Maybe this is an XML Signature problem or maybe it's up to everybody layered on top to solve over and over:
  - Does it make sense to standardize a way, regardless of the “packaging”, to sign-a-blob-of-XML such that everyone does it the same, and the order of keying material and signed data is correct?

Referencing Models

- XML referencing models a source of frequent confusion, non-interoperability, and security issues
- Both ID and XPath models seem to need improvements and clarifying text and examples
  - semantics, location-in-document
  - exposing signed content to applications without reprocessing
  - profiling

Minor Miscellany

- Would like to see a simpler means of conveying bare RSA/DSA public keys.
  - Suggest method analagous to X509Certificate, matching PEM "key block" format of RFC 1421 supported by OpenSSL
- Text describing RetrievalMethod is misleading about whether it points to a KeyInfo or a KeyInfo child element.
  - ID-based, so must be KeyInfo, making the text in §4.4.3 incorrect if read literally