Review of XML Signature Syntax and Processing Version 1.1, W3C Working Draft 30 July 2009

1) Technical Comments

In section 2,1, paragraph [s14-16], there are two reasons given for not requiring the KeyInfo field, signer anonymity or application specific (shared secret) keys. It is specifically called out in section 3.2.2 that the key is specified by the KeyInfo or an external source. I suggest that the KeyInfo field be required and that these to reserved values (anonymous and shared secret key) be defined. Since SignatureMethod and DigestMethod are defined, a null value of the KeyInfo will result in ambiguous results in interoperability testing. If the IUT implements a shared secret key and the digest is generated with an anonymous key, the test result that the DigestMethod was incorrectly implemented will be incorrect.

In section 2.1.1, paragraph [s06-08], the discussion on optional transforms mentions that the transforms may be used to exclude portions of the document from the calculation of the digest. If these transforms are used to obfuscate wholly the document, the authentication will not be strong. As a result, I suggest that a recommended set of excluded fields, e.g., enveloped signatures, be developed and documents excluding unauthorized fields, e.g., the document's author, be labeled as not secure. While this possibility is covered in section 8.1, the application of a large number of transforms that eventually render the digest useless and could be considered a form of DOS attack.

In section 4.2, the statement is made that there are two SignatureMethod algorithms identified, one mandatory and the other optional. No reference for these definitions are given.

2) Grammar and Edit Comments

- Section 2.1, paragraph [s03]

From: Note that this example, and all examples in this specification, **are** not in canonical form.

To: Note that this example, and all examples in this specification, is not in canonical form.

- Section 2.1, paragraph [s09-10]

From: The signing of the DigestValue is what binds **a** resources content to the signer's key.

To: The signing of the DigestValue is what binds resources content to the signer's key.

- Section 3.2, paragraph 3

From: Comparison of values in reference and signature validation **are** over the numeric (e.g., integer) or decoded octet sequence of the value.

To: Comparison of values in reference and signature validation is over the numeric (e.g., integer) or decoded octet sequence of the value.

- Section 3.2.1, paragraph 2

From: The application must ensure that the CanonicalizationMethod has no dangerous side **affects**,…

To: The application must ensure that the CanonicalizationMethod has no dangerous side effects,…

- Section 4.3.3.1, paragraph 3

From: See the Reference Validation (section 3.2.1) for **a** further information on reference processing…

To: See the Reference Validation (section 3.2.1) for further information on reference processing…