Japanese positions on issues around the introduction of XAdES to OPC

2016-02-21

National Body of Japan

There are some important issues around the introduction of XAdES to OPC, which is Part 2 of ISO/IEC 29500 (OOXML). This document shows Japanese positions on these issues.

# Issue 1: Which version of W3C XML Digital Signature?

Although ISO/IEC 29500-2:2015 (OPC) uses Version 1.0 (first edition) of W3C XML digital signature, Japan believes that the new edition of OPC should allow Version 1.1 and nothing else. This is consistent with the upcoming ETSI EN 319 132-1.

# Issue 2: Which XML canonicalization algorithm?

Japan proposes that three algorithms, Canonical XML 1.0 (without comments), Canonical XML 1.1 (without comments), and Exclusive XML Canonicalization Version 1.0 (without comments) should be recommended, and that Canonical XML 1.0 (with comments), Canonical XML 1.1 (with comments), and Exclusive XML Canonicalization Version 1.0 (with comments) be allowed,

# Issue 3: Which version of XAdES should be introduced?

Japan proposes that the next revision of OPC should introduce ETSI EN 319 132-1 rather than ETSI TS 101 903. Japan believes that allowing both versions introduced complexities and no advantages.

# Issue 4: Which specification from ETSI should be referenced?

Japan proposes that ETSI EN 319 132-1 (XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures) as well as EN 319 102-1 (Procedures for Creation and Validation of AdES Digital Signatures Part 1: Creation and Validation) should be referenced.

# Issue 5: New relationship type for XAdES EN digital signatures part?

Japan considered whether OPC should provide any mechanisms for distinguishing ETSI EN 319 132-1 digital signatures and ETSI TS 101 903 digital signatures, which are already used by existing OOXML documents.  In particular, Japan considered whether a relationship type be introduced for ETSI EN 319 132-1. But Japan believes that Implementations should be able to distinguish ETSI TS 101 903 and ETSI EN 319 132-1.

# Issue 6: **SignatureTime** of OPC and **SigningTime** of XAdES

ISO/IEC 29500-2:2015 (OPC) has **SignatureTime**. However, it can be easily updated by malicious users. **SigningTime** of XAdES is also unreliable. Japan proposes that (1) neither **SignatureTime** nor **SigningTime** shall be used for validation, (2) **SignatureTime** or **SigningTime** can be used for display purposes when there is no time stamp, and that (3) users should be warned when **SignatureTime** or **SigningTime** is used for display purposes.

# Issue 7: Is DataObjectFormat/MimeType required for OPC?

It is not clear to us whether DataObjectFormat/MimeType is required for Manifest elements.