[Draft] Minutes of the Teleconference of

ISO/IEC JTC 1/SC 34/WG4, 2015-01-15

Rex Jaeschke (rex@RexJaeschke.com)

2015-01-22

1. Opening remarks

The meeting started at 21:10. The convener, Murata-san, welcomed everyone to the 64th teleconference of WG4.

2. Roll call of delegates

The following members were present during part or all of the meeting:

Name	Affiliation	Employer/Sponsor
Makoto Murata	WG4 Convener, JP	International University of Japan
Rex Jaeschke	Ecma, Project Editor	Consultant
John Haug	Ecma, US	Microsoft
Chris Rae	Ecma	Microsoft

Present were 4 people, from 2 NBs and 1 liaison.

3. Adoption of the agenda

The agenda (SC 34 N 2131) was adopted as published

4. Administration

Approval of Previous Meeting Minutes [WG4 N 0298]

The draft minutes were approved, as circulated.

Outstanding Action Items

- Rex will review and adopt all tracked changes, so WD1 is a clean base. He'll post and announce WD1, as well as point members to the previous draft, which contains the tracked changes. **Done**
- Rex will leave the DR trace-back info in the DCOR set, but make sure the front matter explains it. He'll then submit the DCOR set to Kimura-san for a 90-day ballot. [The 90-day ballot ends 2015-03-16] **Done**

Report from the WG4 Secretariat

The following NBs and liaisons have registered delegates to WG4: BR, CA, CH, CI, CN, CZ, DE, DK, Ecma, FI, FR, GB, IN, IT, JP, KR, NL, NO, OASIS, PL, US, W3C, XML Guild, and ZA. All requests for additions, deletions, and changes to the delegate list should be sent to the WG4 Secretariat (rex@RexJaeschke.com).

The WG4 email list is e-SC34-WG4@ecma-international.org. The document repository is now at http://isotc.iso.org/livelink/livelink?func=ll&objid=8912947&objaction=ndocslist.

Note: New documents are no longer being posted to the Japan-hosted website. Only the LiveLink site will be updated. Members must get themselves added to the LiveLink Global Directory through their National Body or Liaison Organization.

5. Revising Part 2 (Open Packaging Conventions)

Latest draft

WD1 of 29500-2 is now available as N 0301. No one has posted any feedback on it yet.

XAdES

Murata plans to invite XAdES experts to join the Seattle meeting by teleconference.

Here is the email thread titled, "Object elements for XAdES":

2015-01-25 Murata-san:

ISO/IEC 29500-2 distinguishes Object elements having Id="idPackageObject"and those not having it. The former is a package-specific Object element (see 12.3.5.14) while the latter is an application-defined Object element (see 12.3.5.15).

OFF-CRYPTO introduces two other values of Object/@Id. They are "idOfficeObject" and "idXAdESReferenceObject". It appears that "idOfficeObject" are used as containers of SignatureInfoV1, which we are not going to be introduced to OPC.

Thus, it remains to introduce "idXAdESReferenceObject" as XAdeES reference Object in the revision of Part 2. Am I correct?

2015-01-25 Murata-san:

Miyachi-san (an attendee of the Kyoto meeting) agrees with me. We do not have to mention <Object id="idOfficeObject"> but we should allow <Object id="idXAdESReferenceObject"> as a XAdES reference Object element.

2015-01-25 John Haug:

So, recommend making the same explicit allowance in OPC as in MS-OFFCRYPTO for placing a Reference element that specifies a digest of a SignedProperties element inside a Manifest element inside an Object element which has id=”idXAdESReferenceObject”, as specified at the very end of 2.5.2.6 in MS-OFFCRYPTO?

Since at least MS Office and possibly others currently do this when using XAdES, it seems a good idea for compatibility.

We discussed Murata-san’s e-mail “Object elements for XAdES” which suggested including text about the Object element with id=”idXAdESReferenceObject” as described in MS-OFFCRYPTO, subclause 2.5.2.6. (It was easily agreed that about the Object element with id=”idOfficeObject”is not needed). This provides a second (less preferable) way to store a Reference element that specifies the digest of a SignedProperties element. John noted that note #33 in Appendix A appears to indicate that this is documented only for completeness due to unpatched Microsoft Office 2007 systems. John will check with a security contact at Microsoft to verify this and may recommend that this can be safely omitted from Part 2.

Long-Term Digital Signature

Here is the email thread titled, "XAdES elements in OFF-CRYPTO of Microsoft":

2015-01-15 Murata-san:

We have already agreed not to introduce SignatureInfoV1. The rest of XAdES elements in OFF-CRYPTO is described in the following subsection. We probably have to tweak this subsection since we would like to allow all conformance levels of XAdES.

2.5.2.6 XAdES Elements

XML Advanced Electronic Signatures [XAdES] extensions to xmldsig signatures MAY<32> be present in either binary or ECMA-376 documents [ECMA-376] when using xmldsig signatures. XAdES-EPES through XAdES-X-L extensions are specified within a signature. Unless otherwise specified, any optional elements as specified in [XAdES] are ignored. The Object element containing the information as specified in [XAdES] has a number of optional elements, and many of the elements have more than one method specified. A document compliant with this file format uses the following options:

- The SignedSignatureProperties element MUST contain a SigningCertificate property as specified in [XAdES] section 7.2.2.
- A SigningTime element MUST be present as specified in [XAdES] section 7.2.1.
- A SignaturePolicyIdentifier element MUST be present as specified in [XAdES] section 7.2.3.
- If the information as specified in [XAdES] contains a time stamp as specified by the requirements for XAdES-T, the time stamp information MUST be specified as an EncapsulatedTimeStamp element containing DER encoded ASN.1. data.
- If the information as specified in [XAdES] contains references to validation data, the certificates used in the certificate chain, except for the signing certificate (1), MUST be contained within the CompleteCertificateRefs element as specified in [XAdES] section 7.4.1. In addition, for the signature to be considered a well-formed XAdES-C signature, a CompleteRevocationRefs element MUST be present, as specified in [XAdES] section 7.4.2.
- If the information as specified in [XAdES] contains time stamps on references to validation data, the SigAndRefsTimestamp element as specified in [XAdES] section 7.5.1 and [XAdES] section 7.5.1.1

MUST be used. The SigAndRefsTimestamp element MUST specify the time stamp information as an EncapsulatedTimeStamp element containing DER encoded ASN.1. data.

- If the information as specified in [XAdES] contains properties for data validation values, the CertificateValues and RevocationValues elements MUST be constructed as specified in [XAdES] section 7.6.1 and [XAdES] section 7.6.2. Except for the signing certificate (1), all certificates used in the validation chain MUST be entered into the CertificateValues element. There MUST be a Reference element specifying the digest of the SignedProperties element, as specified in [XAdES], section 6.2.1. A Reference element is placed in one of two parent elements, as specified in [XMLDSig]:
- The SignedInfo element of the top-level Signature XML.
- A Manifest element contained within an Object element. A document compliant with this file format SHOULD<33> place the Reference element specifying the digest of the SignedProperties element within the SignedInfo element. If the Reference element is instead placed in a Manifest element, the containing Object element MUST have an id attribute set to "idXAdESReferenceObject".

2015-01-15 Murata-san:

Miyachi-san believes that the quoted paragraphs allow five leveles of XAdES (EPES, T, C, X, X-L) and mandate C and X. He thinks that they should be optional.
Furthermore, as agreed in Kyoto, we should allow EPES/BES, T, X-L, and A.

2015-01-15 John Haug:

Do you know what the basis is for thinking –C and –X are mandatory? I assume he's looking at the 5th and 6th bullets under 2.5.2.6 in MS-OFFCRYPTO. I read these as conditionals – if you use validation data, then you must do it this way.

(1) Are there alternate ways to specify references to validation data other than as specified in XAdES 7.4 (and 4.4/4.4.3, which say signatures with validation data are –T and –C.)? If so, the 5th bullet is just requiring one way where a choice exists. If not and XAdES-C is the only way, the 5th bullet seems to just restate what XAdES-C requires. I don't see other ways and I might read that bullet as precluding use of XAdES-T, which I'm sure is the wrong interpretation.

(2) Are there alternate ways to specify time stamps on references to validation data? It seems so: SigAndRefsTimeStamp and RefsOnlyTimeStamp. In this case, MS-OFFCRYPTO appears to be simply requiring the use of one method where an option exists for implementers. The mandate here appears to be use of XAdES-X type 1 and not XAdES type 2 if you use XAdES-X.

>Furthemore, as agreed in Kyoto, we should allow EPES/BES, T, X-L, and A.

Yes. As reference for today's call, here are my relevant notes from our discussion and decisions at the Kyoto meeting.

What to specify

- Anything re: grace period? NO - for implementers, not for file format.
- Which parts/relationships must/must not be signed? Part 2 does not currently say anything to this effect. NO - for implementers, based on user scenario.
- Additional restrictions a la ODF? (for interoperability) NEEDS RESEARCH
- Other restrictions? (disallow less useful levels?)
  - e.g., BES/EPES plus ISO profile
  - Don't mandate/prohibit, give guidance - normative SHOULD or informative NOTE
- Does OPC require signing a relationship that targets a part that is signed? Don't think so (relationships can be signed, but not required). Should this be mandated? NO.
- RenewedDigests - mention this?
  - Can reference new ETSI std once published (expected within the next year)
  - Should only contain this addition since 1.4.2 (minor bug fixes from 1.4.1)
  - Double-check for any changes, including namespace (all existing features should be in old namespaces, only new features in new ones)

2015-01-15 John Haug:

I nearly forgot, I compared the XAdES-specific requirements in MS-OFFCRYPTO and those we looked at last year in ODF (ODF 1.2 Part 3, section 5.3). Here is what I found.

SignedSignatureProperties > SigningCertificate -- in BOTH

SigningTime – "should" in ODF, "MUST" in OFFCRYPTO

EncapsulatedTimeStamp (DER-encoded ASN.1) -- in BOTH

CompleteCertificateRefs/CompleteRevocationRefs -- in OFFCRYPTO only

SigAndRefsTimestamp for refs to validation data -- in BOTH

CertificateValues/RevocationValues -- in OFFCRYPTO only

Reference element for digest of SignedProperties

-- ODF: child of SignedInfo

-- OFFCRYPTO: child of SignedInfo (preferred) or Object > Manifest (with id=”idXAdESReferenceObject”)

They’re pretty similar, MS-OFFCRYPTO has slightly tighter requirements. So, no notable differences between the two that we would need to research. The XAdES requirements we’ll want to add to Part 2 look fairly well known to the industry.

We discussed Murata-san’s e-mail “XAdES elements in OFF-CRYPTO of Microsoft” which noted that MS-OFFCRYPTO supports XAdES-EPES through XAdES-X-L and seems to mandate XAdES-C and -X. John thinks that –X is not mandatory, but the relevant text in MS-OFFCRYPTO (6th bullet in 2.5.2.6) appears to require use of type 1 of XAdES-X and not type 2. See Annex B.1 in ETSI XAdES 1.3.2 (current normative reference in Part 2) for more on type 1 vs. type 2. John is uncertain how to interpret the 5th bullet in 2.5.2.6, which discusses support for validation data (-T and -C). It appears to either add nothing to what the XAdES standard says or precludes use of -T. John will check with a security contact at Microsoft, and Murata will speak with Japanese XAdES experts.

6. Extensions: 30114-2 Character Repertoire Checking

30114-1 Guidelines for extending OOXML

One approach for extending OOXML is to introduce a new OPC part that is not explicitly introduced in OOXML. Old applications do not use this OPC part, while new applications use it. But what happens when old applications touch the other OPC parts without changing the new OPC part? It appears that new applications check if the new OPC part is consistent with the other OPC parts probably by comparing the timestamp of the new OPC part and those of the other OPC parts. Such consistency checking is not mentioned anywhere in ISO/IEC 29500.

7. Defect Reports

The public, online DR log is now at https://onedrive.live.com/?cid=c8ba0861dc5e4adc&sc=documents&sa=501765342&id=C8BA0861DC5E4ADC%21105. Access individual DRs via the hyperlinks contained within the spreadsheet's left-most column.

DR 14-0008 "SML: Specifying a Range in a Separate Workbook"

After some discussion, we declined to add the suggested reference. Deferred until the Seattle F2F meeting, at which time we expect to close this without change.

DR 14-0010 "SML: Attribute textRotation"

The submitter raises an important issue; Chris is working on a proposal.

8. Other Business

Thanking Host

We thanked Microsoft and John Haug for hosting the teleconference.

9. Future meetings

Face-to-Face Meetings:

- 2015-02-24/26, Seattle, Washington, US (on 2015-02-23, WG8 then 26300 BRM)
- 2015-06-15/17, BSI, London, UK (possibly with other WGs)
- 2015-09-21/25, Beijing, CN (with other WGs, and Opening/Closing Plenaries)

Teleconferences:

- None

10.Adjournment

Adjourned by unanimous consent at 21:25.