Minutes of F2F-Meeting on 2008/10/03

1 Organizational Aspects

1.1 Location

Ditton Mannor, London, UK

1.2 Time

Start: 9:00 GMT - 10:00 CET
End: 6:00 GMT - 17:00 CET

1.3 Attendees

- Orthacker, Clemens (CO)
- Straat, Marc (partly) (MS)
- Farhi, Ezer (phone) (EF)
- Lanz, Konrad (phone) (KL)
- Burgos, Oscar (OB)
- Cruellas, Marta (MC)
- Cruellas, Juan (JC)
- Huehnlein, Detlef (DH)
- Drees, Stefan (phone) (SD)
- Kuehne, Andreas (AK)
- Ernst Jan van Nigtevecht (partly) (EN)

1.4 Organizational parts of the agenda

1.4.1 Welcome by chair (Juan Carlos Cruellas)

1.4.2 Confirmation of minutes takers

DH will compile minutes based on input from the chat (see http://www.oasis-open.org/committees/download.php/29561/Raw-material-for-F2F-minutes-taken-from-chat-at-17-28.txt for raw chat protocol).

1.4.3 Approval of the agenda

The agenda, which is mirrored by the minutes, has been approved.

2 Roadmap and Work Plan

JC states that the F2F-meeting shall be used in particular to discuss

- hot topics for the different profiles
- issues related to the Work style in general
- Concerning the work style there are different proposals how the work of the TC could become more efficient/effective
    - PvdE: Concentrate on certain profiles during telcos
    - AK: Probably more F2F meeting
    - CO/KL: Deadlines for certain actions/document versions
    - EF: Editor and (2) distinguished reviewers
    - DH: Combination of different approaches (in particular deadlines and more F2F)

3 Discussion on new profiles

3.1 Visible signature profile

The discussion is based on

- the WD at http://www.oasis-open.org/apps/org/workgroup/dss-x/download.php/28679/oasis-dssx-1.0-profiles-visualsig-wd2.doc
- the Wiki at http://wiki.oasis-open.org/dss-x/Visible_signature_profile (which has been extended during discussion)

EF states that

- he is waiting for comments and feedback from the committee
- VisSigProf will have Sign and Verify; it should be discussed whether there should be a standardized visualization of verification results

MS raises the question, whether the visualization of verification results would be a standard (PDF@ISO) or product (e.g. Adobe Reader) issue?

AK replies that this does not seem to be a product issue and the VisSigProf should cover such issues.

CO states that there is an Austrian visualization of an "official signature", which should be considered (see http://www.oasis-open.org/committees/download.php/29553/Official_Signature_in_Austria_S%5B1%5D.pdf-pruefbericht-20081003T104026.747Z.pdf , http://www.oasis-open.org/committees/download.php/29552/Official_Signature_in_Austria_S%5B1%5D.pdf-pruefbericht-20081003T104026.747Z.pdf).

MS states that there is a similar discussion in a current ETSI-Project, which aims at standardizing issues related to using {X/C}AdES with/in PDF.

KL mentions that it is not really clear yet, what a "visible signature" actually is? Basic definitions / requirements should be discussed and settled.

PE asks how the ETSI-project and the VisSigProf are related?

KL asks what the questions of this project are and who tries to answer them?

JC/MS state that the two projects are complementary.

MS clarifies that the ETSI-project is focusing on formats, DSS-X not.

MS explains that this STF activity will be articulated into the following phases:

(see Terms of Reference at http://www.oasis-open.org/committees/download.php/29555/CL08_2635%20%284%29.pdf)

- **Phase 1**
  - Specify an ETSI profile for a basic variant of advanced electronic signatures in PDF using the existing features of PDF signatures.
  - Detail requirements for full features to be specified in the next phase.
- **Phase 2**
  - Specify profiles for advanced electronic signatures in PDF incorporating the features of CAdES and XAdES
  - Identify any changes necessary to TS 101 733 and / or TS 101 903 and produce change request documents for detailing the specific changes recommended.
  - Specify enhancements required to ISO 32000 to incorporate these features in ISO 32000-2.
  - Detail requirements of PDF signature support for the next phase.
- **Phase 3**

- Specify enhancement to ISO 32000 for PDF conforming reader support of advanced electronic signatures including visible signatures and interfaces to signature support functions.
- Continue liaison on ISO 32000 support for advanced electronic signatures.

KL suggests that there should be a section in the Wiki for "Related work"

EF suggests that it should be discussed, whether the visualization of a verification result should be within the scope of the VisSigProf.

DH states that this is similar to requesting the addition of a "verification report page" to a pdf.

KL suggests that we should gather the requirements first and then discuss, what should be within the scope and what not.

KL asks whether there are references to such implementations ... ?

DH will try to provide links / further information.

KL states that we should define the abstract content of such a visual verification report - but rather not the way how to render this information.

MS asks EF what should be in the scope of DSS?

JC suggests to put an ACTION for ALL to put ideas and requirements into Wiki.

JC states that the committee agreed that the visualization of a verification result is an OPTIONAL feature.

CO states that the focus should not be on the HOW something is visulized, but WHAT. Furthermore

he gives examples of what elements could be comprised: signer-name, ..., logo-image .

EF states that it is also important to discuss issues in the intersection of different profiles (e.g. visualization of advanced el. sig ...).

JC suggests to put ACTION on EF (and ALL) by 2008/10/10 to collect and structure initial ideas in the Wiki.

EF adds that it is not clear what happens, if multiple profiles are combined?

KL states that in the charter there is point, which deals with the interrelationship of multiple profiles.

JC mentions that this issue is also in the agenda. We should reserve some time in the afternoon to discuss this topic and develop a general strategy to solve this issue.

CO provides an example of a "visual verification report" including an official logo and other important info:

http://www.oasis-open.org/apps/org/workgroup/dss-x/download.php/25700/proposal-visible-signatures-v1.1.pdf

JC states that PE and KL will serve as distinguished reviewer of the VisSigProf.

3.2 Individual verification reports profile

DH suggests to start with the verification report (5.2.1), then archival (5.2.2)

3.2.1 Discussion of topics concerning verification report

DH sketches the agenda:

1) main topics/general directions of profile
2) details

3.2.1.1 Main topics

There are multiple approaches

1) Profile is not defined in a separate schema, but existing definitions of the Core valid/invalid details are used.
2) Define structure of individual signature report details as optional elements in schema. This is the proposal in the draft
3) Approach based on core, but a separate schema that adds the extra options. Drawback is that the schema becomes more complex complex.

DH wants the TC to agree on the direction to take, based on evaluation of pros and cons of each option.

A separate XML schema is better when an accountant needs to determine the legal compliance of a solution. A separate schema makes this possible. Option (1) does not support this well.

Option (3) results in a much more complex schema. Do we prefer to stay close to the core, or to have a simple schema?

CO says that in general sticking to the core is preferable, but not if it becomes too complex.

JC points to the examples in http://wiki.oasis-open.org/dss-x/MultiSignatureVerificationReportsProfile below "25-07-2008. [BR] [BR]"

JC states that the ProcessingDetails element has three elements that can be combined:

- `ValidDetail`,
- `IndeterminateDetail`,
- `InvalidDetail`

KL states that they are based on the `DetailType`, which is defined as follows:

```
<xs:complexType name="DetailType">
  <xs:sequence>
    <xs:element name="Code" type="xs:anyURI" minOccurs="0"/>
    <xs:element name="Message" type="dss:InternationalStringType"
                minOccurs="0"/>
    <xs:any namespace="##other" processContents="lax" minOccurs="0"
            maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="Type" type="xs:anyURI" use="required"/>
</xs:element>
```

The above mentioned elements (`ValidDetail, IndeterminedDetail, InvalidDetail`) reference the parts they refer to using URIs. So the URIs would need to be constrained.

JC explains that the profile defines fixed values for the Type attribute, and allowed values.

DH states that the semantics of the approaches is the same, the difference is the organization of the schema (more/less core re-use, more/less redundancy). In particular the same information is contained in the verification report in each approach.

JC states that he has no strong opinion on the two approaches, goal was to explore the alternatives.

DH states that current draft defines two levels of verification report, one based on DSS Core and the second for individual verification structure.

JC mentions that at Xades plug-test it was found that several vendors are already providing some types of verification reports. Vendors agreed on a need to standardize these reports. So a report structure would be useful in other contexts than DSS.

KL the plugtest did not constrain the format of the report, some vendors used DSS-derived syntax.

KL suggests that we could contact the vendors and ask them what their reporting structures are.

MC asks whether it is easier to implement a Core-compliant approach? Is one more efficient than the other?

JC mentions that the option that is closest to the core is less readable.

KL adds "Readability, what about XSLT ..."

DH asks how tools would use the XML reports? Do they display them using a stylesheet?

DH adds that XSLT stylesheets would likely be more complex for the core-compliant approach, as the main navigation would need to be based on attributes rather than elements.

JC asks whether we are ready for a decision?

KL points to the relevant part of the Core: http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.html#_Toc159076085

Pim in particular states that the `DetailType` is extensible.

CO proposes that JC and DH make a proposal to the TC, the other participants have not looked in details at the options.

KL asks, whether the proposal requires any changes to the core?

DH clarifies that, there is no conflict with core, but the profile does not reuse some DSS Core structures.

JC states that it is not a good message if an extensibility feature that is in the DSS Core is not used.

JC proposes that he and DH will document a proposal that makes a choice and provides the rationale for the choice.

JC suggests that the document will also contain some example XML documents

KL suggests that the profile could also contain this explanation of the choice so implementers of DSS understand the options and trade-offs.

JC agreed to add this information as optional non-normative part of the spec.

JC volunteers to contribute to the rationale document. CO and KL volunteer to review this document.

PE asks if there are provisions for PDF in the verification report?

KL states that he will review visible signatutres

DH explains that for XML there is XPaths, for PDF there is fieldName, for binary documents offset. So multiple document types are supported.

EF mentions that he thinks that Andreas wanted to review the Verification Report Profile.

DH states that PDF has "`Reason`", XAdES has "`CommitmentType`" and ask whether both should be supported?

JC recalls that at a workshop of PDF and XAdES someone mentioned that there is overlap between the two.

AK clarifies that he volunteers to review the verification report profile.

DH asks whether we should wait for the ETSI group to resolve these issues?

JC replies "yes, that is their charter".

PE stresses that some user communities want this today.

EF states that he agrees with Pim. And the terminology used by these users is "`Reason`" and not "`CommitmentType`".

DH proposes that we support multiple options for the moment, and revise (if needed) if the ETSI/PDF work group comes with a better proposal later.

DH proposes to postpone the discussion of the minor issues until a decision on the main strategy is made.

3.2.2 Discussion of topics concerning archiving profile

Discussion is based on document at http://www.oasis-open.org/apps/org/workgroup/dss-x/download.php/29543/2008-10-03-An%20Archiving%20Profile%20for%20OASIS%20DSS.pdf

DH starts presentation

DH asks whether the TC supports this use case?

MC replies "yes, CatCert supports this, strong interest from customers".

PE states that there is also interest in the Netherlands.

CO asks whether e-invoicing also needs archival?

DH states that in Germany, archival is needed but not the cryptographic conservation.

DH states that the main interest in this kind of archiving is in government projects.

PE states that there are some additional requirements, like document transformation (e.g. from a usage-format (e.g. .doc) to .pdf/a)

EF asks whether this is not beyond our scope? Like document management functions?

DH replies that document management is out of scope. The proposal only considers the final (archival) stage.

SD states "ahem, document management no, archival stage yes, this sounds like a floating requirement"

MS asks what kind of archival formats (PDF/A?) are supported?

EF underlines that he wanted to make sure that doc mgmt is out of scope

DH explains that in Germany the recommendation is to first produce durable format (e.g. PDF/A), then wrap this in XML with metadata.

JC points to the XML-schema for the proposed LTAP-protocol at http://tools.ietf.org/html/draft-ietf-ltans-ltap-06#page-55

DH explains that the proposed protocol has a similar purpose, but the XML interface in LTA seems to be underdeveloped. Hence the proposal here would be to base such an interface on DSS base types. The "storage interface" from middle layer to Long Term Storage could be LTA. The Middle layer serves as a kind of proxy.

JC stresses that we need a strong case to justify such a development or liaise/collaborate with LTA people.

AK mentions that this looks like this is an orchestration of multiple services, including DSS.

EF asks, whether the interface to DSS is similar to that of the AdES profile?

EF suggests to re-use or update this profile instead of creating a new archival profile.

JC suggests that we should look more at requirements and study LTA more, before deciding whether to develop this profile or not.

AK suggests to call this development rather a "usage recommendation" than a profile.

The TC agrees that a rationale / requirements document should be created in order to be able to agree on further steps.

Ernst Jan van Nigtevecht joins the meeting

3.3 Encryption profile

The following discussion is based on http://wiki.oasis-open.org/dss-x/EncryptionProfile

CO shows some encryption samples

The TC agrees upon the fact that there should be an encryption-only variant such that encryption can be used without signing. There are no objections against the standalone-encryption.

PE recalls that the conformance section gives the possibility to defined encryption as minimum requirement.

DH asks how such a statement would comply with the conformance of the core?

CO explains `EncryptRequest` ... `EncryptResponse`

KL points at http://wiki.oasis-open.org/dss-x/EncryptionProfile#line-250

AK states that `EncryptedDocuments` is critical as it maybe empty, in contrast to `DocumentBaseType`.

JC explains to Konrad/Ezer/Stefan that it is a split example with text interleaved.

KL points to http://wiki.oasis-open.org/dss-x/EncryptionProfile#line-126

CO introduced a change to next version of the core / errata regarding the KeySelector

The TC agrees to adding the `KeySelector` as a top level element.

JC asks Stefan to put an action to add the `KeySelectorType` issue to the errata list.

The TC agreed upon the fact that CMS encryption should be allowed.

JC recalls that profiles have a common way to define urns for profile specific use.

CO asks whether the version should be added to the profile schemas?

JC asks to look for "Same as above, with `xenc:CipherReference`."...below

CO explains that there is one key selector element but maybe there are multiple encryption content to have several encryption types

CO asks whether this multiplicity has a real usecase?

SD creates an Action#0085.CREATE Add the `KeySelectorType` issue to the errata list

JC explains "The second element (`InsertEncryptedData`), selects a document (`#opaque-data`) to be encrypted and the resulting `xenc:EncryptedData` to be inserted at the specified destination in `EncryptedDocumen#structured`." ... "the one that contains `EncrytpANdReplaceData`, and `InsertEncryptedData`"

JC suggests that there are some explanantions required as the path expressions are absolute, but refer to the input document

PE asks, whether there is some sort of pipelining available: encrypt with key A, than encrypt with key B?

CO clarifies that it is only possible to 'chain' encryption and signing.

CO states that in case of chaining of encryption and signing the appearance of encryption elements and core signing elements decide.

DH states that it's good practice to sign first and encrypt in second stage.

JC suggests to take into account what's defined in DecryptionTransform

KL points to http://www.w3.org/TR/xmlenc-decrypt and http://www.w3.org/TR/xmlenc-decrypt#sec-introduction

CA asks whether there are problems when using chaining of CMS encryption and signing?

CO answers a question concerning the use of attachments and states that it's perfectly correct to refer to attachment data.

KL adds that attachment references are treated as being implicitly part of the request. [OK?]-5

CO states that `SignedReferences` cannot be interleaved with other (encryption) elements.

CO suggests to make `SignedReference` a named top level element.

DH and JC volunteer as reviewers for the encryption profile.

3.4 ebXML profile

PE states that there were no comments on ebXML profile.

The TC agreed on motion for progressing the ebXML profile as committee spec.

KL abstained, all others agreed.

There is an Action#0086.CREATE Open ballot for progressing the ebXML profile as committee spec

3.5 European Signature Law profile

EF states that one question is 'can DSS align with EU directive?'

EF adds that there are too few real use cases to define such an EU profile

MC suggests to write some recommendations to build a EU directive compliant server

AK remarks that the DSS TC is at the interface level, we can't solve the EU compliance problems in DSS

DH suggests to check whether legal measures (as sketched in Section 2 of http://www.ecsec.de/pub/2004_PKI.pdf) can be used to solve the problem.

4 Committee work-plan

JC states that we should concentrate on one or two profiles for the near future.

DH makes clear that he would prefer to accomplish encryption and verification asap.

JC suggests to concentrate for two or three meetings on one profile.

KL suggests that the editors and reviewers may meet in every second week where there is no conf call.

JC suggests to start with two TC meetings per profile.

EF states that there is no personal restriction for the work on visual profile

KL points to http://www.oasis-open.org/apps/org/workgroup/dss-x/manage/add_event.php?day=1223287200

DH suggests to start with encryption profile.

The TC agreed on the schedule: encryption, verification report, visual signatures

There will be an ACTION on the chairs to contact the editors to build deadlines for the different profiles

JC states that he will circulate the work plan before the next meeting

JC states that we will discuss the work plan on the Oct, 13.

JC suggested a discussion to have f2f meetings with a 3 month frequency.

SD created an Action#0087.CREATE Contact the editors to build deadlines for the different profiles.

5 Any other business

5.1 Reply to ODF-question

JC pointed to http://www.oasis-open.org/apps/org/workgroup/dss-x/email/archives/200809/msg00027.html and explained that some of the question regarding ODF are forwarded to the ESI group, one issue (#4) left for the DSS-X TC.

There is an action on all to review the reply to ODF until October 8th, 2008

SD created an Actio#0088.CREATE Review the reply to ODF

5.2 BIOSIG2009-Workshop

DH stated that there will be a workshop on (biometrics and) electronic signatures in June or September 2009 (in Darmstadt, Germany). It would be highly appreciated, if TC-members would like to

- join the program committee (suggest topics, help to review submissions etc.)
- contribute papers / talks
- etc.

As in the last years there will be proceedings for the workshop, which are indexed by DBLP for example (see http://www.informatik.uni-trier.de/~ley/db/conf/biosig/biosig2007.html and http://gi-ev.de/fachbereiche/sicherheit/fg/biosig/index.htm).

The draft of the CfP is at http://www.oasis-open.org/apps/org/workgroup/dss-x/download.php/29566/BIOSIG2009-CfP-eng_081004.doc .