CEN/ISSS WS/BIIGL10

Signature

GUIDELINE

Business Domain: All

Business Process: All

Document Identification: CEN/ISSS WS/Guideline 10

Version: 1.0

Release: 2009-11-05

Date of approval: 2009-11-05

TABLE OF CONTENTS

1   Introduction

BII, Business Interoperability and Interchange was established to enable interoperability of procurement data.

The focus of BII is to define the specific use of electronic procurement documents domestically and between the European countries. The definition covers semantic interoperability within and between all business sectors, public and private.

This guideline is one of a series of documents describing the purpose and use of the business transactions that comprise BII.

All cardinalities shown in this document represent elements and associations at BII library level; see 'BII Information Model Architecture' for further information.

1.1   Purpose

The purpose of this guideline is to specify the use of signature.

1.2   Summary

- Signature may be used at document level in all BII documents

2   Signature classes and elements

2.1   Signature

Signature information is described in the Signature class. Associated information is described in:

1. Signatory Party
2. Digital Signature Attachment
3. Original Document Reference

3 Description

Signature describes the digital signature(s) applied to a document. A Signature should not be mistaken for or confused with a signature used for securing the transport, or with a XMLDSIG signature.

A Signature is used in a document when the business processing of the document requires it. A digital signature on a electronic document does not warrant its integrity any more than a hand written signature does on a paper document.

3.1 Specifying who signed

The signatory is specified by the use of an ID on the Signature and a description (such as the organisation name) of the Party who signed the document.

Such a Signature may be used in the recipient's business workflow. For example. a Supplier may require specific Signatures to be included in an Order for it to be processed; different Signatures may be required for specific values or Item groups.

The recipient must trust that the sender's system secures that the Signature originates from the correct person.

3.1.1 signatory example

```xml
<cac:Signature >
        <cbc:ID>Peter.Hansen@oioubl.dk</cbc:ID>
        <cac:SignatoryParty>
                <cac:PartyName>
                        <cbc:Name>OIO fælleskøb A/S</cbc:Name>
                </cac:PartyName>
                <cac:Person>
                        <cbc:FirstName>Peter</cbc:></FirstName>
                        <cbc:FamilyName>Hansen</cbc:FamilyName>
                        <cbc:Title>Indkøbschef</cbc:Title>
                </cac:Person>
        </cac:SignatoryParty>
</cac:Signature>
```

3.2 Specifying the validator

The Signature may be validated by use of the ValidatorID, the ValidationDate and ValidationTime.

When these are specified, it should be possible to locate the original Signature at the Validator; in the example below, DoorTrade.net.

3.2.1 Validator example

```xml
<cac:Signature >
    <cbc:ID>Peter.Hansen@oioubl.dk</cbc:ID>
    <cbc:ValidationDate>2006-09-13</cbc:ValidationDate>
    <cbc:ValidationTime>14:20:02</cbc:ValidationTime>
    <cbc:ValidatorID>DoorTrade.net/signout</cbc:ValidatorID>
    <cac:SignatoryParty>
        <cac:PartyName>
            <cbc:Name>OIO fælleskøb A/S</cbc:Name>
        </cac:PartyName>
        <cac:Person>
            <cbc:FirstName>Peter</cbc:></FirstName>
            <cbc:FamilyName>Hansen</cbc:FamilyName>
            <cbc:Title>Indkøbschef</cbc:Title>
        </cac:Person>
```

```
    </cac:SignatoryParty>
</cac:Signature>
```

3.3   Specifying the Signature

In NES, it is possible to reference or to attach the Signature that is used in the document. If so, a specification of the document that the signatory saw when he signed the document should be included. This document is rarely the same as the forwarded document; usually, it is an html or a graphical representation (e.g. JPG or TIFF) of the xml-document itself.

In the example below, the XMLDSIG signature is attached as a MIME attachment (Base64 encoded xml), while the original document is linked via a URI (see http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview.html).

CanonicalizationMethod and SignatureMethod can be used to check the signatory against the original document.

If the transformation method is valid and trusted by all parties, the original document may instead be represented by a list of paths (Xpath) from the document that was the source of the one seen by the signatory.

3.3.1   Signature example

```
<cac:Signature>
    <cbc:ID schemeID="CVR">16356709</cbc:ID>
    <cbc:ValidationDate>2006-09-13</cbc:ValidationDate>
    <cbc:ValidationTime>15:20:02</cbc:ValidationTime>
    <cbc:ValidatorID>DoorTrade.net/signout</cbc:ValidatorID>
    <cbc:CanonicalizationMethod>http://www.w3.org/TR/2001/REC-xml-c14n-20010315 </cbc:CanonicalizationMethod>
    <cbc:SignatureMethod>http://www.w3.org/2000/09/xmldsig#dsa-sha1</cbc:SignatureMethod>
    cac:SignatoryParty>
        <cac:PartyIdentification>
            <cbc:ID schemeID="CVR">16356709</cbc:ID>
        </cac:PartyIdentification>
        <cac:PartyName>
            <cbc:Name>Tavleleverandøren</cbc:Name>
        </cac:PartyName>
        <cac:PartyLegalEntity>
            <cbc:RegistrationName>Tavleleverandøren</cbc:RegistrationName>
                <cbc:CompanyID schemeID="CVR">16356706</cbc:CompanyID>
        </cac:PartyLegalEntity>
        <cac:Contact>
            <cbc:Name>Hugo Jensen</cbc:Name>
            <cbc:Telephone>15812337</cbc:Telephone>
            <cbc:ElectronicMail>Hugo@tavl.dk</cbc:ElectronicMail>
        </cac:Contact>
    </cac:SignatoryParty>
    <cac:DigitalSignatureAttachment>
        cbc:EmbeddedDocumentBinaryObject mimeCode="text/xml">
```

CA8U2lnbmF0dXJlIIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaGRzaWcjIj4NCiAgICA8U2lnbmVk
SW5mbz4NCiAgICAgIDIDxDYW5vbmljYWxpemF0aW9uTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmc
vVFIvMjAwMS9SRUMteG1sLWMxNG4tMjAwMAMWRTKAJzUMDTIUTiHILCO8U+IDSQEoOgLIICVAIgAICA8U2lnbmF0d
XJlTWV0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3JzYS1zaGExIiAvPg0K
ICAgICAgPFJlZmVyZW5jZSBVUkk9IiI+DQogICAgICAgIDxUcmFuc2Zvcm1zPg0KICAgICAgICAgIDxUcmFuc2Zvcm
0gQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjZW52ZWxvcGVkLXNpZ25hdHVy
ZSIgLz4NCiAgICAgICAgPC9UcmFuc2Zvcm1zPg0KICAgICAgICA8RGlnZXN0TWV0aG9kIEFsZ29yaXRobT0iaHR0cD
MjAwMC8wOS94bWxkc2lnI3NoYTEiIC8+DQogICAgICAgIDxEaWdlc3RWYWx1ZT5KL0dvvFNkekpoOXJfbFVppEp
wMDJpUzdnN1E9PC9EaWdlc3RWYWx1ZT4NCiAgICAgIDwvUmVmZXJlbmNlPg0KICAgIDwvU2lnbmVkSW5mbz4gl
A0KI1NpZ25hdHVyZZT4

```
        =</cbc:EmbeddedDocumentBinaryObject>
     </cac:DigitalSignatureAttachment>
    <cac:OriginalDocumentReference>
        <cbc:ID>A00095678</cbc:ID>
        <cbc:CopyIndicator>false</cbc:CopyIndicator>
        <cac:Attachment>
            <cac:ExternalReference>
            <cbc:URI>archieve.DoorTrade.net/signature/16356709/6E09886B-DC6E-43EE-82D1-7CCAC7F4E3B1.jpg</cbc:URI>

            <cbc:DocumentHash>UxNQUFPLMnHHJU1tQ1p0dU1GUXhEUzOIUbhhGHJ
            </cbc:DocumentHash>
            <cbc:ExpiryDate>2011-08-13</cbc:ExpiryDate>
        </cac:ExternalReference>
    </cac:OriginalDocumentReference>
</cac:Signature>
```