



Guideline
Signature

Version 1.0



NES Guideline - Signature

1	introduction.....	2
1.1	purpose.....	2
1.2	summary	2
2	Signature classes and elements	3
2.1	Signature.....	3
2.1.1	Signature elements	3
3	description	4
3.1	specifying who signed	4
3.1.1	signatory example	4
3.2	specifying the validator.....	5
3.2.1	validator example.....	5
3.3	specifying the Signature.....	5
3.3.1	Signature example.....	6



NES Guideline - Signature

1 introduction

The Northern European Subset (NES) group was established to enable interoperability of procurement data between users of the Universal Business Language (UBL). UBL is a royalty-free library of XML documents addressing the requirements of electronic procurement and international trade and transportation. Its second version (UBL 2.0) was released as an OASIS standard in December 2006. NES members contributed extensively to the development of this version of the standard.

The focus of NES is to define the specific use of UBL 2.0 electronic procurement documents domestically and between the member 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 documents that comprise the NES subset of UBL 2.0.

All cardinalities shown in this document represent elements and associations at NES library level; see 'NES 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 NES documents

NES Guideline - Signature

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

2.1.1 Signature elements

name	definition	cardinality
ID	an identifier for the Signature	1
Note	free form text about the signature or the circumstances where the signature has been used	0..1
ValidationDate	specifies the date when the signature was approved	0..1
ValidationTime	specifies the time when the signature was approved	0..1
ValidatorID	identifies the organization, person, service or server that has validated the signature	0..1
CanonicalizationMethod	the mathematical logic method used by the Signature	0..1
SignatureMethod	the method of signature	0..1
<i>SignatoryParty</i>	an association to the signing Party	1
<i>DigitalSignatureAttachment</i>	an association to the actual encoded signature (e.g., in XMLDSIG format)	0..1
<i>OriginalDocumentReference</i>	a reference to the actual document that the signature applies to. For evidentiary purposes, this may be the document image that the signatory party saw when	0..1

NES Guideline - Signature

applying their signature

3 description

Signature describes the digital signatures 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-related 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 be required to have specific Signatures 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

```
<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:;></First Name>
      <cbc:FamilyName>Hansen</cbc:FamilyName>
      <cbc:Title>Indkøbschef</cbc:Title>
    </cac:Person>
  </cac:SignatoryParty>
</cac:Signature>
```

NES Guideline - 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

```
<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-xmlsig-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.

