

PEPPOL AS2 and Envelope/SBDH specification update

Philip Helger, 2018-10-31, Brussels

AS2 version 1.01



- > Released in May 2018
- > Mandatory since June 1st 2018
- > PDF version of the specification
https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-AS2_Service_Specification-1.01-2018-02-09.pdf
- > News item: <https://peppol.eu/updated-peppol-as2-specification/>

What changed and what did not

- > Each PEPPOL AS2 AccessPoint **MUST** support TLS 1.2 (old text was: **SHOULD**)
 - Specified in RFC 5246: <https://tools.ietf.org/html/rfc5246>
 - TLS 1.2 is the security baseline
 - This is a non-exclusive requirement
 - Support for other TLS versions (like 1.3) is allowed
 - If both clients support TLS 1.2 they will not agree on an older version
- > No new requirements TLS certificate usage
 - Everything is allowed except self-signed certificates
- > No requirements on the TLS cipher suites to be used
 - But this is true for the upcoming AS4 protocol

Plans for specification release 1.2



- > Used MIC algorithm (SHA-1) is out-of-date
 - We’re currently using the algorithms from RFC 3851 (where “sha1” is mandatory and “md5” is optional)
 - We plan to switch to the algorithm suites defined in RFC 5751
 - Implications:
 - “sha-256” will be the mandatory MIC algorithm
 - “sha1” is now called “sha-1” and it becomes optional
- > Current TLS certificate requirements are very vague
 - We need to find a better way... LOTL or gTSL?

Envelope/SBDH specification 1.1.1

- > Released September 2018
- > Mandatory immediately, because it is backwards compatible
- > Version 1.1.1 is a minor bug fix to version 1.1
- > PDF version of the specification
[https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-OpenPEPPOL-Envelope Specification-111 2018-09-28.pdf](https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-OpenPEPPOL-Envelope%20Specification-111%202018-09-28.pdf)
- > News items:
 - <https://peppol.eu/release-sbdh-v-1-1-1-specification/>
 - <https://peppol.eu/openpeppol-release-of-sbdh1-1/>

What changed in SBDH version 1.1?

- > Added the possibility to specify document type identifier scheme and process identifier scheme
- > Added the possibility to specify additional/custom attributes
- > `<HeaderVersion>1.0</HeaderVersion>`
 - is not changed for backwards compatibility

Identifier schemes

Old version 1.0

```
<BusinessScope>
  <Scope>
    <Type>DOCUMENTID</Type>
    <InstanceIdentifier>urn:oasis:names:specification:ubl:schema:xsd:Invoice-
2::Invoice##urn:www.cenbii.eu:transaction:biitrns010:ver2.0:extended:urn:www.peppol.eu:bis:peppol4a:
ver2.0::2.1</InstanceIdentifier>
  </Scope>
  <Scope>
    <Type>PROCESSID</Type>
    <InstanceIdentifier>urn:www.cenbii.eu:profile:bii04:ver1.0</InstanceIdentifier>
  </Scope>
</BusinessScope>
```

New version 1.1

```
<BusinessScope>
  <Scope>
    <Type>DOCUMENTID</Type>
    <InstanceIdentifier>urn:oasis:names:specification:ubl:schema:xsd:Invoice-
2::Invoice##urn:www.cenbii.eu:transaction:biitrns010:ver2.0:extended:urn:www.peppol.eu:bis:peppol4a:
ver2.0::2.1</InstanceIdentifier>
    <Identifier>busdcox-docid-qns</Identifier>
  </Scope>
  <Scope>
    <Type>PROCESSID</Type>
    <InstanceIdentifier>urn:www.cenbii.eu:profile:bii04:ver1.0</InstanceIdentifier>
    <Identifier>cenbii-procid-ubl</Identifier>
  </Scope>
</BusinessScope>
```

Additional/custom attributes

Name

Value

```
<BusinessScope>
  <!-- Document type and process ID -->
  <Scope>
    <Type>TECHNICAL_VALIDATION_URL</Type>
    <InstanceIdentifier>http://peppol.example.org/as4</InstanceIdentifier>
  </Scope>
  <Scope>
    <Type>TECHNICAL_VALIDATION_REQUIRED</Type>
    <InstanceIdentifier>true</InstanceIdentifier>
  </Scope>
</BusinessScope>
```

Name only

```
<BusinessScope>
  <!-- Document type and process ID -->
  <Scope>
    <Type>IndicatorAttribute</Type>
    <InstanceIdentifier />
  </Scope>
</BusinessScope>
```


Plans for specification release 1.2

> Support for text and binary content that is not XML

```
<xs:schema xmlns="http://peppol.eu/xsd/ticc/envelope/1.0"
            xmlns:xs="http://www.w3.org/2001/XMLSchema"
            targetNamespace="http://peppol.eu/xsd/ticc/envelope/1.0"
            elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="BinaryContent" type="BinaryContentType"/>
  <xs:complexType name="BinaryContentType">
    <xs:simpleContent>
      <xs:extension base="xs:base64Binary">
        <xs:attribute name="mimeType" type="xs:token" use="required"/>
        <xs:attribute name="encoding" type="xs:token" use="optional"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
  <xs:element name="TextContent" type="TextContentType"/>
  <xs:complexType name="TextContentType">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="mimeType" type="xs:token" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:schema>
```

Example with text content

```
<?xml version="1.0" encoding="utf-8"?>
<StandardBusinessDocument
  xmlns="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader">
  <StandardBusinessDocumentHeader>
    ...
  </StandardBusinessDocumentHeader>
  <TextContent xmlns="http://peppol.eu/xsd/ticc/envelope/1.0"
    mimeType="Application/EDIFACT">
    UNB+UNOA:2+9930711378399:14+7798032711116:14+160927:2252+EW861380947
    'UNH+186453437+CONTRL:D:96A:UN:EAN002....
  </TextContent>
</StandardBusinessDocument>
```

Example with binary content

```
<?xml version="1.0" encoding="utf-8"?>
<StandardBusinessDocument
  xmlns="http://www.unece.org/cefact/namespaces/StandardBusinessDocumentHeader">
  <StandardBusinessDocumentHeader>
    ...
  </StandardBusinessDocumentHeader>
  <BinaryContent xmlns="http://peppol.eu/xsd/ticc/envelope/1.0"
    mimeType="application/vnd.etsi.asic-e+zip" encoding="UTF-8">
    ABCD45678922 ...
  </BinaryContent>
</StandardBusinessDocument>
```