

**Business Interoperability Specification**

**OpenPEPPOL AISBL**

**Pre Award Coordinating Community**

**ICT - Models**

BIS eDocuments guide for pre-award

**Version: 1.2**

**Status: Final DRAFT**

***Statement of copyright***

This PEPPOL Business Interoperability Specification (BIS) document is based on the CEN CWA prepared by the BII workshop specified in the Introduction below.

The original CEN CWA document contains the following copyright notice which still applies:

|  |
| --- |
| © 2012 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members. |

The CEN CWA documents and profiles prepared by the BII workshop are not specific to a business area. Subject to agreement with CEN, customizations have been made by PEPPOL to establish the PEPPOL BIS, detailing and adding further guidance on the use of BII profiles.

OpenPEPPOL AISBL holds the copyright in the customizations made to the original document. The customizations appear from the corresponding conformance statement which is attached to this document. For the purpose of national implementations, customizations covered by the conformance statement may be further refined and detailed by PEPPOL Authorities and/or other entities authorized by OpenPEPPOL AISBL, provided that interoperability with PEPPOL BIS is ensured.

This PEPPOL BIS document may not be modified, re-distributed, sold or repackaged in any other way without the prior consent of CEN and/or OpenPEPPOL AISBL.

**Table of Contents**

[1 Introduction 4](#_Toc14098283)

[1.1 Audience 4](#_Toc14098284)

[2 References 5](#_Toc14098285)

[3 Document history 6](#_Toc14098286)

[3.1 Revision history 6](#_Toc14098287)

[3.2 Contributors 6](#_Toc14098288)

[4 ENISA SOG-IS standards 7](#_Toc14098289)

[5 ASiC-E container with CAdES signature 7](#_Toc14098290)

[5.1 Introduction 7](#_Toc14098291)

[5.2 Description 7](#_Toc14098292)

[5.2.1 mimetype 8](#_Toc14098293)

[5.2.2 sbdh.xml (SBDH) 8](#_Toc14098294)

[5.2.3 Business documents 8](#_Toc14098295)

[5.2.4 Additional documents 8](#_Toc14098296)

[5.2.5 META-INF/asicmanifest\*.xml 8](#_Toc14098297)

[5.2.6 META-INF/signature\*.p7s 9](#_Toc14098298)

[5.2.7 Additional rules 9](#_Toc14098299)

[5.3 ASiC signing 9](#_Toc14098300)

[6 Tender encryption 10](#_Toc14098301)

# Introduction

This document describes the cryptographic specifications you need to implement to execute pre-award processes. The cryptographic specifications apply both for the outer corners (corner 1 and 4, e.g. the tendering systems) as for the inner corners (corner 2 and 3, the access points).

All requirements in this document have been designed, tested and approved in the European Large Scale Pilot e-SENS. The document is based on “Signing-and-encrypting-CEN-BII-transactions” by Jon Ølnes (Difi). It explains the usage of the CMS encryption schemes, compliant with IETF RFC 5652 and ENISA SOG-IS standards for recommended crypto schemes and strengths.

## Audience

The audience for this document is organizations wishing to be PEPPOL enabled for exchanging pre-award business documents, and/or their ICT-suppliers. These organizations may be:

 Service providers

 Contracting Authorities

 Economic Operators

 Software Developers

More specifically, it is addressed towards the following roles:

 ICT Architects

 ICT Developers

 Business Experts

For further information on PEPPOL/OpenPEPPOL please see [COMMON BIS].

# References

[PEPPOL] <http://www.peppol.eu/>

[PEPPOL\_EIA] <http://www.peppol.eu/peppol_components/peppol-eia/eia>

[PEPPOL\_Transp] <http://www.peppol.eu/peppol_components/peppol-eia/eia#ict-architecture/transport-> infrastructure/models

[COMMON BIS] To be developed

[CEN\_BII2] [http://www.cenbii.eu](http://www.cenbii.eu/)

[eSENS] <http://wiki.ds.unipi.gr/display/ESENSPILOTS/D5.6-1+-+5.1.1+-+eTendering>

[DSI] https://joinup.ec.europa.eu/news/cef-building-blocks-cros

[UBL] <http://docs.oasis-open.org/ubl/UBL-2.2.html>

[Schematron] [http://www.schematron.com](http://www.schematron.com/)

[XSLT] <http://www.w3.org/TR/xslt20/>

[EIF] European Interoperability Framework 2.0, found at:<http://ec.europa.eu/isa/library/index_en.htm> [http://ec.europa.eu/isa/documents/isa\_annex\_ii\_eif\_en.pdf](%20http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf)

[GS1 Keys] <http://www.gs1.org/barcodes/technical/id_keys>

[ETSI] <https://portal.etsi.org/webapp/WorkProgram/SimpleSearch/QueryForm.asp>

[IETF] <http://trustee.ietf.org/trust-legal-provisions.html>

[ENISA SOG-IS] https://www.enisa.europa.eu/events/sog-is

# Document history

## Revision history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Organisation** | **Description** |
| 0.1 | 01-02-2018 | Chander Khoenkhoen | PIANOo | First version |
| 0.2 | 08-03-2018 | Kornelis Drijfhout | PIANOo | Addressed review comments difi |
| 1.1 | 25-06-2018 | Kornelis Drijfhout | PIANOo | Addressed review comments from CMB, adding Specifications for ASiC, deleting cryptographic specifications for REM-evidence. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Contributors

|  |  |  |
| --- | --- | --- |
| Country | Name | Organization (= Beneficiary – Organization in national consortium – Subcontractor) |
| NL | Kornelis Drijfhout | PIANOo – WG leader |
| GR | Jerry Dimitriou | University of Piraeus Research Center (UPRC) |
| GR | Lefteris Leontaridis | NetSmart – senior OpenPEPPOL advisor |
| GR | Andriana Prentza | University of Piraeus Research Center (UPRC) |
| ES | Manuel Cano Gomez | NEXUS IT |
| NO | Jan Mærøe | Difi |
| NO | Siw Midtgård Meckelborg | Difi |
| NO | Bergheim, Erlend Klakegg | Difi |
| IT | Elisa Bertocchi | Intercent-ER Agency |
| IT | Gandolfi Gabriele | Intercent-ER Agency |
| IT | Isabella Rapisarda | Consip – Pre-Award CC leader |
| DE | Ansgar Mondorf | University of Koblenz |
| SE | Daniel Simonsson | Visma |
| BE | Stefan Van Der Meulen | BOSA |
| DK | Anna-Lis | Difi – OpenPEPPOL office |
| DE | Rolf Kevitz | Beschaffungsamt des Bundesministeriums des Innern |
| PT | Daniel Lobo | Vortal |
| NL | Sander Fieten | Chasquis |
| ES | Alberto Chacon | Pixelware |
| PT | Helder Aranha | EsPAP |
| PT | Isabel Martins | EsPAP |

# ENISA SOG-IS standards

ENISA specifies cryptographic protocols, underlying algorithms and strengths. Different cryptographic mechanisms, although incomparable at first, are recalculated to so called comparable bit strength values. ENISA mandates a 128 bit comparable bit strength from 2020 on, accepting 112 bits as legacy until then. This 2-pager document works on the 128 bit strength for symmetric and 112 bits for asymmetric keys.

# ASiC-E container with CAdES signature

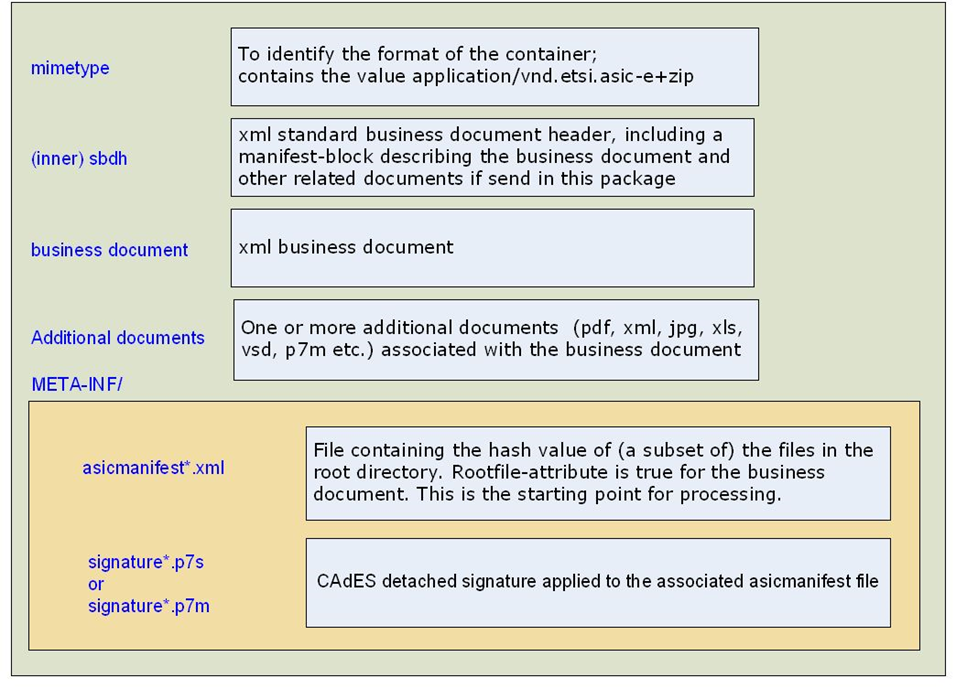
## Introduction

There is a need to pack all separate parts of a message together in order to achieve a single payload document for the transport network. This note specifies use of an ASiC-E container (Associated Signature Container Extended) for this purpose. ASiC is based on the zip format.

ASiC-E includes an ASiC manifest that holds metadata, identification of all parts inside the container, and hash values of these parts. Parts in this case are the SBDH, the CEN BII document, and all attachments that are included as separate parts. ASiC requires the manifest to be signed by a detached signature. Since the manifest holds hash values of all other parts, these are implicitly also signed. The signature is placed in the ASiC container as a separate part. This packaging allows security to be applied at message level, preserving security properties across asynchronous message passing with temporal storage at intermediate nodes. Authenticity and integrity are ensured by the ASiC signature, and confidentiality can be achieved by encrypting relevant parts.

The container described in this chapter is based on ETSI TS 102 918 V1.2.1[[1]](#footnote-1).

## Description



*Picture 1: Directory structure of an ASiC-E container with CAdES signature*

The container includes the following files:

### mimetype

* The purpose of this file is to identify the format of the container.
* Fixed name with the value “application/vnd.etsi.asic-e+zip”.

### sbdh.xml (SBDH)

* Xml file containing the standard business document header.
* It includes manifest-block for describing the business document and other related documents.
* All files except mimetype (having fixed name and value) and sbdh will be described in the manifest block.

### Business documents

* Xml file containing the business document.+

### Additional documents

* One or more documents of different types e.g. xml, pdf, jpg, xls, p7m and vsd associated with the business document and that needs to be signed.
* Files which are signed and encrypted has extension p7m.

### META-INF/asicmanifest\*.xml

* One or more files containing the hash values of all the documents (except mimetype) or the hash values of a subset of the data objects.
* If Rootfile attribute present and set to "true" it specify how to begin processing the container. The rootfile is the business document to be processed e.g. biitrdm082.xml.
* If one or more documents needs to be signed separately than the name should be suffixed by a number starting with 1.

Example: asicmanifest1.xml, asicmanifest2.xml etc.

### META-INF/signature\*.p7s

* One or more files containing the signature of the asicmanifest\*.xml.
* If one or more documents needs to be signed separately than the name should be suffixed by a number starting with 1 e.g. signature1.xml, signature2.xml etc.
* For each asicmanifest\*.xml file exactly one associated signature file must be present.

The sub directory META-INF includes an optional file manifest.xml, containing an overview of the files in the main directory of the container (except the mimetype).

### Additional rules

For the implementation of the transactions the following additional rules are implied:

* Exactly one asicmanifest.xml and consequently one signature.xml file will be used.
* In asicmanifest.xml the hash value of all the files, except mimetype will be calculated and stored.
* For calculating the hash value sha256 hash algorithm will be used.
* The mimetype, sbdh, business document, asicmanifest and the signature are not encrypted.
* Additional documents can be encrypted[[2]](#footnote-2) depending on the content of the document
* When encryption is required, each document is encrypted separately.

## ASiC signing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Signing values** | | | | |
| Protocol | Algorithm | KeySize | HASH | Reference |
| CADES B-B detached | DS-RSA; PSS (PKCS#1v2.1) | 2048[[3]](#footnote-3) | SHA-256 | RFC3447, PKCS1, ISO9796-2] |

|  |  |
| --- | --- |
| **Certificate for signing** | |
| type | X.509 V3 |
| CN / Identity holding private key | C1, Tendering Service Provider Legal Person |
| Sign / Seal | Sealing, authenticity and integrity from signature creation time |
| DATA / Payload | ASiC container; signing encrypted data |
| Key specs | RSA-2048 |
| Key usage | Signature |
| extensions | Subject Key Identifier (CMS type 2) |
| HASH algorithm | SHA-256 |
| PKI | PEPPOL PKI (Pre-award) |
| Qualified | No (Use of PEPPOL PKI) |
| Verifiable / can be validated | YES (PTN PKI) |

# Tender encryption

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Protocol** | **Protocol part** | **Algorithm** | | **strength** | **Comp.**  **strength** | **Encryptor** |
| CMS (Type 2) Enveloped-Data RFC 5652[[4]](#footnote-4) | Data encryption: | AES\_CBC[[5]](#footnote-5)  ISO10116 7-Padding | Symmetric Block Cipher | 128 | 128 | Tendering Service Provider (C1) |
| Key encryption | RSA | Asymmetric | 2048 | 112[[6]](#footnote-6) | idem |

|  |  |
| --- | --- |
| **Certificate for encryption** | |
| type | X.509 V3 |
| CN / Identity holding private key | C4, Sourcing Service Provider / CA |
| Key specs | RSA-2048 |
| Key usage | Key encipherment |
| extensions | Subject Key Identifier (CMS type 2) |
| HASH algorithm | SHA-256 |
| PKI | Self signed allowed if sealed by ASiC signing |
|  |
| Qualified | Not Required |
| Verifiable / can be validated | YES; by means of verifying ASiC signature |
|  |
| Per Tendering Process | Yes |

1. https://portal.etsi.org/webapp/workprogram/Report\_WorkItem.asp?WKI\_ID=42455 [↑](#footnote-ref-1)
2. For more information on encrypting document see BIS Cryptographic Specifications [↑](#footnote-ref-2)
3. ENISA allows RSA 2048 (112 bits comparable bit strength) as legacy until 2020 [↑](#footnote-ref-3)
4. RFC 5083 (authenticated encryption) is not used. Tender Signing is done on encrypted data (ASiC container) rendering a function equivalent of authenticated encryption as in RFC 5083 [↑](#footnote-ref-4)
5. In order to provide security in a strong sense, the encryption scheme must either be probabilistic and generate a random initialization vector to bootstrap encryption, or require an additional input, whose value can only be used once with a given key, i.e. a nonce. The specifications of modes of operation describe what is expected (nonce or random IV). Implementations shall follow these specifications, e.g., CBC with a constant or more generally a predictable IV does not follow the CBC specification [SP800-38A] and is not accepted. [↑](#footnote-ref-5)
6. ENISA allows RSA 2048 (112 bits comparable bit strength) as legacy until 2020 [↑](#footnote-ref-6)