

**Business Interoperability Specification**

**OpenPEPPOL AISBL**

**Pre Award Coordinating Community**

**ICT - Models**

BIS Cryptographic Specifications

**Version: 1.0**

**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](#_Toc506291853)

[1.1 Audience 4](#_Toc506291854)

[2 References 5](#_Toc506291855)

[3 Document history 6](#_Toc506291856)

[3.1 Revision history 6](#_Toc506291857)

[3.2 Contributors 6](#_Toc506291858)

[4 ENISA SOG-IS standards 7](#_Toc506291859)

[5 ASiC signing 7](#_Toc506291860)

[6 REM-MD Evidence Signing 7](#_Toc506291861)

[7 Tender encryption 8](#_Toc506291862)

[8 Appendices 9](#_Toc506291863)

[8.1 Appendix A 9](#_Toc506291864)

[9 Appendices 10](#_Toc506291865)

[9.1 Appendix A 10](#_Toc506291866)

# Introduction

This document describes the cryptographic specifications you need to implement to excecute 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 has been designed, tested and approved in the European Large Scale Pilot eSENS. 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Contributors

|  |  |  |
| --- | --- | --- |
| Country | Name | Organization (= Beneficiary – Organization in national consortium – Subcontractor) |
| NL | Kornelis Drijfhout | PIANOo – WG leader |
| GR | Jerry Dimitriou | NetSmart |
| GR | Lefteris Leontaridis | NetSmart – senior OpenPEPPOL advisor |
| GR | Andriana Prentza | University of Piraeus |
| 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 signing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tender Submission Signing** | | | | |
| Protocol | Algorithm | KeySize | HASH | reference |
| CADES B-B detached | DS-RSA; PSS (PKCS#1v2.1) | 2048[[1]](#footnote-1) | 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 Indentifier (CMS type 2) |
| HASH algorithm | SHA-256 |
| PKI | Waiting on outcome of PEPPOL RFC |
| Qualified | Waiting on outcome of PEPPOL RFC |
| Verifiable / can be validated | YES (PTN PKI) |

# REM-MD Evidence Signing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **REM-MD Evidence signing** | | | | |
| Protocol | Algorithm | KeySize | HASH | reference |
| XADES B-B | DS-RSA; PSS (PKCS#1v2.1) | 2048 | SHA-256 | RFC3447, PKCS1, ISO9796-2] |

|  |  |
| --- | --- |
| **Certificate for signing** | |
| type | X.509 V3 |
| CN / Identity holding private key | C3, Access Point for C4, actor in charge of C3 |
| Sign / Seal | Sealing, authenticity and integrity from signature creation time on |
| DATA / Payload | Includes Hash of received data (ASiC) container and receiving time |
| Key specs | RSA-2048 |
| Key usage | Signature |
| extensions | Subject Key Indentifier (CMS type 2) |
| HASH algorithm | SHA-256 |
| PKI | Waiting on outcome of PEPPOL RFC Different certificate than certificate used for the C2-C3 communication network. |
| Qualified | Waiting on outcome of PEPPOL RFC |
| Verifiable / can be validated | YES (PTN PKI) |

# Tender encryption

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Protocol** | **Protocol part** | **Algorithm** | | **strength** | **Comp.**  **strength** | **Encryptor** |
| CMS (Type 2) Enveloped-Data RFC 5652[[2]](#footnote-2) | Data encryption: | AES\_CBC[[3]](#footnote-3)  ISO10116 7-Padding | Symmetric Block Cipher | 128 | 128 | Tendering Service Provider (C1) |
| Key encryption | RSA | Asymmetric | 2048 | 112[[4]](#footnote-4) | 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 Indentifier (CMS type 2) |
| HASH algorithm | SHA-256 |
| PKI | Self signed allowed if sealed by ASiC signing |
| PEPPOL ok if supported by PEPPOL |
| Qualified | Waiting on outcome of PEPPOL RFC |
| Verifiable / can be validated | YES; by means of verifying ASiC signature |
| Or by means of trust in PTN PKI |
| Per Tendering Process | Yes |

1. ENISA allows RSA 2048 (112 bits comparable bit strength) as legacy until 2020 [↑](#footnote-ref-1)
2. 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-2)
3. 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-3)
4. ENISA allows RSA 2048 (112 bits comparable bit strength) as legacy until 2020 [↑](#footnote-ref-4)