

OpenPEPPOL Capacity Building Deliverable

Security; time stamps and checksums

Last updated 12/22/2016 12:31:00 AM

OpenPEPPOL AISBL

Rond-point Schuman 6, box 5

1040 Brussels Belgium

# 

Document Logistic

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed. Refer to the author if you are in any doubt about the currency of this document.

This Document relates to: Upgraded security within AS2 transmissions in OpenPEPPOL

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date of this revision: 25-04-2016 | | | Date of next revision (date) | |
| NR | Date | Summary of Changes | | Changes marked |
|  | 28 April 2016 | First draft | | S.O.Cook |
|  | June 23rd, 2016 | Added illustration on modification of MDN | | S.O.Cook |
|  | June 23rd, 2016 | Review | | P. Helger |
|  | October 12th, 2016 | Adding alternative approach. | | E. K. Bergheim |
|  | December 21st, 2016 |  | | E. K. Bergheim |

Approvals

This document is approved by:

|  |  |
| --- | --- |
|  |  |
|  | [Unit and role] |
|  | [Unit and role] |

Owner, Editor and Contributors

This document is provided by:

|  |  |
| --- | --- |
| **Feil! Fant ikke referansekilden.** | **Feil! Fant ikke referansekilden.** |
| Unit | [Community ore organizational reference] |
| Owner | Steinar Overbeck Cook, Difi, Deliverable Owner |
| Editor(s) | Christian Vindinge Rasmussen, Difi, Project Manager |
| Contributors | [Name and role]  [Name and role] |

Distribution

This document has been distributed to

|  |  |
| --- | --- |
| *Feil! Fant ikke referansekilden.* ***/ usergroup*** | *Feil! Fant ikke referansekilden.* |
|  | [Unit and role] |
|  | [Unit and role] |

Table of Content

[1. Pre-analyse report: identification of the need for extensions 3](#_Toc454448725)

[1.1. The current NRR (AS2 MDN) 4](#_Toc454448726)

[2. Requirement specification to all of the identified new Capability Extensions 5](#_Toc454448728)

[3. Design Documentation for all of the identified new Capability Extensions 5](#_Toc454448730)

[2. The message digest of the original payload, which was produced in C1, must be included in the machine-readable part of the AS2 MDN. 5](#_Toc454448731)

[3.1. Modified AS2 MDN (RFC3798) 6](#_Toc454448732)

[4. Revised eDelivery specifications/profile 6](#_Toc454448733)

[5. Implementation plan 6](#_Toc454448734)

[6. Relevant request for change to CEF eDelivery 6](#_Toc454448735)

1. Pre-analyse report: identification of the need for extensions

Directive 2014/24/EU, Annex IV contains requirements relating to tools and devices for the electronic receipt of tenders, requests for participation as well as plans and projects in design contests.

Item (a) of the said annex states “*the exact time and date of the receipt of tenders, requests to participate and the submission of plans and projects can be determined precisely;* “.

This raises the question of when and where the “exact time and date” should be registered. This matter has been discussed extensively in the eSENS project, which has concluded that the Time of Arrival (TOA) should be registered at C3 when the message has been received. The TOA should be returned to C2 as part of the Non-Repudiation Receipt (NRR).

I addition to TOA is SHA-1 not seen as secure enough, thus is a stronger hashing algorithm required. Based on work in eSENS is SHA-256 seen as a minimum when using hashing, resulting in a need to use a stronger hashing algorithm in AS2 messages.

* 1. The current NRR (AS2 MDN)

The current NRR, which is implemented in AS2 in accordance with RFC3798 has been depicted below: 

The contents of the human readable part is free form text, even though it might look like it contains structured information. This example simply contains an “echo” of the http headers received by the sender’s Access Point and MUST NOT be constructed as structured.

The machine-readable part contains strictly name-value pairs, which follow the syntax for MIME headers.

As can be seen, the human readable part is meant to be read by a human being and is henceforth not suitable for parsing by a computer program.

The machine readable part, which is intended for consumption by computer programs, does not contain the required fields (TOA and digest of original payload).

1. .Requirement specification to all of the identified new Capability Extensions

The requirements as set forth in 2014/24/EU implies that the transport infrastructure must register a) the TOA and b) the message digest of the original payload as produced by C1 upon receipt in C3 using a trustable hashing algorithm.

The AS2 protocol currently being used by PEPPOL does not provide these two information elements. The AS2 MDN, which serves as the NRR, is missing two pieces of information:

1. The time of arrival (TOA)
2. The message digest of the payload.

The current AS2 MDN does not include these fields:

* There is no timestamp in the machine-readable and signed part of the MDN.
* There is a digest of the payload however, this uses SHA-1 only.

This implies that AS2 currently does not comply with the provisions of the directive.

1. Design Documentation for all of the identified new Capability Extensions

In AS2, the NRR is named Message Delivery Notification (MDN) and specified in RFC3798[[1]](#footnote-1).

In order to comply with the provisions of Directive 2014/24/EU, we must add the following features to the transport protocol:

1. The time of arrival (TOA) of the message at C3, must be included in the machine readable part of the AS2 MDN.
2. The message digest of the original payload, which was produced in C1, must be included in the machine-readable part of the AS2 MDN.
3. Upon request from C1 and C4, C2 and C3 must provide a NRR, which contains the said information elements. The NRR must be transport protocol agnostic. I.e. the AS2 MDN should not be provided as-is.   
   The eSENS project has mandated the use of REM evidence in accordance with a slightly extended version of ETSI TS 102 640-2 v2.1.1[[2]](#footnote-2)  
     
   This provision should be included in the Transport Infrastructure Agreement (TIA). The details of the REM evidence are specified in a separate document.
   1. Modified AS2 MDN (RFC3798)

Section 3.3 of RFC3798 specifies that “additional MDN fields may be defined in the future by later revisions or extensions to this specification”.

In accordance with the provisions of section 3.3, this additional field should be added to the MDN:

|  |  |
| --- | --- |
| Field name | Field description |
| Date | Contains the “time of arrival” TOA of the message as defined by IANA. The value should be formatted as specified by RFC5322 3.3. It must include the date and time up to seconds accuracy. |

* 1. Updated hashing algorithm

RFC4130, written in 2005, states that MD5 and SHA-1 are “[t]he currently supported values for MIC algorithm <micalg> values”. RFC3851, which RFC4130 is based upon specifies support for SHA-256, SHA-384 and SHA-512 in addition to MD5 and SHA-1, and it also allows for other hashing algorithms to be used.

Based on our current knowledge (2016) related to weaknesses in hashing algorithms and the development in computer hardware since 2005, it is reasonable to update the algorithm used by OpenPEPPOL to be a stronger when new requirements arises. Based on requirements is SHA-512 chosen as the proposed hashing algorithm.

* 1. Introducing “busdox-transport-as2-ver1p0r1”

To be able to distinguish the version using SHA-1 from the one using SHA-512, we should introduce this revisited OpenPEPPOL AS2 profile as version 1.0.1, both as a new version of the profile and as a separate endpoint in the SMP. AS2 versions 1.0/1.1/1.2 are already defined, and as this proposal does not introduce functionality found in those minor versions, it is only appropriate to add this as a revision of our existing implementation.

Introducing SHA-512 means in practice to introduce SHA-512 not only in the MDN, but also in the AS2 message. By doing so may the AS2 endpoint be able to handle both versions as the AS2 message contains information regarding digest used in its header.

We should not expected that all endpoint in the network may handle version 1.0.1, but as this is a rather minor update, we should be able to see an upgrade of the network in a timely manner.

1. Revised eDelivery specifications/profile

As described above should the OpenPEPPOL AS2 profile be updated to version 1.0.1. Changes are rated as such:

* Changing from SHA-1 to SHA-512 – As this is grounded on standards AS2 builds upon, this is fully within the scope of a profile.
* Adding the Date field in MDN – This is seen as an extension to the OpenPEPPOL AS2 profile.

The current OpenPEPPOL AS2 profile defines new error codes in the MDN not part of AS2 or any standards AS2 builds upon. Not only is the new error codes specified in the profile, OpenPEPPOL also recommends to use them. By defining new error codes is the OpenPEPPOL AS2 profile in fact the OpenPEPPOL AS2 extension.

Both proposed changes fits nicely inside the current OpenPEPPOL AS2 extension, thus are there no needs to look for other protocols to implement this rather minimal change to the existing extension that fulfils our new requirements.

1. Implementation plan

OpenPEPPOL AS2 profile/extension 1.0.1 should be made available as an optional extension for those domains requiring this update. The proposal is not in conflict with traffic in the PEPPOL network not using this extension.

1. Relevant request for change to CEF eDelivery

This update does not require changes related to CEF eDelivery.

1. https://tools.ietf.org/html/rfc3798 [↑](#footnote-ref-1)
2. http://www.etsi.org/deliver/etsi\_ts/102600\_102699/10264002/02.01.01\_60/ts\_10264002v020101p.pdf [↑](#footnote-ref-2)