PEPPOL Transport Infrastructure AS2 Profile 2.0

News from TICC

Philip Helger, philip@helger.com

26.03.2019

AS2 profile v2.0

- Specification: https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/PEPPOL-EDN-AS2-Profile-2.0-2019-03-14.pdf
- News items:
  - https://peppol.eu/release-of-peppol-as2-v-1-2-specification-and-peppol-policy-for-use-of-identifiers-v-4/
  - https://peppol.eu/member-review-of-peppol-as2-profile-v-2-0/
- This version is not backwards compatible to v1.1
- This version is NOT YET in effect

AS2 profile v2.0

- Main motivation: replace SHA-1 with SHA-256 because SHA-1 is considered unsafe
- Update from
  “RFC **3851** S/MIME v3.1 Specification” to
  “RFC **5751** S/MIME v3.2 Specification”
- Has implications on main message sending/receiving as well as for MDN sending/receiving

AS2 profile v2.0

Algorithm	RFC 3851 (old)	RFC 5751 (new)
MD5	`md5`, optional	`md5`, optional
SHA-1	**`sha1`, mandatory**	`sha-1`, optional
SHA-224	Not supported	`sha-224`, optional
SHA-256	`sha256`, optional	**`sha-256`, mandatory**
SHA-384	`sha384`, optional	`sha-384`, optional
SHA-512	`sha512`, optional	`sha-512`, optional

AS2 profile v2.0

- Implications on AS2 messages
  - The MIC algorithm SHA-256 MUST be supported
    - By the message sender for creation
    - By the message receiver for verification
- `Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=`**`sha-256;`** `boundary="any"`

AS2 profile v2.0

- Implications on AS2 MDN messages
  - The MIC algorithm SHA-256 MUST be supported
    - Must be requested by the message sender
    - By the MDN sender for creation
    - By the MDN receiver for verification
- `Disposition-Notification-Options: signed-receipt-protocol= required, pkcs7-signature; signed-receipt-micalg=required, sha-256, sha256`

AS2 profile v2.0

- Update from RFC 2616 to RFC 7230-7235
- Both RFCs handle HTTP 1.1
- Change log: https://tools.ietf.org/html/rfc7230#page-80
- RFC 2616 support is running out

AS2 profile v2.0

- The transport profile identifier for this version of the specification changed.
- Old: `busdox-transport-as2-ver1p0`
- New: `busdox-transport-as2-ver2p0`
- Requires new SMP registrations
- Maybe supported on the same AP URL
- Use them in parallel during migration

AS2 profile v2.0

- Also added support for “RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3”
- The TLS connection MUST be using TLS v1.2 or v1.3
- TLS v1.3 support is quite wide spread already

AS2 profile v2.0

- Allowed protocol ports are limited to 443, 44300 to 44399
  - https default (443) is preferred
- Aligned with AS4 profile
- See also the PEPPOL Transport Security Policy

AS2 profile v2.0

- Migration procedure
- T1: start using profile v2, optionally
- T2: v2 becomes mandatory and v1 optional
- T3: v1 MUST NOT be used anymore

- Exact dates are not yet finalized