ESI(19)65_036r3

LIAISON STATEMENT

Title: Digital Signatures formats for PSD2 Secure Communications

Date: 2019-03-27

From (source): ETSI TC Electronic Signatures and Infrastructures

Contact(s): Sonia Compans: Technical Officer ETSI ESI <sonia.compans@etsi.org>
Nick Pope: Vice Chair ETSI ESI <nick.pope@secstanassoc.com>

To: PSD2 API Standards Communities (OBE, Berlin Group, STET, Polish API, Open Banking UK, EBA)

Response to: Not applicable
(if applicable)

Attachments: No attachment
(if applicable)

ETSI wishes to bring to the attention of those communities working on PSD2 API Standards the risks associated with some digital signature formats and the availability of standard digital signature formats which provide comprehensive features to counter known risks.

Firstly, ETSI ESI has become aware that some PSD2 API standards communities are considering adoption of the Internet Draft standard for HTTP Signatures (https://tools.ietf.org/html/draft-cavage-http-signatures-10). It should be noted that:

1. HTTP Signature has status draft only and has not necessarily undergone full review by cryptographic experts concerning possible vulnerabilities inherent to that format
2. It makes no direct provision for preventing certificate substitution attacks and can consequently be vulnerable such attacks (cf. RFC 5035, https://tools.ietf.org/rfcmarkup/5035 - Enhanced Security Services for S/MIME)

ETSI ESI has published a set of standards, commonly referred to a CAdES and XAdES for digital signatures applied to binary or XML data formats, which support signing arbitrary content even for signatures detached from the data being protected (reference: EN 319 122 and EN 319 132 respectively) which could be used for PSD2 APIs. Also the ETSI PAdES (EN 319 142) standard can be used for signing PDF documents. These mature standards provide protection against known risks, can be used to assure the evidential value of the signatures over the long term and are the accepted formats for advanced electronic signatures and seals under the eIDAS regulation 910/2014.

ETSI is also working on an equivalent standard digital signature format to apply signatures to JSON data structures. This builds on the existing IETF RFC 7515 standard for JSON Web Signatures.

ETSI would be pleased to provide further information on its digital signature formats. Enquiries can be sent through the contacts listed above. ETSI standards can be downloaded from: https://www.etsi.org/standards-search.