OPEN
BANKING
EXCHANGE

JSON Web Signature Profile - Factsheet

The Open Banking Europe JSON Web Signature Profile aims at addressing the concerns about standardisation & security in signing Open Banking APIs & aligning European APIs onto one security model

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE
ČESKÁ BANKOVNÍ ASOCIACE CZECH BANKING ASSOCIATION
SLOVAK BANKING ASSOCIATION
POLISH BANK ASSOCIATION
CONSORZIO CBI
customer to business interaction
stet
OPEN BANKING
SIBS.
TEAM PER LA TRASFORMAZIONE DIGITALE
BORICA
BANK SERVICES

Background

Under PSD2, Account Servicing Payment Services Providers (ASPSPs) are obliged to allow regulated Third-Party Providers (TPPs) to access customer accounts via Application Programming Interfaces (APIs) that are found on developer portals. Most implementations require that the data sent across the APIs is digitally signed for security reasons. However different API communities and frameworks are suggesting a different mechanism for signing and this needs to be aligned with current practices for "Advanced Electronic Signatures" under the eIDAS Regulation (reference). This fact highlighted both by Open Banking Europe (OBE) (reference) and the European Telecommunication Standards Institute (ETSI) (reference).

Together OBE and ETSI, along with the API communities created a standardised JSON Web Signature Profile, which will allow all ASPSP to standardise the way APIs are signed, and so make them easier and safer for TPPs and the market.

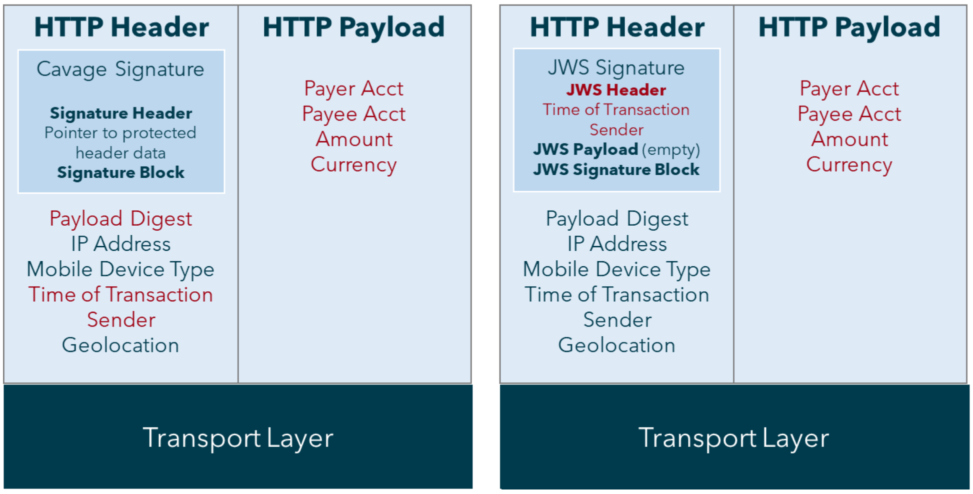
Methodology

OBE brought together a group of experts from the PSD2 API communities with experts on signature formats from ETSI. The group carried out a survey of the current approaches to secure communications for PSD2 based on EU Qualified Certificates as required under the EU "regulatory technical standards for strong customer authentication and common and secure open standards of communication"

Based on the survey results, it was agreed to produce a common specification of how to protect PSD2 payloads which brings together the JSON Web Signatures with the ability of HTTP Signatures to protect HTTP header information and is aligned with current practices under the eIDAS Regulation.

Questionnaire & Security Model

At the end of the questionnaire, the main findings were that eIDAS certificates (QSealC) are used with public-key cryptography to create digital signatures and that two alternative standards are being used : one is the Internet Draft for HTTP Signature (Cavage v10) and the other is standard for JSON Web Signatures (JWS) as defined in Internet RFC 7515. These two different protocols protected the HTTP header and payload in different ways. The main feature of HTTP Signatures (Cavage) is that HTTP header information is protected as well as the payload. This has been adopted by those requiring more than the payload to be protected. JWS was used just to protect the payload. However, JWS allowed additional attributes of the signature to be protected. This is illustrated in the following figure:



The Items in red are protected by the signature

Data items in HTTP header & Payload are purely illustrative & do not reflect any real-life example

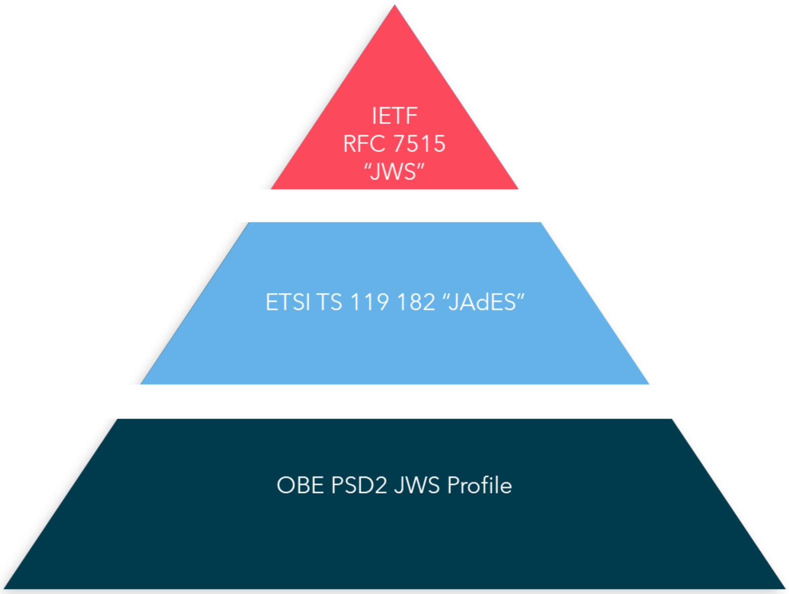
Figure 1: Illustration of HTTP Signature (Cavage v10) and RFC 7515 JSON Web Signatures

Key Requirements of the Signature

Different groups want different HTTP header elements protected. However, there are a few mandatory requirements for the signature:

- To define a single harmonised solution.
- To base the solution on an existing stable standard (i.e. JWS).
- To align the solution with the framework of the ETSI standard practices for eIDAS Advanced Electronic Signatures as being applied in the upcoming ETSI “JAdES” standard (to be ETSI TS 119 182.
- To protect the HTTP Payload.
- To protect selected parts of the HTTP header information.

Relation of the OBE JWS Profile to ETSI TS 119 182 "JAdES" & IETF RFC 7515 "JWS"



The OBE PSD2 JWS profile is fully compatible with ongoing ETSI TS 119 182 JAdES standard (currently under development) which is itself compatible with the IERF FRS 7515 which is the JWS standard.

Next Steps

The final version of the OBE JWS Profile will be lodged in the official JWS (IANA) repository and made public to avoid additional fragmentation. The JWS Profile will then be taken and offered to ETSI as the basis of a JAdES standard at some time in the future - at which point it will be up to ETSI to decide whether and how to take it forward.

It is expected that the profile will be integrated into the specifications of the API communities and integrated into the APIs of the ASPSPs.

Where Can I Find Out More?

To learn more about Open Banking Exchange visit our website or contact us at info@openbanking.exchange .

OPEN
BANKING
EXCHANGE

https://www.openbanking.exchange/