OPEN
BANKING
EUROPE

OBE/ETSI Meeting on Digital Signatures Formats for PSD2 Secure Communications #6

OPEN BANKING EUROPE

1.1 Welcome

Participants (Possible based on last meeting & registrations)

OBE / ETSI Group Secretariat
John Broxis & Nick Pope

Financial Community / OBE

Community	Name
Berlin Group	Detlef Hillen
UK Open Banking	Ralph Bragg
STET	Hervé Robache
SIBS	Eduardo Galvão
Poland Banking Association	Maciej Kostro (apologies)
Czek Banking Association	Tomáš Hládek
CBI Italy	Liliana Fratini Passi

Trust Services / ETSI

Organisation	Name
DAC-UPC	Juan Carlos Cruellas
Luxtrust	Thomas Kopp
Microsec	Kornél Réti
InfoCert	Luigi Rizzo
Bundesdruckerei	Christian Seegebarth
TIMT	Michal Tabor
Cryptolog	Andrea Rock

Expert Invitee

Roberto Polli	Team Digitale, Italy

OPEN BANKING EUROPE

1.2 Agreement of the Agenda

Agenda

#	Items
01	Welcome, Roll call, Anti-Competition Statement Agreement of the Agenda Outstanding actions from previous meetings (see below) Agreement of minutes of last meeting (Document 1)
02	Recap on Previous Meetings
03	JWS Profile Final review - Proposed Final Combined Disposition of comments (document 3) - Minor Microsec comments + NP on OBE JWS v0.4 (document 4) Approval of final draft
04	Next steps on JWS Profile - Example OBE JSON Web Signature - OBE / UPC Demonstrator - Test implementations - ETSI JAdES
05	Meeting calendar To be agreed AOB

OPEN BANKING EUROPE

1.3 Anti Competition Statement

Reminder of the importance to comply with antitrust law

- Strict compliance with EU and national competition laws forms part of the business discipline of PRETA and is key to its commercial success;

- Any violation of the antitrust laws can lead to lengthy and costly administrative (and in some countries criminal) investigations, significant reputational damage, business disruption, hefty fines, civil liability for damages, and, in a growing number of EU States, sanctions against individuals having engaged in illicit conduct;

- All attendees are kindly invited to review carefully this brief and general reminder on Do's and Don'ts to help ensuring that inadvertent breaches of antitrust rules are avoided.

Do's and Don'ts

Do not	Do
Do not share commercially sensitive information: • Exchanges on prices and sales volume ; • Exchanges on current production, costs, business plans; Do not participate in any statistical exercise, market survey or benchmarking exercise that allows access to individualised business sensitive information from the various reporting companies. Do not discuss or agree with competitors: • To limit supply of services, output, technical development or investments; • To allocate markets or customers; • To exclude (potential) competitors or alternative solutions, including boycotts.	• Only attend meetings with written agenda's / a clear purpose. • Limit discussions during meetings to agenda topics. • Please remember that competition law can apply even if the disclosure of information is informal (made orally, in a social or other informal context such as dinner) or non-reciprocal. • Consult your own legal / competition counsel in case of doubts or concerns for specific / additional guidance.

OPEN BANKING EUROPE

Confirmation of minutes of last meeting

1.3 Actions from last meeting

Ref.	Action	Who	Status
SigFormat #3-5	Prepare information on signatures in non-API channels for discussion at next meeting.	OBE	Ongoing

Confirmation of minutes

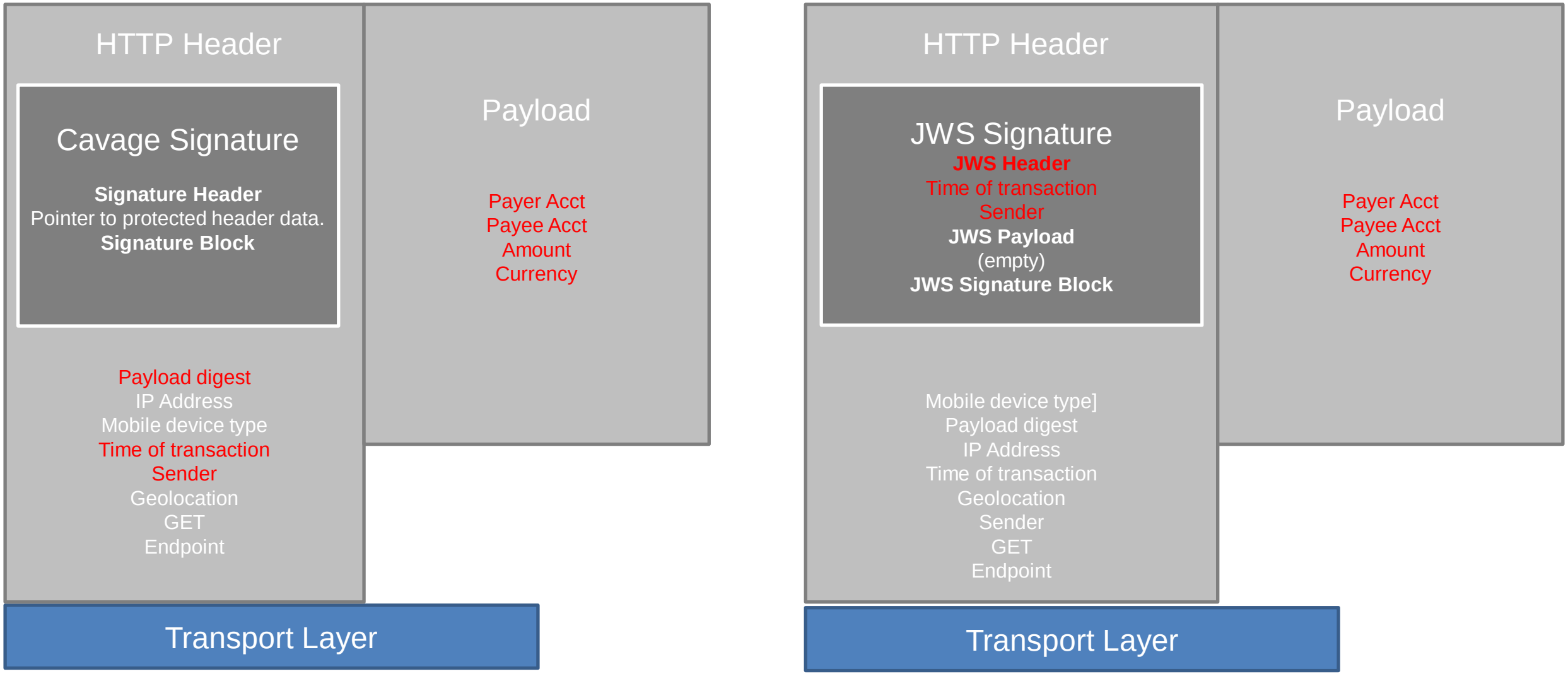
See: 20200316 OBE-ETSI meeting on Sig Formats #5 minutes Draft r1

2. Recap on Previous Meetings

API Communities Survey on Communication Security Practices

	Berlin Group	Czech Open Banking	Poland	SIBS (Portugal)	STET	UK Open Banking	Comparison
Q12 What existing standards are used as the basis of applying digital signatures to the PSD2 secure communications?	HTTP Signature (Cavage v10)	HTTP Signatures (Cavage) v. 10 or JWS	JWS (RFC 7515), JWT not allowed	HTTP Sig (Cavage v10)	HTTP Sig (Cavage v10)	Detached JWS (RFC 7515) carried in HTTP header … [see document for more detail]	JWS or Cavage signature carried in HTTP header In Poland JWS port of payload
Q13 Is it required to apply signatures on HTTP payloads without impacting legacy software (e.g., ISO 20022 based software)?	Yes	Yes	No	Yes	Yes Can be XML or JSON Separate signature from business data	Where content type is present normally set to application/json	Most require to support legacy software ISO2022 can encoded in XML or JSON
Q14 What information, other than the payload, needs to be protected by the digital signature?	Only if TPP signature is requested: request-ID …..	COBS does not specify this, it is on each of the ASPSPs	No	a. Signing time b. PSU-Id e. Other – Transaction identifier ….. [see document for more detail]	Signing time …. [see document for more detail] For all signatures	Signing time Yes – seconds from 1970 Key id PSP Identifier Trust anchor	Varying. Varied support for certificate protection and signing time as required by AdES.

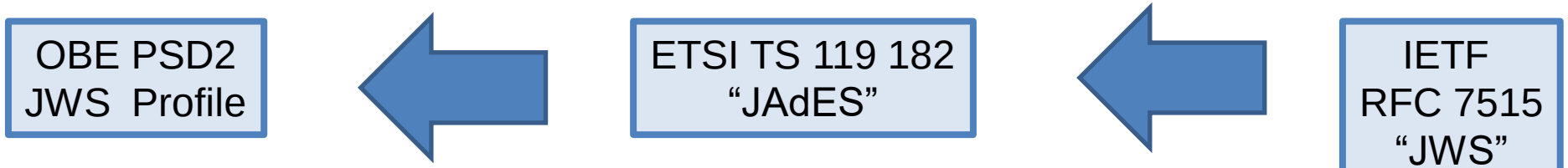
Summary of methodologies



Alternative approaches to API harmonisation & alignment with AdES basic requirements

1) Adopt common approach around JWS (detached) Signatures in HTTP Header ○ Define extensions to protect HTTP header elements (including HTTP header "date" ?) ○ Agree how to carry certificate reference and hash in keyId & x5t#S256 ○ Agree common JWS baseline profile for Open Banking aligned with ETSI JAdES ➢ JWS Profile	✔ Following an IETF standard ✔ Could be recognised under eIDAS (JAdES in progress). ✘ More reworking of the standards (and their corresponding implementations). Agreement to work on this approach
2) Define harmonised approaches for HTTP Signature and JWS 2a) HTTP Signatures ○ Clarify in HTTP Signature how any signature header can be included in "header" parameter (including keyId) ○ Agree how to carry certificate reference and hash in keyId ○ Agree common HTTP Signature Baseline Profile for Open Banking ○ 2b) JWS as 1) above ➢ JWS Profile ➢ HTTP Signatures Profile.	✘ Not an IETF standard. ✘ Not on any current roadmap for eIDAS. - Could become IETF and work could be proposed to ETSI for "HAdES"? ✔ Less reworking of the standards (and their corresponding implementations).

OBE JWS profile & JAdES & JWS (RFC 7515)



1) Requirements on Use of JWS structures

2) Requirements on use of JWS & JAdES headers (2+)

3) PSD2 specific profile (aligned with JAdES B-B Baseline)

1) Requirements on JWS Headers

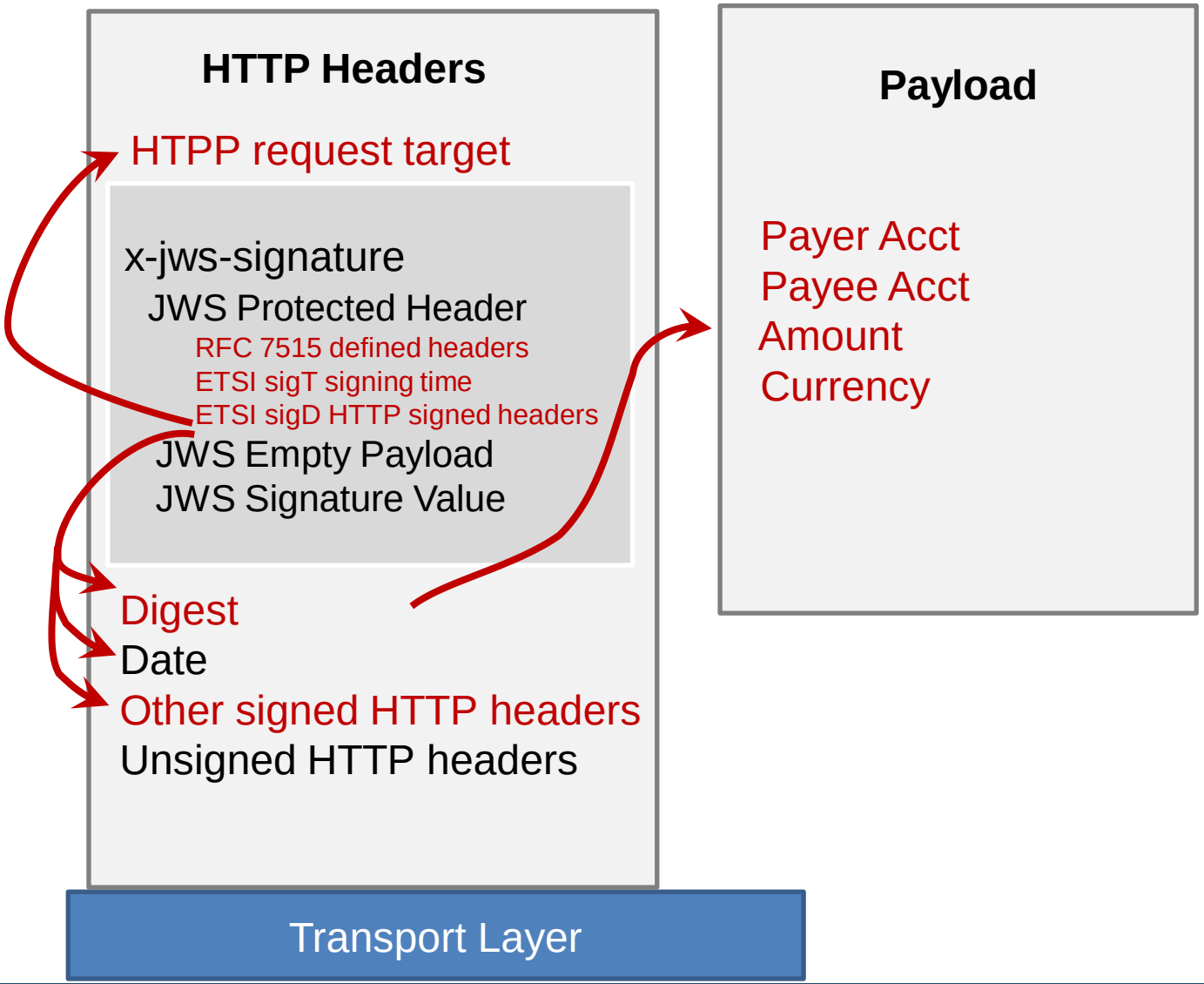
2) Definition of additional JWS header parameters (8)

3) “Baseline” profiles

1) JWS Structures

2) JWS Headers

JWS Basic Structure



OPEN BANKING EUROPE

3. OBE PSD2 JWS Signature Profile Updates

Proposed Final Disposition of Comments on v0.2

See: Proposed final Combined Disposition of comments on OBE JWS profile 0.2+mtg - 2020-03-23-revs
(document 3)

Microsec comments and final review

See: Microsec comments + NP on PRETA-OBE-ID-000-004-PSD2-JWS-Protection-Profile-OBE review Draft v0.4b – 2020-04-13 draft

(Document 4)

Approval of stable draft

- Agree an approach in principle (last meeting)
- Initial Draft (Before Christmas)
- Discuss initial draft (January meeting)
- Confirmed support in principle (January meeting)
- Updated draft produce following January meeting
- Disposition of comments 95% agreed (16 March meeting)
- Proposed stable draft distributed (30 March)

- **<u>This meeting to discuss (and confirm !) stable draft</u>.**

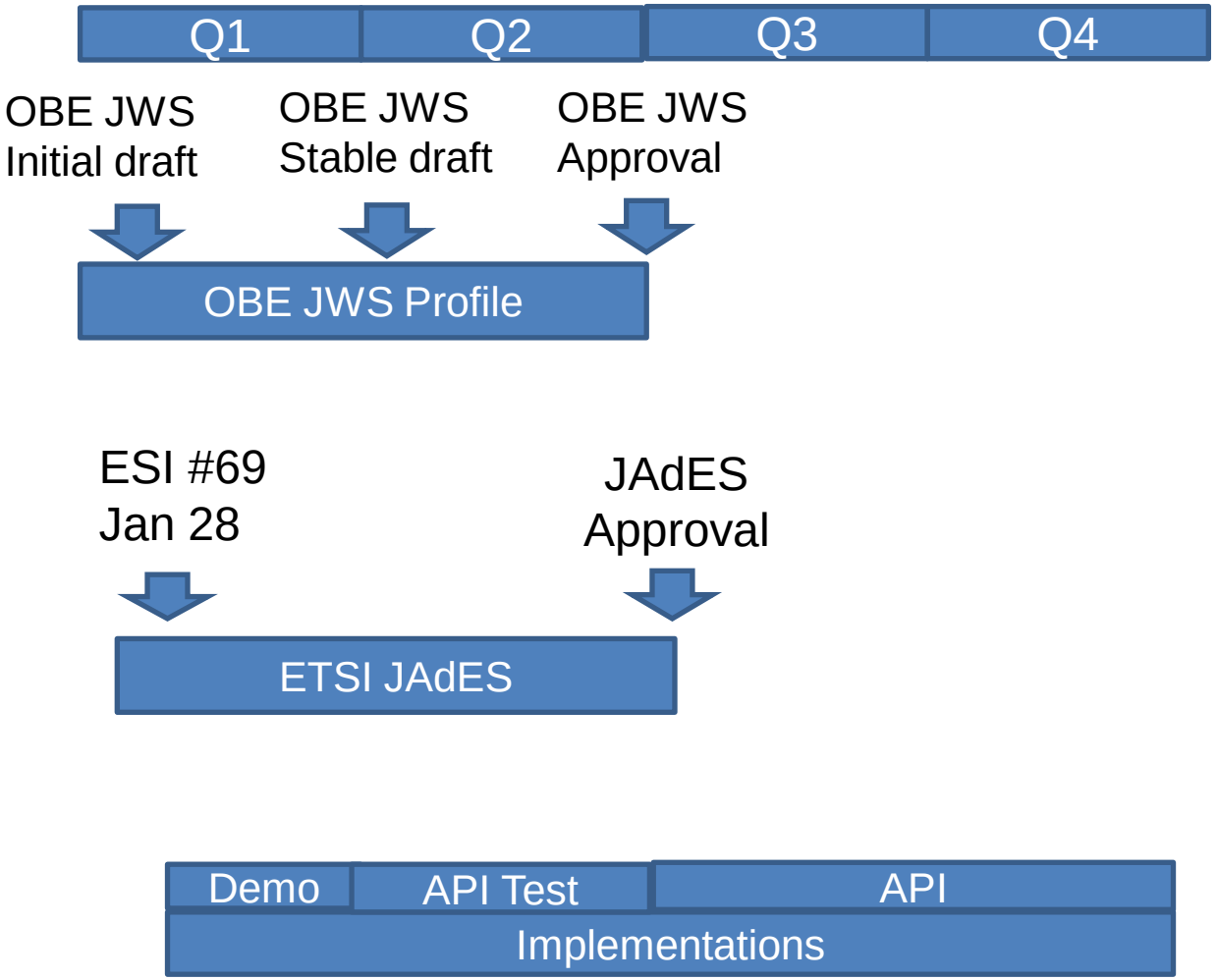
OPEN BANKING EUROPE

4. JWS Next Steps

Next steps

- Example OBE JSON Web Signature
- OBE / UPC Demonstrator
- Test implementations
- ETSI JAdES

Overall plan



OPEN BANKING EUROPE

Date of Next Meeting & A.O.B.

Next Meeting

Next meeting: Mid June
(a Doodle will be sent for agreement of date)

OPEN
BANKING
EUROPE

For more information

www.openbankingeurope.eu