Berlin Group

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

BITS

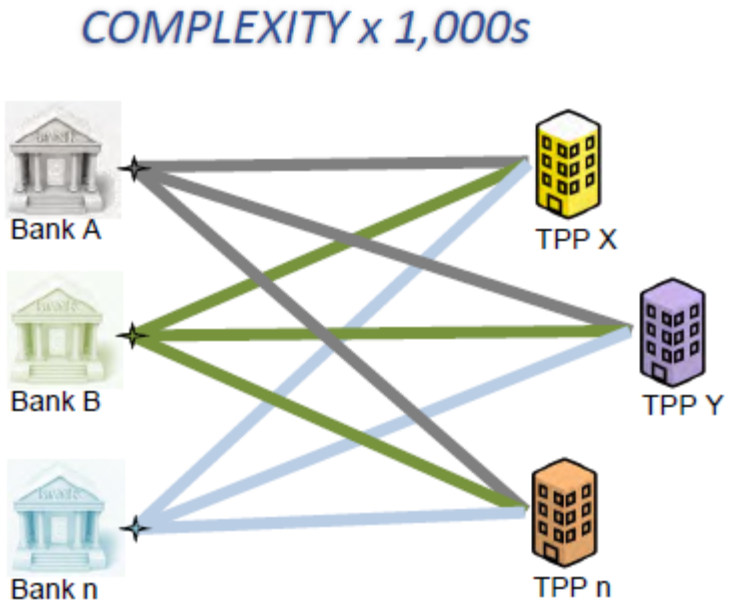
Betalingsinfrastruktur i verdensklasse !!

Bakgrunn og fordeler med arbeidet

- PSD2 krever at bankene, forutsatt samtykke fra kunden, gir tredjeparter tilgang til følgende tjenester:
  - Initiering av betaling iht artikkel 65 (PISP)
  - Tilgang til kontoinformasjon iht artikkel 67 (AISP)
  - Tilgang til å bekrefte dekning i henhold til artikkel 65 (AISP)
- PSD2 artikkel 98 gir mandat til EBA for å utvikle RTS for SCA & CSC
- RTS artikkel 30 krever at ASPSP tilbyr minst ett grensesnitt for TPP

NextGen PSD2

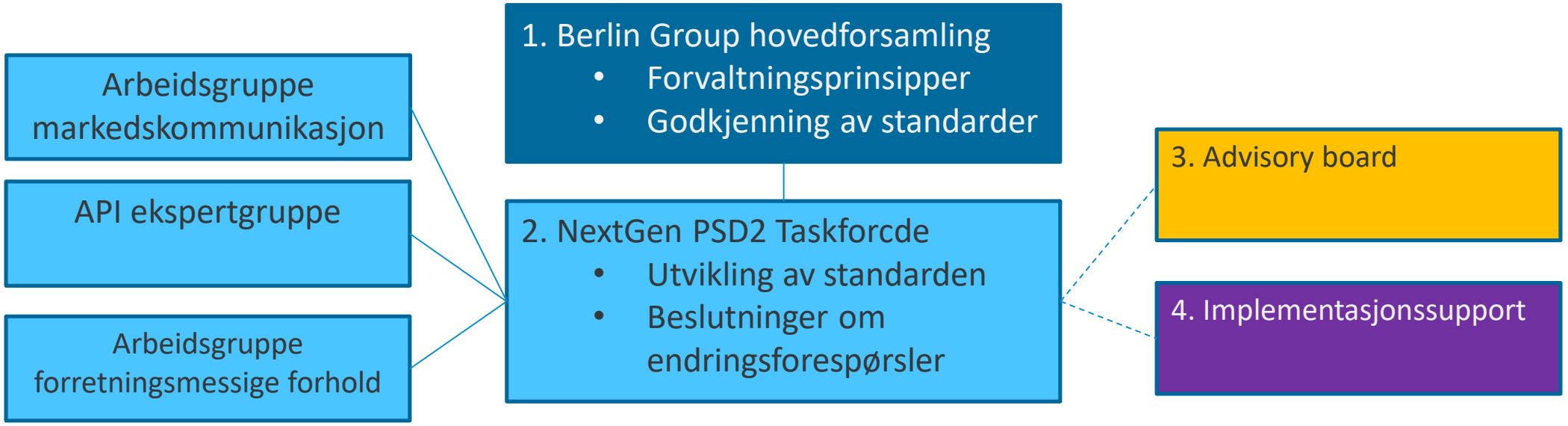
- Hvis hver bank utvikler, dokumenterer, tester og vedlikeholder sin eget proprietære XS2A standard gir dette:
  - Høy nettverkskompleksitet
  - Høy grad av testing og operasjonell risiko
  - Mye dokumentasjon
  - Økt risiko på bakgrunn av pan-europeisk skala



Den store tanken

NextGen PSD2 taskforce

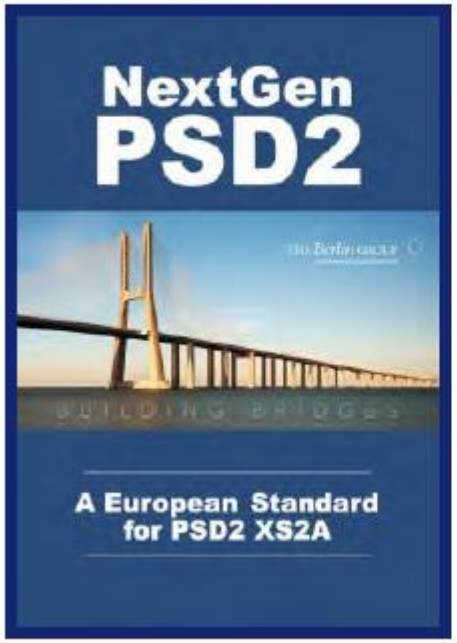
- NextGenPSD2: teknisk arbeidsgruppe i regi av Berlin Group
- Mål: levere en åpen, harmonisert XS2A spesifikasjon i samsvar med PSD2 og EBA RTS SCA & CSC
- Medlemskap åpen for aktører på tilbudssiden: ASPSP, bankforeninger, betalingsschemes og interbank prosessorer i SEPA
- Etterspørsels-siden deltar via 'Advisory board', høringer og gjennom direkte feedback på e-post



NextGenPSD2 rammeverk

- Åpen, harmonisert XS2A spesifikasjon for å implementere 'dedicated interface'
- Definerer et obligatorisk minimums-sett av tjenester for å oppnå samsvar
- Tilgjengelig for TPPer for tilkobling til ASPSP som supporterer standarden
- Publisert gratis under Creative Commons (CC-BY-ND)

INTRODUCTION PAPER

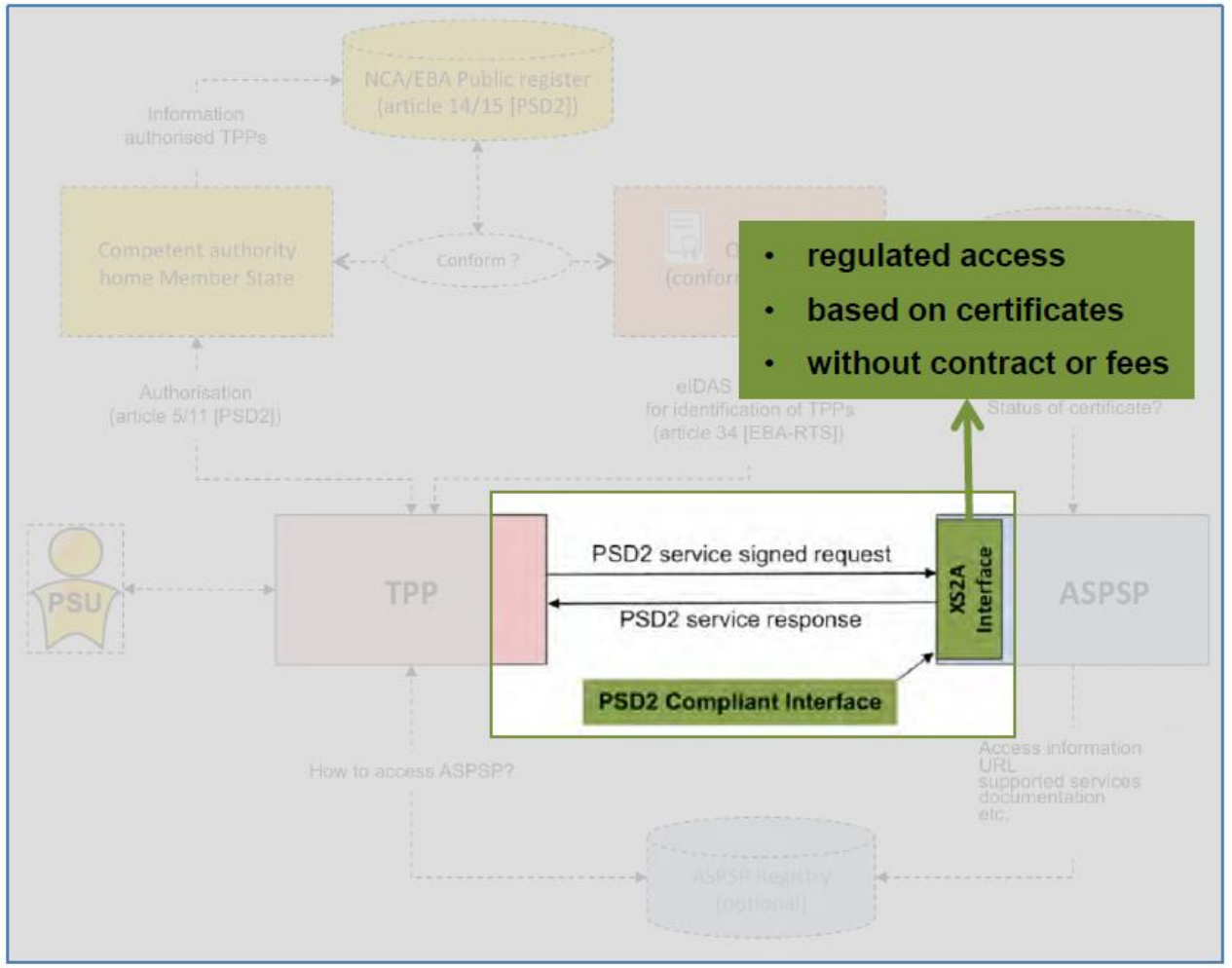


OPERATIONAL RULES

IMPLEMENTATION GUIDELINES

OPENAPI FILE

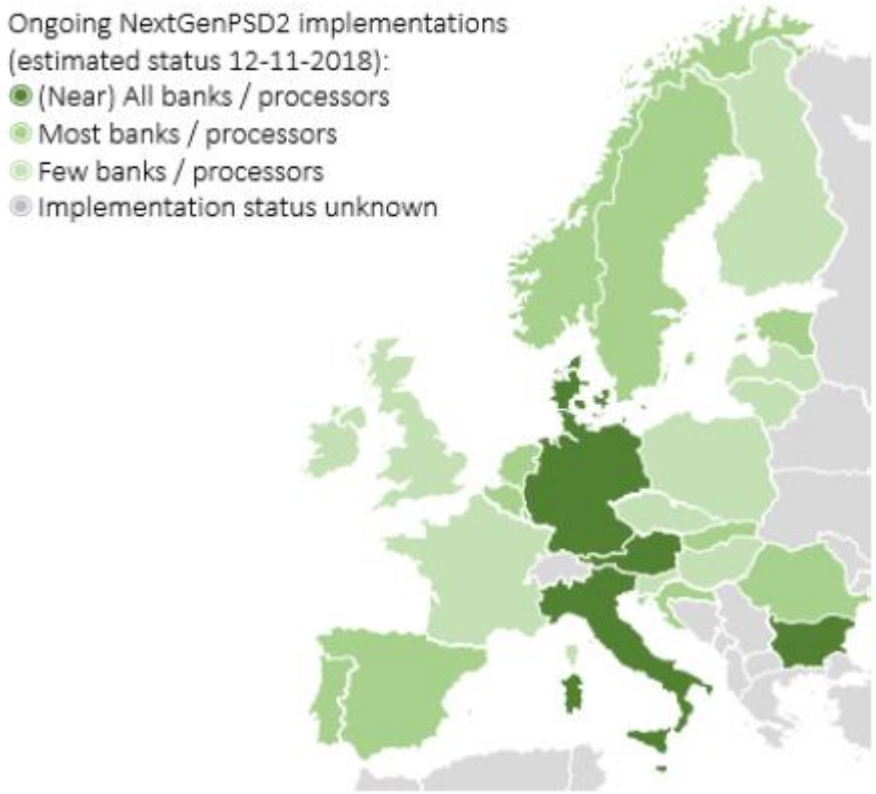
Scope of work



Deltagere


First Data
J.P.Morgan
THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE
Swedbank
BITS
DNB
Banking & Payments Federation Ireland
nets
Danske Bank
FINANCE LATVIA ASSOCIATION
mastercard
PAN-NORDIC CARD ASSOCIATION
SDC
VISA
bankdata
HOLVI
SIA
SEB
equensWorldline
Dutch Payments Association
Deutsche Bank
trionis
N26
bankart
Bancontact
SIX
SOCIETE GENERALE
Payment Services Austria
stet
RAIFFEISEN
ERSTE
bankenverband
Raiffeisen Bank International
SIBS
Liber bank
UniCredit
BORICA
Redsys
DZ BANK
credorax
PRETA
Postbank
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken
EURO
nexi
© The Berlin Group
Updated: 18-03-2019

Hvilke APIer vil bli tatt i bruk i Europa?



Which "API standard" expected in which country?

Berlin Group	Open Banking	STET	Others	Adaptations?
X				YES
X			X	YES
X				unknown
X				unknown
X				NO
	X			unknown
X	X			YES
X				unknown
		X		NO
X				YES
X				unknown
X	X			likely
X				YES
X	X			likely
X		X		unknown
X				unknown
X				YES
X	X			YES
X				YES
			X	partly reusing BG
			X	unknown
X				YES
	X	X		unknown
18	6	3	3	

- Berlin Group expected in large majority (78%) of countries.
- Open Banking and STET not fully bound to the UK and France.

all ASPSPs expected to apply the API standard
most or some ASPSPs expected to apply the API standard
few ASPSPs expected to apply the API standard

- Many adaptations* being made by national banking communities.

* Adaptations: interface implementations with changes to the functional and/or technical specifications of the respective API standard.

Kilde ECB

Med hvilke APIer vil tredjeparter kunne nå banker i Norge?

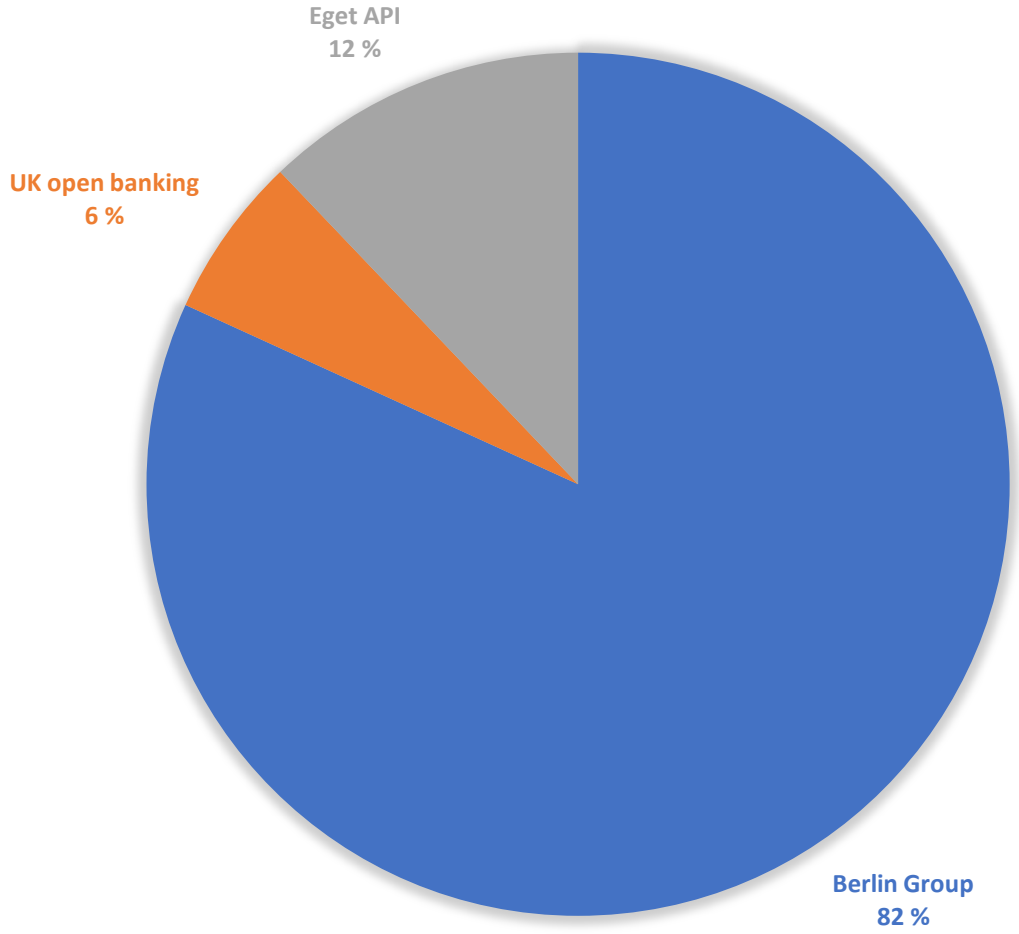
Ingen banker vil tilby dårlige API'er, og de fleste har valgt å standardisere på Berlin Group.

Figuren viser markedsandeler for de ulike API-standardene i Norge basert på relativ størrelse på banker som opererer i Norge.

Fakta:

- Så å si alle norske banker vil tilby PSD2 API basert på Berlin Group API-standarden.

- Enkelte utenlandske banker som opererer i Norge vil tilby API basert på andre standarder.



Prosess

- Definere og tydeliggjøre relevante PSD2, EBA RTS og eIDAS roller og artikler
- Definere og tydeliggjøre relevante use-cases med generelle dataflyter
- Sammenstilling med SEPA
- Definere relevante forretningsprosesser, datamodeller og transaksjoner
- Definere REST API metoder, endepunkter og stier
- Importere JSON/XML skjemaer i API modelleringsverktøy og legge til implementasjonsspesifikk informasjon

Støttede tjenester

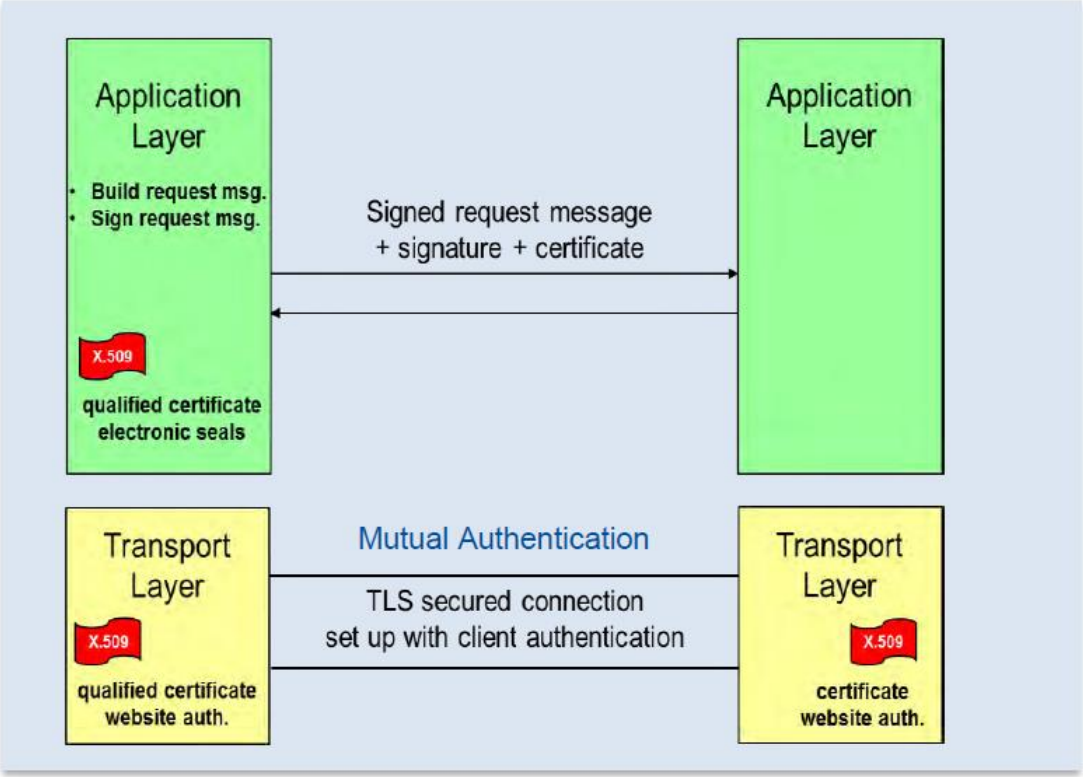
Use-case	Tjeneste	
Initiation of a single payment	PIS	
Initiation of a future dated single payment	PIS	Optional
Initiation of a bulk payment	PIS	Optional
Initiation of a recurring payment	PIS	Optional
Cancellation of payments	PIS	
Grouping transactions to signing baskets	PIS/AIS	Optional
Establish account information consents	AIS	
Get list of reachable accounts	AIS	optional
Get account details of the list of accessible accounts	AIS	
Get balances for a given account	AIS	
Get transaction information for a givent account	AIS	
Get a confirmation on the availability of funds	PIIS	

TPP identifisering

- PSD2 krav: TPP må identifisere seg for enhver tilgang til konto
- EBA RTS: TPP identifisering skal være basert på kvalifiserte eIDAS sertifikater
- Kvalifiserte sertifikater skal inneholde PSD2-spesifikke attributter
  - Referansenummer til TPP registrering hos tilsynsmyndighetene
  - Navn på tilsynsmyndighet
  - En eller flere roller som TPP er autorisert for å benytte
- ASPSP skal nekte en hver forespørsel hvis TPP ikke kan bli verifisert korrekt, eller hvis sertifikatet ikke inneholder korrekt rolle
- Det er ikke krav til at ASPSP skal ha et eIDAS sertifikat.

eSeal er en opsjon

- Alltid TPP identifisering på transportlaget
- TPP identifisering på applikasjonslaget kun hvis det er et krav fra ASPSP



Identifisering i transportlaget

- At the transport layer, the TPP is identified by means of the client authentication which is part of the TLS-connection setup between the TPP and the ASPSP.

- For this identification the TPP needs a qualified certificate for website authentication according to section 8 of [eIDAS].

- This certificate has to be compliant with the additional requirements defined by [RTS]. The profile of these certificates (QWAC profile) is specified by the technical specification [TS 119 495] of ETSI.

Clarification: If a TPP uses further technical service provider(s) to access the XS2A interface of an ASPSP the qualified certificate of the TPP must be used for the setup of the TLS-connection with the ASPSP. The certificate of a technical service provider(s) may not be used.

Identifisering i applikasjonslaget (Berlin Group)

- To identify the TPP at the application layer, the TPP has to sign all messages to be sent to the ASPSP.
- The electronic seal (i.e. the electronic signature) and the certificate of the TPP have to be sent to the ASPSP as part of the message.
- The electronic seal for a message shall be calculated based on the Internet standard for signing HTTP messages defined by the IETF Network Working Group.
- The TPP needs a qualified certificate for electronic seals according to section 5 of [eIDAS] for identification.
- This certificate has to be compliant with the additional requirements defined by [RTS]. The profile of these certificates (QSealC profile) is specified by the technical specification [TS 119 495] of ETSI.

Clarification: If a TPP uses further technical service provider(s) to implement its accesses to the XS2A interface of an ASPSP the electronic seal shall be generated by the TPP and the qualified certificate of the TPP shall be sent to the ASPSP. The certificate of a technical service provider(s) may not be used.

Signering i applikasjonslaget (Berlin Group)

- The ASPSP may require the TPP to sign request messages.
- This requirement shall be stated in the ASPSP documentation.
- The signature shall be included in the HTTP header as defined by [signHTTP], chapter 4.
- The electronic signature of the TPP has to be based on a qualified certificate for electronic seals.
- This qualified certificate has to be issued by a qualified trust service provider according to the eIDAS regulation [eIDAS].
- The content of the certificate has to be compliant with the requirements of [EBA-RTS]. The certificate of the TPP has to indicate all roles the TPP is authorised to use.

Attribute	Type	Condition	Description
Digest	String	Conditional	Is contained if and only if the "Signature" element is contained in the header of the request.
Signature	cp. Section 12	Conditional	A signature of the request by the TPP on application level. This might be mandated by ASPSP
TPPSignatureCertificate	String	Conditional	The certificate used for signing the request, in base64 encoding. Must be contained if a signature is contained, see above.

Signaturer

- **Signatures**

  When an ASPSP requires the TPP to send a digital signature as defined in [signHTTP], chapter 4 in his HTTP-Requests, the signature must obey the following requirements according or additional to [signHTTP], chapter 4.
- **"Digest" Header mandatory**

  When a TPP includes a signature as defined in [signHTTP], chapter 4, he also must include a "Digest" header as defined in [RFC3230]. The "Digest" Header contains a Hash of the message body. The only hash algorithms that may be used to calculate the Digest within the context of this specification are SHA-256 and SHA-512 as defined in [RFC5843].
- **Requirements on the "Signature" Header**

  As defined in [signHTTP], chapter 4, a "Signature" header must be present. The structure of a "Signature" header is defined in [signHTTP], chapter 4.1, the following table lists the requirements on the "Signature" header from [signHTTP] and additional requirements specific to the PSD2-Interface.

Eksempel

So using signature algorithm rsa-sha256 the signed request of the TPP will be

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Type:           application/json
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address:         192.168.8.78
PSU-ID:                 PSU-1234
PSU-User-Agent:          Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
TPP-Redirect-URI:       https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&
code_Cchallenge_Mmethod="S256"
Date:                   Sun, 06 Aug 2017 15:02:37 GMT
Digest:                 SHA-
256=ZuYiOtZkVxhjWmwTO5lOpsPevUNMezvk6dfb6fVhebM=
Signature:              keyId="SN=9FA1,CA=D-TRUST%20CA%202-1%202015,O=D-
Trust%20GmbH,C=DE",algorithm="rsa-sha256",
   headers="Digest X-Request-ID PSU-ID TPP-Redirect-URI Date",
   signature="Base64(RSA-SHA256(signing string))"
TPP-Signature-Certificate: TPP's_eIDAS_Certificate

{
   "instructedAmount": {"currency": "EUR", "amount": "123"},
   "debtorAccount": { "iban": "DE23100100101234567 89"},
   "creditor": { "name": "Merchant123"},
   "creditorAccount": {"iban": "DE23100120020123456789"},
   "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

Where *signing string* is

```
digest: SHA-256=ZuYiOtZkVxhjWmwTO5lOpsPevUNMezvk6dfb6fVhebM=

x-request-id: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
psu-id: PSU-1234
tpp-redirect-uri:
     https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&code_Cchallenge_Mmethod="S2
56"
date: Sun, 06 Aug 2017 15:02:37 GMT
```

- Brynjel Johnsen
  - Fagsjef, Bits AS
  - brynjel.johnsen@bits.no