Open Banking Europe

Finanstilsynets seminar om Sikker kommunikasjon mellom betalingstjenestetilbydere
2.april 2019
Bent Bentsen

PSD2 requirements in combination with lack of guidelines, processes and tools from authorities create risks for banks

Authenticate third parties using **certificates**

→

Certificates do **not contain all information** required for authentication, e.g. passporting

Allow access to third parties with a **valid FSA authorization** only

→

Possible mismatch between FSA authorization and certificate status may result in **unauthorized access**

EBA provides a **TPP register** with information from all national FSAs

→

Register does not contain information on banks and is **only updated once a day** (at best)

Open Banking Europe objective is to reduce these risks

Innhold

- Om Open Banking Europe/Preta
- Hvorfor Open Banking Europe ?
- Hvorfor har DNB deltatt i arbeidet ?

Om Open Banking Europe

2016/2017:

ERPB Working Group on PIS peker på behov for en katalogtjeneste som kan vise oppdatert informasjon om TPP'ers autorisasjoner

Våren 2017:

Preta S.A.S. tar initiativ til å bygge en slik tjeneste, støttet av banker

Preta S.A.S.:

Et heleid datterselskap av **EBA Clearing**

Sommeren 2017:

Preta etablerer programmet ***Open Banking Europe***, fundet av banker. DNB blir deltager i programmet

Fase 1, 2017-2018:

- Analyse
- Spesifikasjon av tjenesten.
- Utvikle Proof of Concept

Fase 2, 2018-2019:

Operasjonalisere tjenesten

OPEN BANKING EUROPE OBE Participants

ASPSPs

SERVICE PROVIDERS

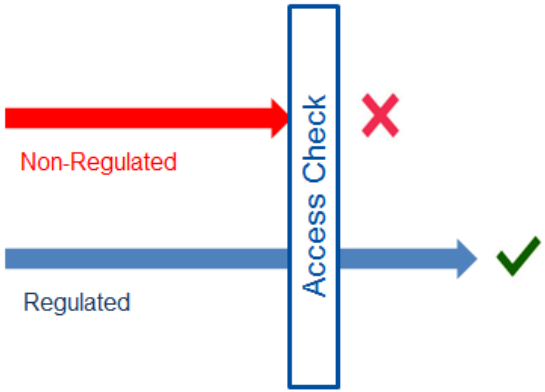
Preta S.A.S. is a wholly owned subsidiary of EBA CLEARING

Hvorfor Open Banking Europe ?

Granting **Access** to the Account

ASPSPs have the obligation to allow access to regulated entities, and block access to those that do not have access.

Failure to properly authenticate, leads to the risk of unauthorised transactions and subsequent claims under PSD2, or unauthorised data sharing and subsequent claims under GDPR.



COMMISSION DELEGATED REGULATION (EU) 2018/389

of 27 November 2017

supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [1], and in particular the second subparagraph of Article 98(4) thereof,

Whereas:

(1) Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

(2) As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments and operationally independent. In order to allow competent authorities to monitor the quality of the review of these measures, such reviews should be made available to them upon their request.

(3) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.

(4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

[1] OJ L 337, 23.12.2015, p. 35.

Article 30

General obligations for access interfaces

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements:

(a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;

Article 34

Certificates

1. For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation.

2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance with Annex III (c) or Annex IV (c) to Regulation (EU) No 910/2014 shall be the authorisation number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU of the European Parliament and of the Council [1] in accordance with Article 20 of that Directive.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

(a) the role of the payment service provider, which maybe one or more of the following:

  (i) account servicing;

  (ii) payment initiation;

  (iii) account information;

  (iv) issuing of card-based payment instruments;

(b) the name of the competent authorities where the payment service provider is registered.

How to check Access

- ASPSPs will use eIDAS certificates for the **Identification** of a party.
- ASPSPs will use the National registers for the **Authorisation** of a party, i.e. understanding if a party is regulated and what that party is authorised to do.

Difficulties in interpreting the national registers require a consolidated source of information, such as the Open Banking Europe Directory.

ERPB/2017/005
ERPB PIS 017-17
Version 1.0
24 May 2017

Euro Retail Payments Board (ERPB)

Report of the ERPB Working Group on Payment Initiation Services

ERPB Meeting 12 June 2017

ERPB PIS 017-17 Report ERPB WG on Payment Initiation Services 1/14

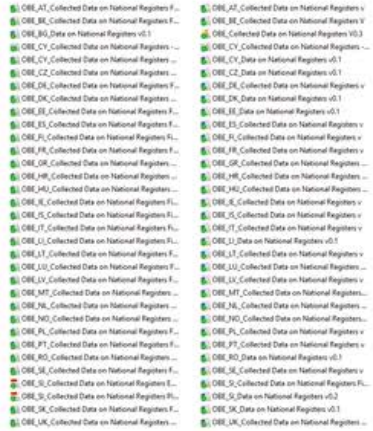
Maintaining Trust

- **The EBA register may not contain sufficient information for the purposes of identification**. In order to address this potential issue, the following two approaches were identified without any general consensus in the working group at this stage on the preferred direction:
  - Include extra information in the certificate with the need for a process to handle certificate revocations and for the renewal of certificates to reflect changes in the status of the PSP.
  - Use the certificate as a trusted key to a directory which will contain additional and up-to-date information that the ASPSPs and TPPs may need to interact with each other securely and effectively. **Ideally, this directory should be pan-European in scope, it should be machine-readable with proper service levels, and it should assume a sufficient level of liability to be trustworthy**. The working group believes that there is a need for the directory to include information not only about TPPs but also about ASPSPs.

Working together: Public Registers

Define

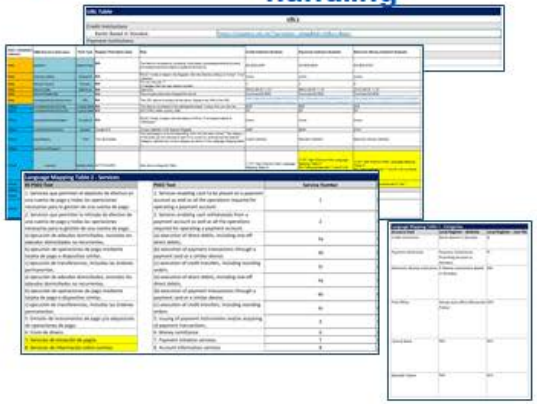
Engagements & Regulatory Analysis



…Audit of 31 registers, discussion with NCAs, leading 31 country books

Design

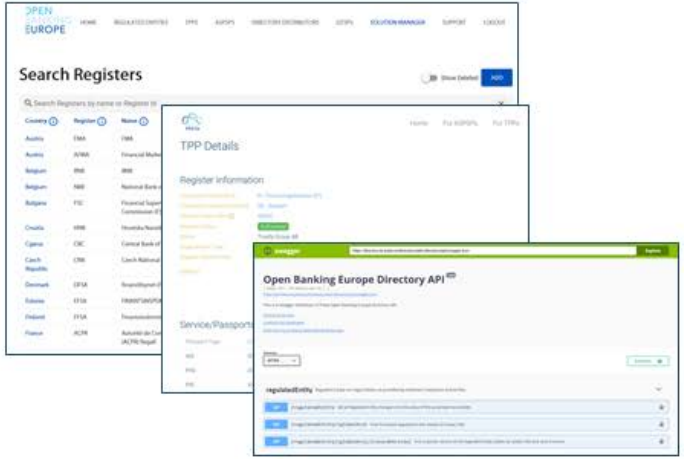
Creation of specifications for standardised NCA register handling



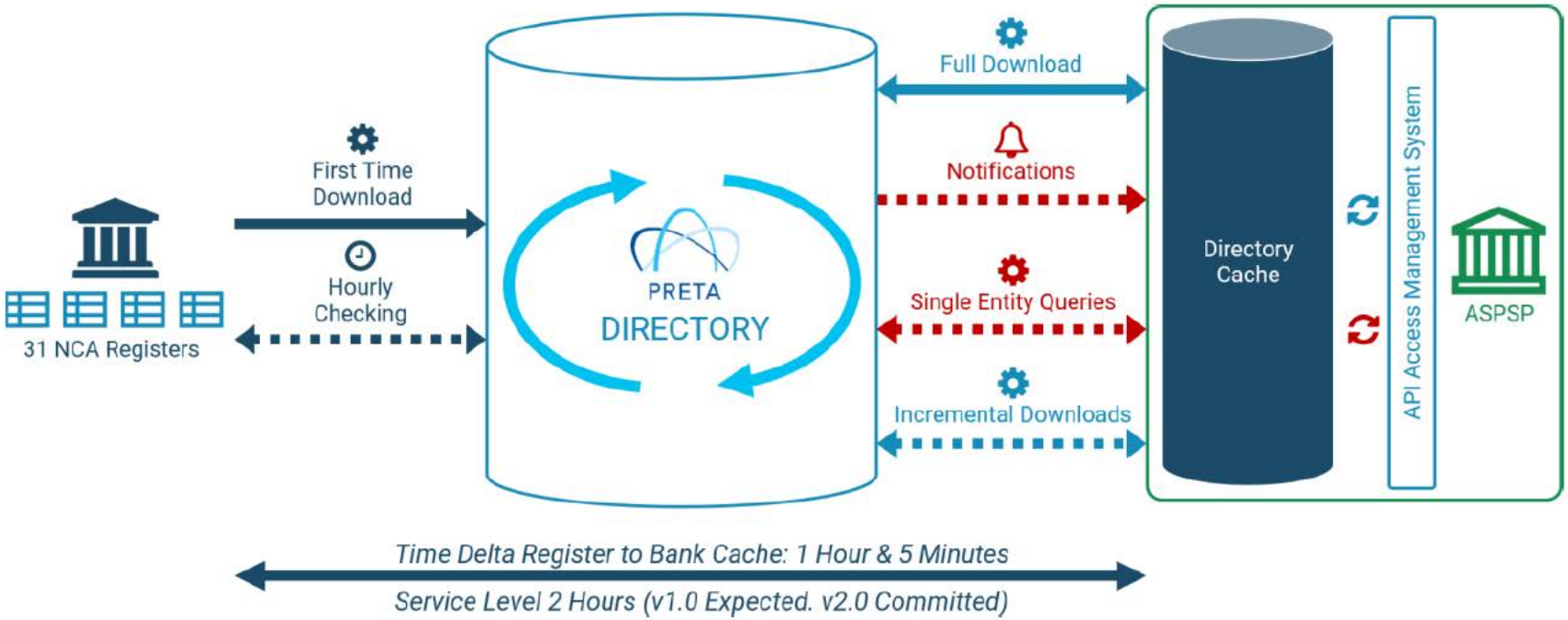
…detailed interface specifications describing how to take data from a national register and import it into the directory

Develop

Centralised, pan European directory



… working register import programs, secure api and notification system for participant and operational data.


First Time Download
Hourly Checking
31 NCA Registers
PRETA
DIRECTORY
Full Download
Notifications
Single Entity Queries
Incremental Downloads
Directory Cache
API Access Management System
ASPSP
Time Delta Register to Bank Cache: 1 Hour & 5 Minutes
Service Level 2 Hours (v1.0 Expected. v2.0 Committed)

Hvorfor ikke benytte EBA-registeret ?

- Bortsett fra at det ikke har vært tilgjengelig før nylig…. :
  - Det inneholder ikke opplysninger om banker
  - Det blir i beste fall oppdatert med opplysninger fra nasjonale registre én gang daglig
  - Det inneholder ikke G-URN (Global Unique Reference Number), som er den unike enhetsreferansen benyttet i eIDAS-sertifikatet.
  - Ingen mulighet for deltagerne i PSD2-økosystemet til å foredle informasjon om PSD2-aktører.
  - EBA tar overhodet ikke ansvar for informasjonen som ligger i registeret

Disclaimer

The present Register has been set up by the EBA solely on the basis of information provided by national competent authorities of the EEA Member States. Therefore, unlike national registers under PSD2, this Register has no legal significance and confers no rights in law. If an unauthorised institution is inadvertently included in the Register, its legal status is in no way altered; similarly, if an institution has inadvertently been omitted from the Register, the validity of its authorisation will not be affected.

With regard to any content in the field 'Name of the institutions' that describes the 'legal form' of the institution, it should be noted that such content is in most cases untranslatable and that any terminological similarities between two such entries are not to be taken to indicate that the legal status is the same.

The European Banking Authority is responsible only for the accurate reproduction of the information received by competent authorities for each natural or legal person included in the register, while responsibility for the accuracy of that information lies with the competent authorities at national level.

Dessuten…

- Det er ennå ingen som vet hvordan samspillet mellom tilsynsmyndigheter, sertifikatutstedere og sertifikatholdere kommer til å ta form:
  - Når og hvordan endringer i autorisasjoner blir formidlet fra tilsynsmyndighet til sertifikatutsteder
  - Når og hvordan sertifikatutstedere gjør endringer i forhold til utstedt sertifikat
  - Når og hvordan sertifikatholder tar nytt (oppdatert ?) sertifikat i bruk.

- **Det nasjonale registeret er «sannheten»**

Hvorfor har DNB deltatt i arbeidet?

If you want to go fast, travel alone.
If you want to go far, travel together.

- African proverb

PRETA

OPEN BANKING EUROPE

Trusted in EU

EBA Clearing & Preta MyBank have been delivering successfully with Banks in Europe for over 10 years.

Pan-EU Coverage

Preta has ability to reach all Countries in the EU today, through existing relationships, trust and operational branches.

Experts in the Market

Our SMEs are connected within EU for Interfaces, Regulatory Practices, and International Standards Organisations.

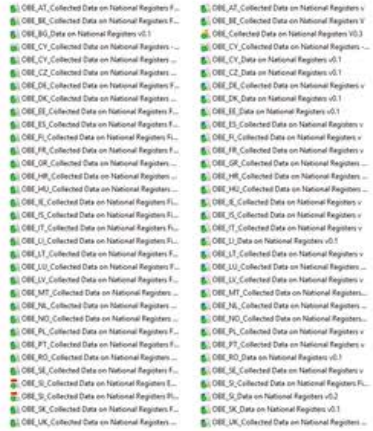
Community Led

Design Decisions made by consensus and priority, so Europe's stakeholders can agree on standards before we all build XS2A.

Working together: Public Registers

Define

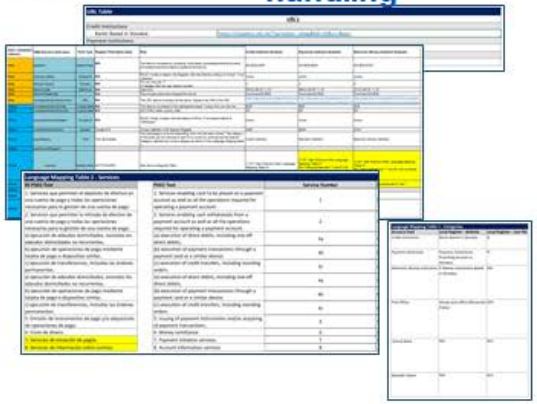
Engagements & Regulatory Analysis



…Audit of 31 registers, discussion with NCAs, leading 31 country books

Design

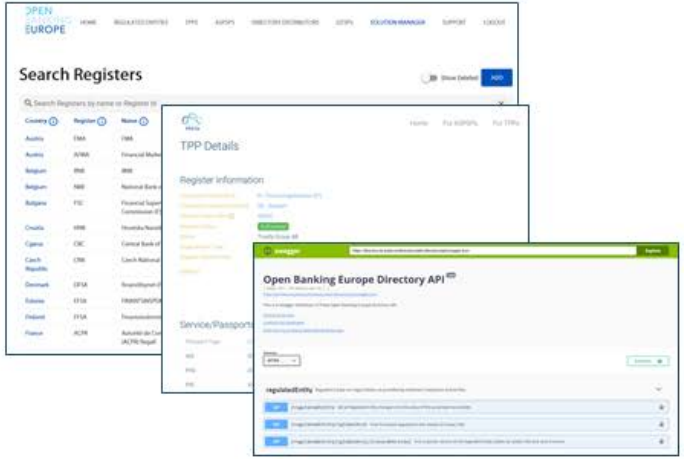
Creation of specifications for standardised NCA register handling



…detailed interface specifications describing how to take data from a national register and import it into the directory

Develop

Centralised, pan European directory



… working register import programs, secure api and notification system for participant and operational data.

Working together: eIDAS certificates

Define

Engagements & Regulatory Analysis

ETSI / ERPB PIS Experts PSD2 Workshop
Discussion Document on PSD2
Requirements for Qualified Certificate
Date: 10 Oct 2017

Introduction

Early discussion documents

Design

Design & Standardisation: Handbook & Miniguides

PRETA

PRETA Op

Security Model,
Certificates

Release

Status: V1.0 For Discussi

Classification: Closed Use

Copyright © 2017

This document is the prop
confidential.

This document is the prop
CLEARING. The information
or distributed without PRETA

ETSI TS 119 495 V0.0.0d (2017-11)

ETSI

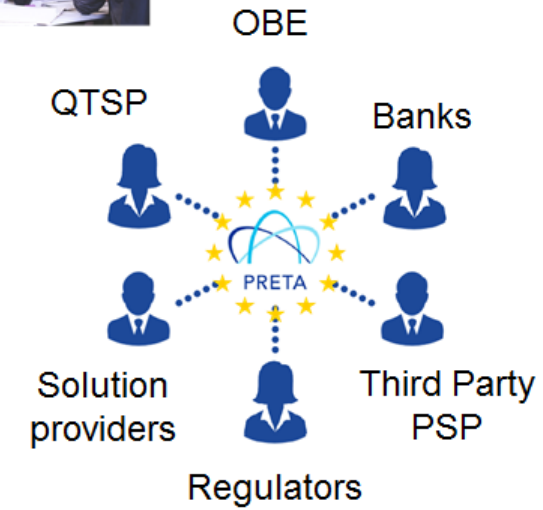
TECHNICAL SPECIFICATION

Electronic Signatures and Infrastructures (ESI);
Sector Specific Requirements;
Qualified Certificate Profiles and TSP Policy Requirements
under the payment services Directive 2015/2366/EU;

ETSI Technical Standard … TS 119 495

Develop

QTSP Engagement group



Regular meetings with PSD2 certificate issuers.

Working together: Other work streams

- Security considerations in the dedicated interface
- Understanding agents and outsourcing in PSD2 (four party models)
- Providing transparency on bank implementations
- Considerations around testing and conformance
- Monitoring live APIs
- Calling for help!

Sist, men ikke minst….

- Open Banking Europe/Preta =
  - Plattform for læring og forståelse
  - Tilgang til informasjon
  - Nettverksbygging og relasjoner

PSD2 requirements in combination with lack of guidelines, processes and tools from authorities create risks for banks

Authenticate third parties using **certificates**

→

Certificates do **not contain all information** required for authentication, e.g. passporting

Allow access to third parties with a **valid FSA authorization** only

→

Possible mismatch between FSA authorization and certificate status may result in **unauthorized access**

EBA provides a **TPP register** with information from all national FSAs

→

Register does not contain information on banks and is **only updated once a day** (at best)

Open Banking Europe objective is to reduce these risks


DNB