

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)



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



BANKING OBE Participants

ASPSPs

































HSBC (X)

















Swedbank @











SERVICE PROVIDERS

























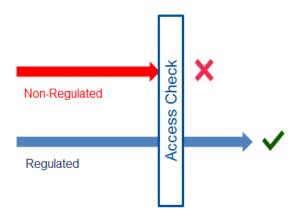
Hvorfor Open Banking Europe?



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.



13.3.2018	EN	Official Journal of the European Union	L 69/23

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,

Haring regard to Directive (EU) 2015/1366 of the European Parliament and of the Council of 25 November 2015 on payment service in the internal market, amending Directives 2002/45/EC, 2009/110/EC and 2013/39/ED Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (), and in particular the second subparagraph of

Whereas

- (1) Psyment cervices 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 ritis of fistual. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalized security residentials that were lost, stone, or misappopriated and should also ensure that the payment service user is the legislamst user and therefore is giving content for the transfer of funds and access to its account information through a normal use of the personalized security credentials. Furthermore, it is necessary to pecify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment around conformation or carrier out any action through a remote channel which may imply a risk of payment fusion of other abuse, by requiring the generation of an authentication code which should be relational against the risk of being forged in its entirety or by disclosure of any of the element 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, toth review 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 payer specified by the payer when inhitating the transaction.
- (4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirement. To remain technologiscally neutral a specific technology for the implementation of authentication codes should be based on solutions such as generating and validating one-time parawords, digital signatures or other cryptographically underpined validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

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.

⁽¹⁾ OJL 337, 23.12.2015, p. 35.

How to check Access

- ASPSPs will use <u>elDAS</u> 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 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

OBE,AT, Collected Data on National Registers F	6) DBL,AT, Collected Data on National Registers in
OBE_SE_Collected Data on National Registers F	6 ORE SE Collected Data on National Registers V
OSE_BG_Data on National Registers v0.1	. ORK, Collected Data on National Registers VO.3
OBE_CV_Collected Data on National Registers	M OBIL CV_Collected Data on National Registers
CBE_CV_Collected Data on National Registers	B) ORL CY, Date on National Registers v0.1
OBE_CZ_Collected Data on National Registers	6 OBE CZ Data on National Registers v0.1
OBE_DE_Collected Data on National Registers F	6 DEE DE Collected Data on National Registers o
OBE DK Collected Data on National Registers	SCORE DK Date on National Registers v0.1
OBE_EE_Collected Data on National Registers F	S. DEE, EE, Date on National Registers v0.1
GBE_ES_Collected Data on National Registers F	6 ORE 15 Collected Date on National Registers v
CRE_FL_Collected Data on National Registers FL	6 DREF, Collected Date on National Registers v
OBE_FR_Collected Data on National Registers F	6 OBL FR, Collected Date on National Registers v
OBE OR Collected that on National Registers	6 Offi GR Collected Data on National Registers
OBE_HR, Collected Data on National Registers	6 OSE, HR, Collected Data on National Registers.
CBE_HU_Collected Data on National Registers	6 ORE HU Collected Data on National Registers
GBE_IE_Collected Data on National Registers FL	B. DBE, E. Collected Date on National Registers v
ORE, IS, Collected Data on National Registers FL	6 DBE IS Collected Data on National Registers v
CBE_IT_Collected Data on National Registers Fi	6. ORE IT Collected Data on National Registers v
OBE_U_Collected Data on National Registers FL.	6 OSE 1) Data on National Registers v0.1
OBE_LT_Collected Outs on National Registers F	5. OSE LT Collected Data on National Registers v
OBE_UU_Collected Data on National Registers F	6 OBE LU Collected Data on National Registers .
OBE_LV_Collected Creta on National Registers F	6 Off LV Collected Data on National Registers v
CGE_MT_Collected Date on National Registers	S. DBE, MT, Collected Data on National Registers.
OSE, NE, Collected Data on National Registers	6. DEE No. Collected Data on National Registers .
CBE_NO_Collected Data on National Registers	6 OBE, NO, Collected Date on National Registers.
OBE_PL_Collected Data on National Registers F	S. OSE, PL. Collected Outs on National Registers v
OBE, PT, Collected Data on National Registers F	6, OSE 97, Collected Data on National Registers of
OBE_RO_Collected Data on National Registers	6 DBE RO Data on National Registers v0.1
OBE, SE, Collected Data on National Registers F	6 OBE SE Collected Data on National Registers v
OBE_SL Collected Data on National Registers E	6 ORE S. Collected Date on National Registers Fi
CBE_SI_Collected Data on National Registers Pl	6 OEE, St. Data on National Registers v0.2
	and management of the contract

...Audit of 31 registers, discussion with NCAs, leading 31 country books Design



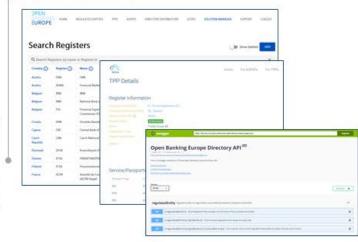
Creation of specifications for standardised NCA register handling

		K RANG							
		eh)							
		Section of the	197 (197						-
		Facility Second C. Str.		RIALADUS	والمشتنا الوثب				
	100	_					_		
THE REAL PROPERTY.	min nya	Name and Address at the	Pro .	Accessed to	Party of the Party	_			
The Part of the Pa	SM:	-	Name and the second	Name .	-	-	2000		
000.00		10.	Paris 1		jum .	jum.			
Married		-	CARL THE RESIDENCE	L.	L	the same			
THE REAL PROPERTY.	100	G -	Service teams of	20254	20112	202010			
		-	The Residence of the Control of the			277			
-		0	TO SEE COME OF PERSONS AND PARTY OF SEC.		-	-			
	-	4.5	the tell on the second of the second	-	-	-			
	100	Sect	DOM: THE SECOND CO.	ie	-	bc .			
_	100	matrice.	EXPERIMENT REPORTS AND ADDRESS.	and the same	Section 1	-			
	_			_					
		-	NAME OF TAXABLE PARTY.		the same	-			
_				Honey Service	Edward and a				
Large age Mapping	Fielde 2	Services							
es risks have	200	SASSESSED FOR THE PARTY OF THE	PRESIDE LANGUAGE CONTRACTOR		Service Sumber	-			
I fertilett an jamen		make the effectively pain	2. Services enqueling count for tax phonons on a			- 1			
solid transfer (Archellio E. Ja			durant as end in all the operations traus	methr	4	- 1			
reconstruction parts, for process the construction for angel-			payment a control or control	2.7					
J. briskist das protitto is stitulo di efection de			2. Service-andreas and settlement from						
and rushing throughty for			payment account to self-at all the operation		411	- 15	-	Salts I Adaptive	
remarks period drive			inspired to specify, control school.				State of the last		- merber
complete directions in			men anni		No.	. 14		A-1-	- 3
Name of the Parties of			- the administration of appropriate communities often	naths.					
hearts or page 4. Rose			payment and in a print deeper				-	Angerry (citations) Transfer, in cost or	
CHEMINA STRANGO	-	halls in bridge.	In emission of youth tracken, including	monthly .	- 6	1.0	1	Access .	
performance			(MATE)			-	-	Colonia Colonia	
di igeraction de sebastos directionistes, promote des tallendos directificados na recurrentes.			In execute of start mint, naming to describe		**	- 1		681776	
No concentration of the page of the later of		regio de alterna	the section of physical triangement than	matter .		7.4			
NOTE RUNG! Lifting			protect areas contactives.				No. of Co.	Marin Bridge	
Copiuson in creation		and in case	SC encycles of codd encycles, recoding territors	-		- 1		Anne .	
to Gentle de Sentimore	200		It many of present includes and in						
dispersional Parison		the beautiful to	of secret forcedors.	-		- 7	1		
			It Work terriform						
in the control of the control			25 Applicable billiagettes automos-		1	- 1	and sec	-	
Name of Street,	200		The state of the s						
	22	-	A Kinet Honda arms	_		-	1		
The second	22	-	A house offenday array						
1 March & Committee	-	_	A functional areas						
Name of Street,			A Named offernation service				_		Ų.

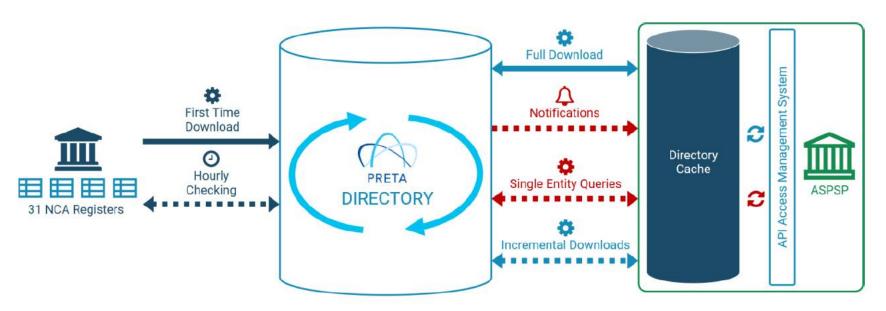
...detailed interface specifications describing how to take data from a national register and import it into the directory Develop



Centralised, pan European directory



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



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?



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

OBE,AT, Collected Data on National Registers F	6 DBE,AT, Collected Data on National Registers
OBE_SK_Collected Data on National Registers F	6 ORE SE Collected Data on National Registers
OBE_BG_Data on National Registers vC.1	3. OBE, Collected Data on National Registers VO
OBE_CY_Collected Data on National Registers	M OBE_CV_Collected Data on National Registers
CBE_CY_Collected Data on National Registers	6) OSE, CY, Date on National Registers v0.1
OBE_CZ_Collected Data on National Registers	6 OBE_C2_Data on National Registers v6.1
OBE_DE_Collected Data on National Registers F	6. DEE_DE_Collected Data on National Registers
ORE DIC Collected Data on National Registers	SCORE DK Date on National Registers v0.1
OBE SE Collected Data on National Registers F	S. DEE, EE Date on National Registers v0.1
OBE_ES_Collected Data on National Registers F	6 ORE IS Collected Data on National Registers
ORE FL Collected Data on National Registers FL.	6 DREP, Collected Data on National Registers
OBE_FR_Collected Data on National Registers F	6 OBE, FR, Collected Date on National Registers
OBE OR Collected that an National Registers	6. OBIL SR, Collected Data on National Registers
OBE_HR_Collected Data on National Registers	6 OSE, HR, Collected Data on National Registers
085_HU_Collected Outs on National Registers	6 ORE HU Collected Data on National Register
OSE_IE_Collected Data on National Registers FL	S. OBE, E. Collected Data on National Registers
OBE_IS_Collected Data on National Registers FL	6 OBE IS Collected Data on National Registers
OBE, IT, Collected Date on National Registers Fi	6. ORE, IT, Collected Data on National Registers
OBE_U_Collected Data on National Registers Fl	6 OSE 1) Date on National Registers v0.1
OBE_LT_Collected Data on National Registers F	S. OBE, LT, Collected Data on National Registers
OBE_UU_Collected Data on National Registers F	6 OBE LU Collected Data on National Register
OBE_LV_Collected Data on National Registers F	6 ORE, LY_Collected Data on National Registers
OSE_MT_Collected Date on National Registers	S. DBE_MT_Collected Data on National Register
OBE,NL, Collected Data on National Registers	6. OSE Nr. Collected Data on National Registers
OSE_NO_Collected Data on National Registers	6 Obt. NO_Collected Date on National Register
OBE_PL_Collected Data on National Registers F	S. OSE, Ps., Collected Outs on National Registers
OBE_PT_Collected Data on National Registers F	5, OSE 97, Collected Data on National Registers
OBE_RO_Collected Data on National Registers	6 DBC RO Data on National Registers v0.1
OBE_SE_Collected Data on National Registers F	6 OBE SE Collected Data on National Registers
OBE_SL_Collected Data on National Registers E	6 Off, S. Collected Data on National Registers
CBE, St. Collected Data on National Registers PL.	6 OSE, St. Data on National Registers v0.2

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

ORE SK Collected Data on National Registers F... 6 ORE SK Data on National Registers VI.1

Design



Creation of specifications for standardised NCA register handling

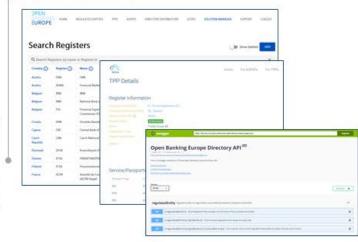
		K RANG							
		eh)							
		Section of the	10.7 (1)						-
		Facility Second St. To.		RIALAGOUS	والمشتنا الوثب				
	100	_					_		
THE REAL PROPERTY.	min nya	Name and Address at the	Pro .	Accessed to	Party or other Party.	_			
The Part of the Pa	SM:	-	Name and the second	Name .	-	-	2000		
000.00		10.	Paris 1		jum .	jum.			
Married		-	CARL THE RESIDENCE	L.	L	-			
THE REAL PROPERTY.	100	G -	Service teams of	20254	20112	202010			
		-	The Residence of the Control of the			277			
-		0	TO SEE COME OF PERSONS AND PARTY OF SEC.		-	-			
	-	4.5	the tell on the second of the second	-	-	-			
	100	Sect	DOM: THE SECOND CO.	ie	-	bc .			
_	100	matrice.	EXPERIMENT ENGINEERING SERVICE	and the same	Section 1	-			
	_			_					
		-	NAME OF TAXABLE PARTY.		the same	-			
_				Hone ben-in	Edward and a				
Large age Mapping	Fielde 2	Services							
es risks have	200	SASSESSED FOR THE PARTY OF THE	PRESIDE LANGUAGE CONTRACTOR		Service Sumber	-			
I fertilett an jamen		make the effectively pain	2. Services enqueling count for tax phonons on a			- 1			
solid transfer (Archellio E. Ja			durant as end in all the operations traus	methr	4	- 1			
reconstruction parts, for process the construction for angel-			payment a control or control	2.7					
J. briskist das protitto is stitulo di efection de			2. Service-andreas and administrative from						
and rushing throughty for			payment account to self-at all the operation		411	- 15	-	Salts I Adaptive	
remarks period drive			inspired to specify, control school.				State of the last		- merber
complete directions in			men anni		No.	. 14		A-1-	- 3
Name of the Parties of			- the administration of appropriate communities often	naths.					
hearts or page 4. Rose			payment and at a print about				-	Angerry (citations) Transfer, in cost or	
CHEMINA STRANGO	-	halls in bridge.	In emission of youth tracken, including	monthly .	- 6	1.0		Access .	
performance			(MATE)			-	-	Colonia Colonia	
di igeraction de sebastos directionistes, promote des tallendos directificados na recurrentes.			In execute of start mint, naming to describe		**	- 1		681776	
No concentration of the page of the later of		reproduction reproduction	the section of physical triangement than	matter .		7.4			
NOTE RUNG! Lifting			protect areas contactives.				No. of Co.	Marin Bridge	
Copiuson in creation		and in case	SC encycles of codd encycles, recoding territors	-		- 1		Anne.	
to Gentle de Sentimore	200		It many of present includes and in						
dispersional Parison		the beautiful to	of secret forcedors.	-		- 7	1		
			It Work terriform						
in the control of the control			25 Applicable billioning advances.		1	- 1	and sec	-	
Name of Street,	200		The state of the s						
	22	-	A Kinet Honda arms	_		-	1		
The second	22	-	A house offenday array						
1 March & Committee	-	_	A functional areas						
Name of Street,			A Named offernation service				_		Ų.

...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.



SANKING Working together: eIDAS certificates



Define



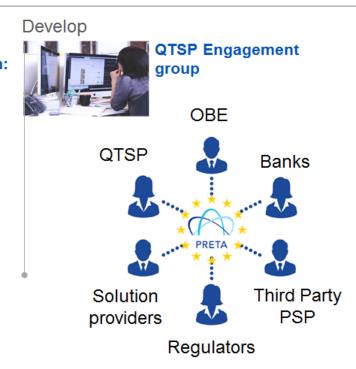
Engagements & Regulatory Analysis



Early discussion documents



ETSI Technical Standard ... TS 119 495



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)

DNB