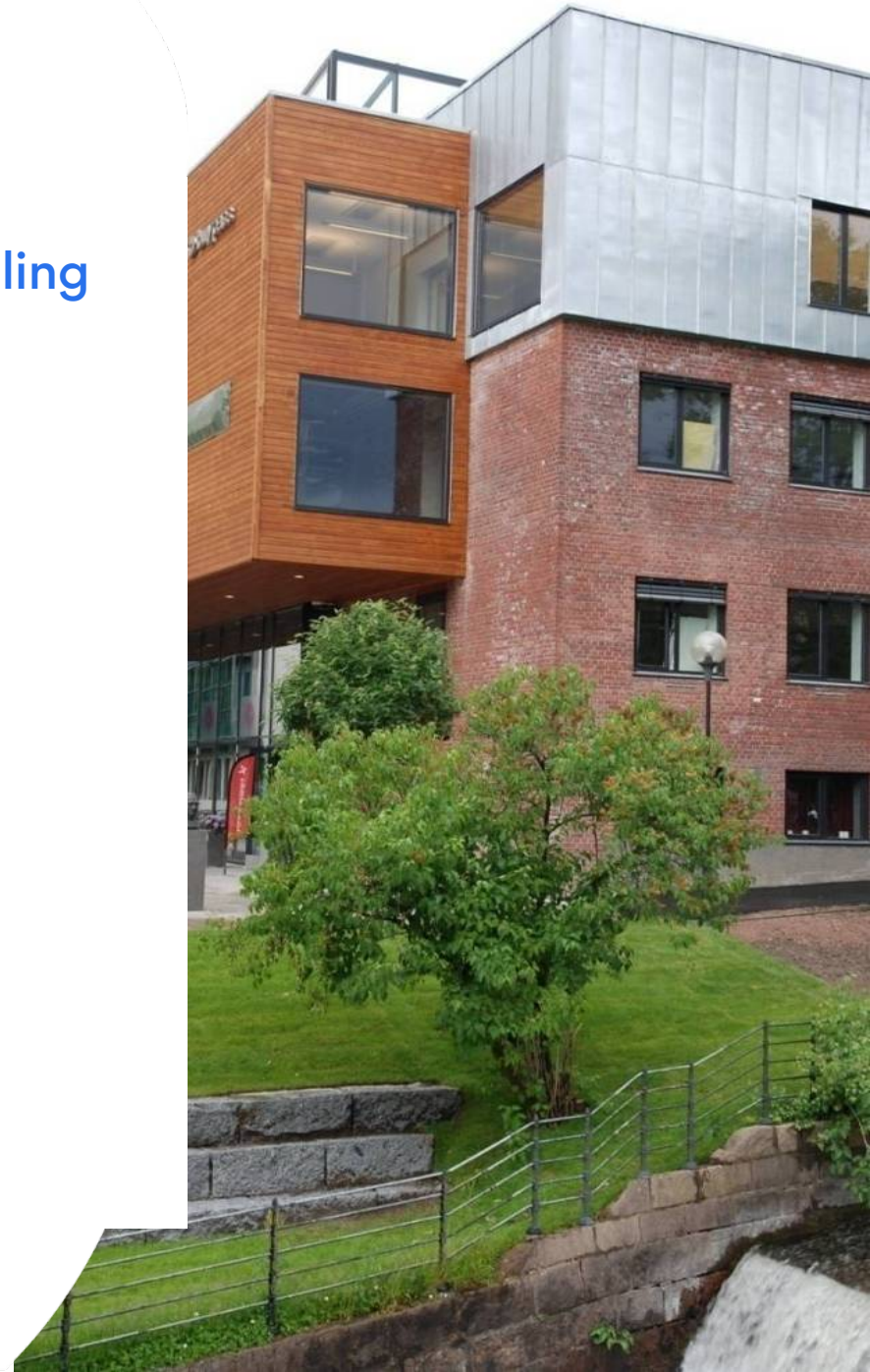
PSD2 og eIDAS-sertifikater

Seminar Finanstilsynet 2.april 2019

buypass

Fakta om Buypass

- Norsk selskap eid av EVRY og Norsk Tipping
- Et løsningshus for elektronisk identitet, signatur og betaling
  - 2,8 mill sluttbrukere
  - 36 milliarder NOK i formidlet omsetning (2018)
  - Mer enn 45 millioner transaksjoner pr måned (2018)
  - Utsteder av digitale sertifikater for personer og virksomheter
  - Leverandør i alle offentlige prosjekter
- TLS/SSL
  - Rot CA og utsteder av TLS/SSL sertifikater
  - Medlem av CA/Browser Forum
- Sertifisert for informasjonssikkerhet og kvalitet
  - ISO/IEC 27001 and ISO/IEC 9001
  - PCI DSS
  - ETSI EN 319 411 (digitale sertifikater)
- QTSP i hht eIDAS



Regulatory Technical Standard (RTS)

13.3.2018 EN

COMMIS

supplementing Directive (EU
regard to regulatory technic
s

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Fun

Having regard to Directive (EU) 2015/
payment services in the internal m
Regulation (EU) No 1093/2010, and
Article 98(4) thereof,

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.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

buypass

eIDAS-forordningen

Regulation (EU) No 910/2014 of 23 July 2014

for electro

and

LOVDATA

Søk etter lover, forskrifter, dommer og stortingsvedtak

Rettskilder

- Lover
- Stortingsvedtak
- Sentrale forskrifter
- Lokale forskrifter
- Norsk Lovtidend
- Norges traktater
- Dommer
- Statens personalhåndbok
- Oversatte lover / Translated Acts

Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektr...

Innholdsfortegnelse

Gå til opprinnelig kunngjort versjon

Lov om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester)

Dato	LOV-2018-06-15-44
Departement	Nærings- og fiskeridepartementet
Ikrafttredelse	15.06.2018
Endrer	LOV-2001-06-15-81
Kunngjort	15.06.2018
Korttittel	Lov om elektroniske tillitstjenester

Jf. *tidligere* lov 15. juni 2001 nr. 81. – Jf. EØS-avtalen vedlegg XI nr. 5l (forordning (EU) nr. 910/2014).

§ 1. *eID og elektroniske tillitstjenester i EØS*

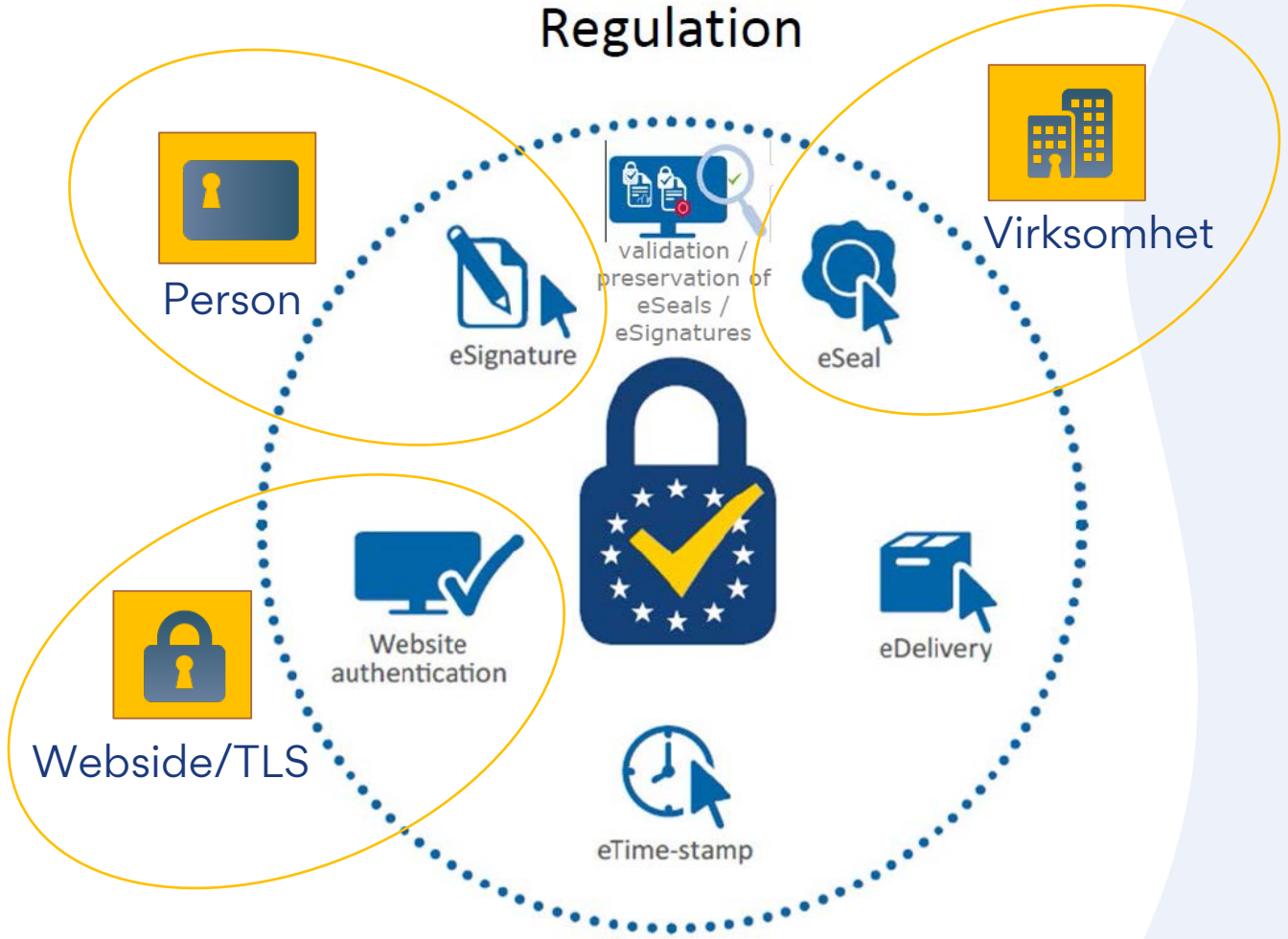
buypass

eIDAS forordning

Directive
1999/93/EC

Person

eIDAS
Regulation



buypass

Hva er et sertifikat?

- Elektronisk dokument på et standardisert format som knytter en offentlig nøkkel til en identitet (person, virksomhet, system etc)
- Utstedes av sertifikatutsteder (Certificate Authority) som er ansvarlig for å verifisere sertifikatinnehavers identitet og annen informasjon som skal inn i sertifikatet
- Et sertifikat inneholder blant annet:
  - Gyldighetsperiode
  - Sertifikatinnehavers identitet
  - Offentlig nøkkel - som knyttes til sertifikatinnehaver
  - Sertifikatutsteder (for eksempel Buypass Class 3 CA 3)
  - Sertifikatutsteders digitale signatur
- Sertifikatet er signert av sertifikatutsteder som med dette ”går god for” innholdet i sertifikatet

buypass

Hva er et kvalifisert sertifikat?

Buypass CA

- Et sertifikat som er regulert av eIDAS-forordningen
  - Skal øke tilliten til elektroniske transaksjoner i EU (og EØS)
  - eIDAS-forordningen stiller krav til kvalifiserte sertifikater og utstedere av slike (QTSP)
- Et kvalifisert sertifikat er et sertifikat som har en juridisk forankring og som tilfredsstiller tekniske og sikkerhetsmessige krav
- Kravene til kvalifiserte sertifikater er i samsvar med industristandarder og gjeldende praksis, men forsterket for å sikre tilliten

QUALIFIED
TRUST SERVICE
PROVIDER
compliant with eIDAS

buypass

eIDAS forordningen – artikkel 24

Article 24

Requirements for qualified trust service providers

1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

(a) by the physical presence of the natural person or of an authorised representative of the legal person; or

(b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or

(c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

(d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

buypass

eIDAS og tillitslister

European Commission: List of Trusted List information as notified by Member States

NORGE (NORWAY) : Trusted List

Nasjonal kommunikasjons-myndighet

QUALIFIED TRUST SERVICE PROVIDER compliant with eIDAS

2 - TSP: Buypass AS

TSPName

Name	[en]	Buypass AS
Name	[no]	Buypass AS

ElectronicAddress

URI	mailto:post@buypass.no

TSPInformationURI

URI	[en]	http://www.buypass.com/home/support/ca-documentatic
URI	[no]	http://www.buypass.no/bedrift/kundeservice/dokumenta

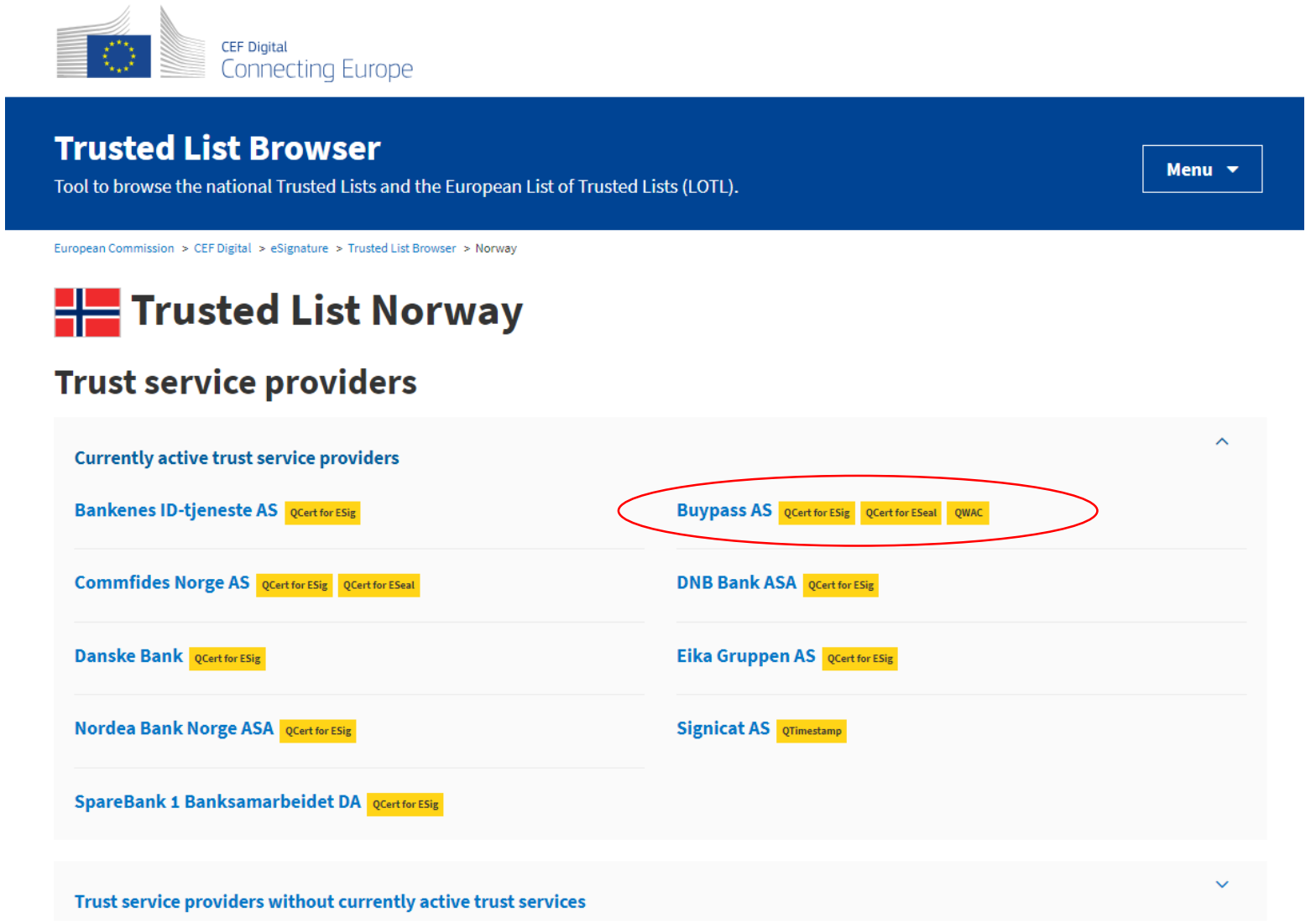
2.1 - Service: Certification Authority issuing Qualified Certificates

ServiceTypeIdentifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC

ServiceName

buypass

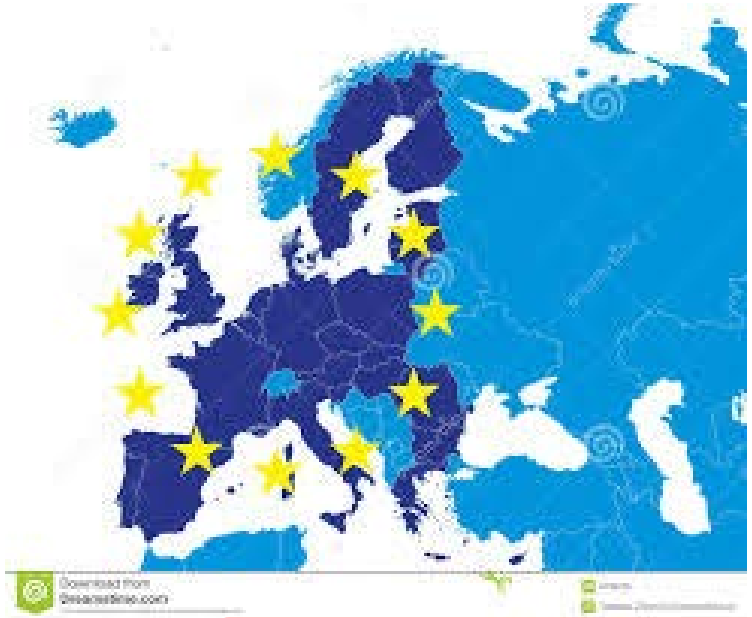
Den norske tillitslisten

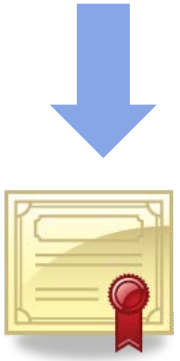


Buypass CA – QTSP i hht eIDAS

Buypass CA

QUALIFIED TRUST SERVICE PROVIDER compliant with eIDAS





QC eSignature

QC eSeal

QWAC

buypass

Kvalifiserte sertifikater for PSD2

PSD2 QWAC

PSD2 QC eSeal

QWAC

QC eSeal

CA/BROWSER FORUM

Extended Validation (EV)

Virksomhets-sertifikater

buypass

Kvalifiserte sertifikater for PSD2

ETSI TS 119 495 V1.3.1 (2019-03)

Electronic Signatures and Infr
Sector Specific Requ
Qualified Certificate Profiles and TS
under the payment services Dire

buypass

To ulike typer sertifikater

For the purpose of identification PSPs shall rely on

QUALIFIED CERTIFICATE FOR ELECTRONIC SEAL

Issued to: Payment Service Provider
Issued by: Qualified Trust Service
Valid from: 2018/03/20 **to:** 2020/03/20

Qualified Certificates for Seals (QCSEALs)
EU 910/2014 (eIDAS)
Annex III

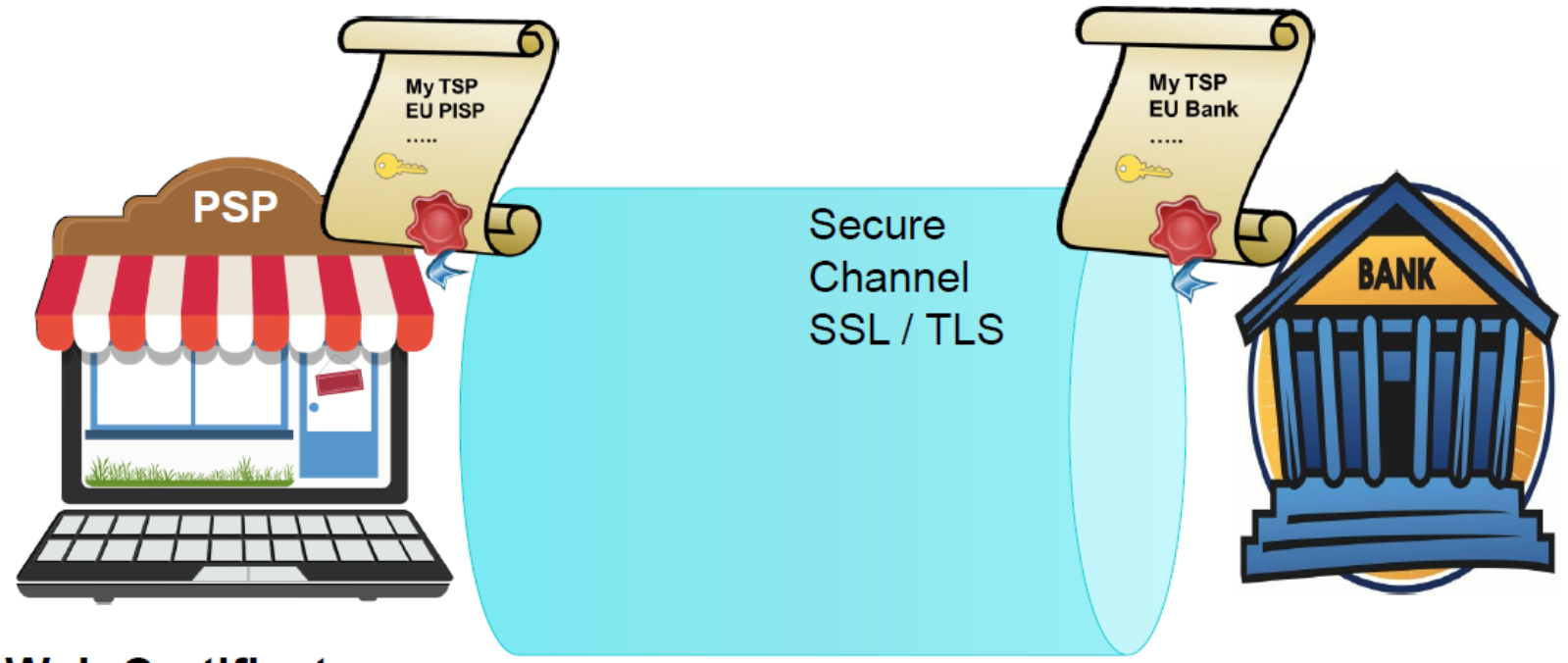
QUALIFIED WEBSITE CERTIFICATE

Issued to: Payment Service Provider
Issued by: Qualified Trust Service
Valid from: 2018/03/20 **to:** 2020/03/20

Qualified Website Certificates (QWACs):
EU 910/2014 (eIDAS)
Annex IV

buypass

Kvalifisert TLS-sertifikat - QWAC

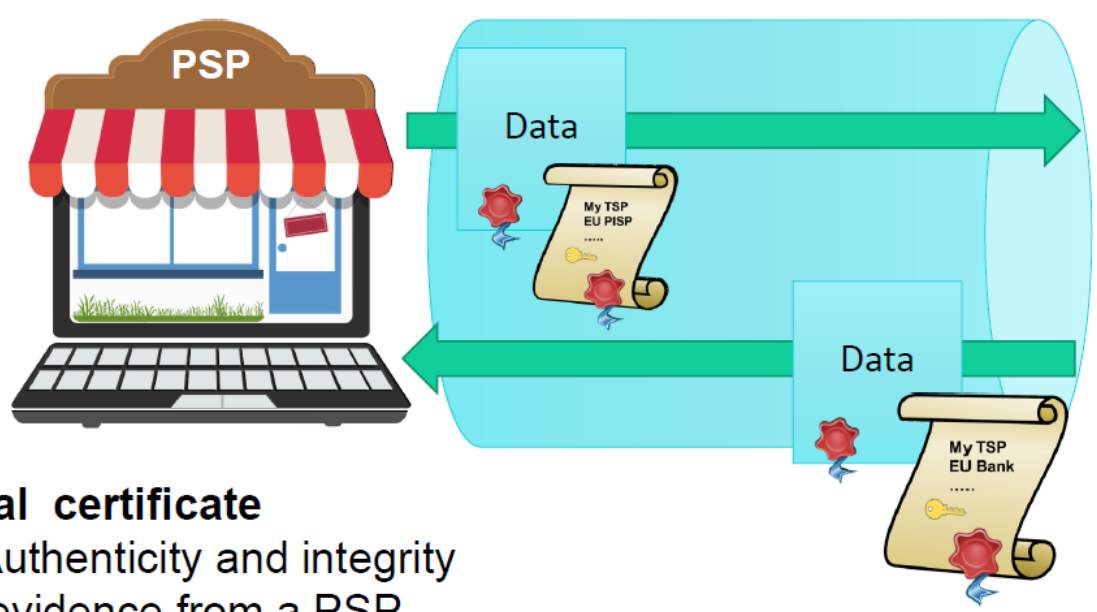


Web Certificate
- Authenticate PSP
  (bound to channel)

Web Certificate
- Authenticate Bank
- Set up secure channel

buypass

Kvalifisert sertifikat for elektronisk segl (QC eSeal - QSealC)



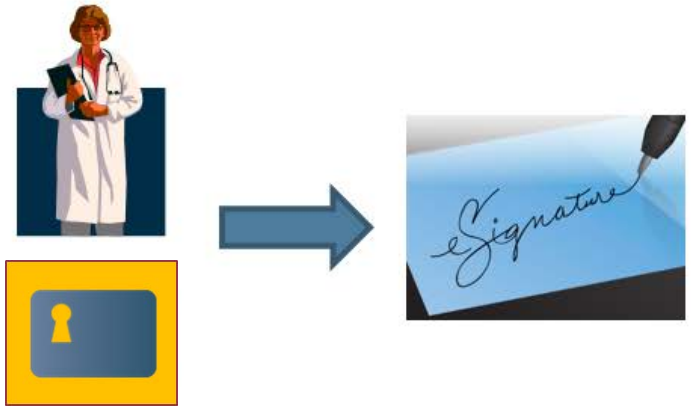
Seal certificate
- Authenticity and integrity of evidence from a PSP

Seal certificate
- Authenticity and integrity of evidence from a bank

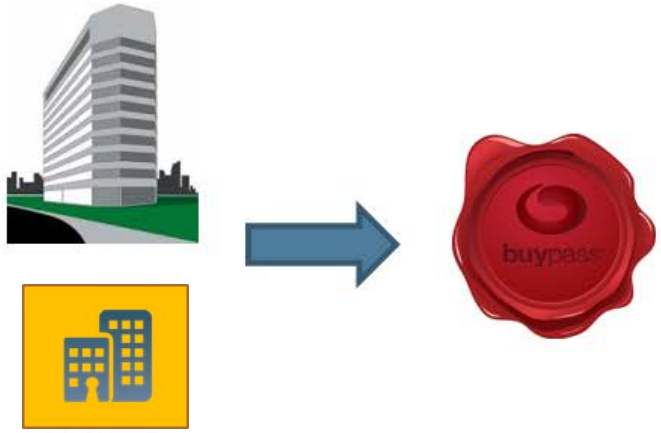
buypass

Elektronisk signatur og elektronisk segl

- **Elektronisk signatur (eSignature)**
  - Privatperson ”generer digital signatur” på data
    - Signaturen uttrykker samtykke til data som signeres
      - (og sikrer integritet og opprinnelse til data)
  - Digitalt sertifikat bekrefter personens identitet

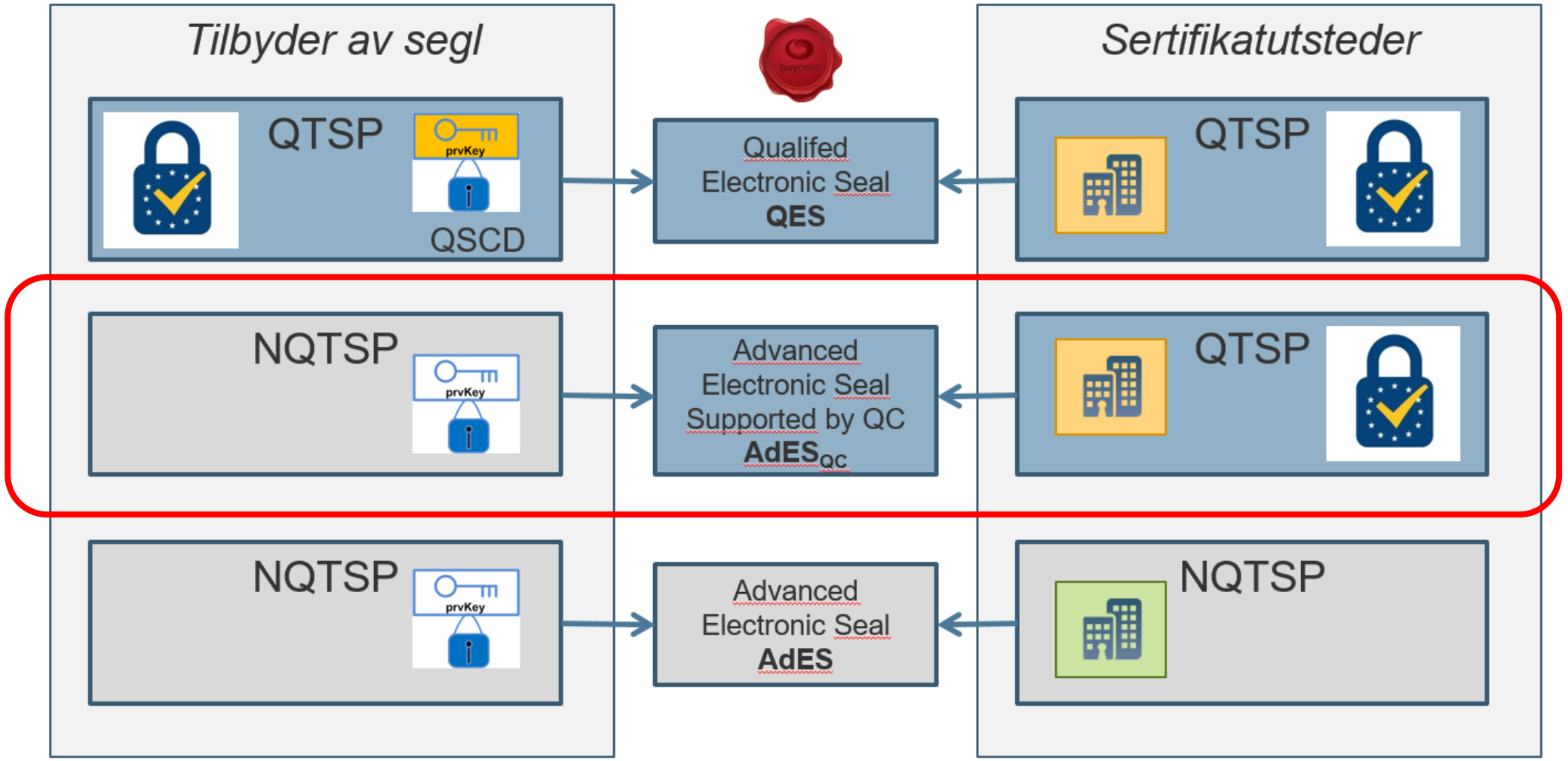


- **Elektronisk segl (eSeal)**
  - Virksomhet ”genererer digital signatur” på data
    - Seglet sikrer integritet og opprinnelse til data
  - Digitalt sertifikat bekrefter virksomhetens identitet



buypass

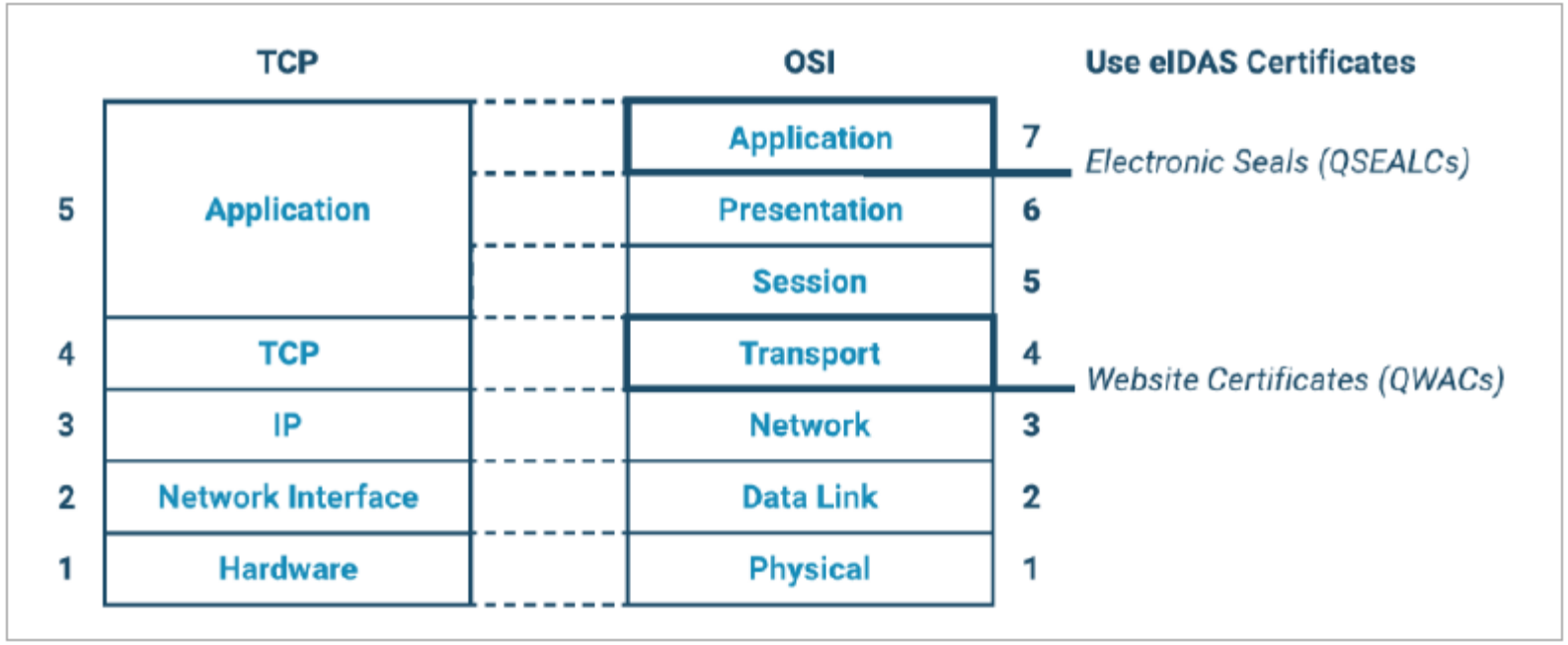
Kvalifisert sertifikat vs kvalifisert segl



buypass

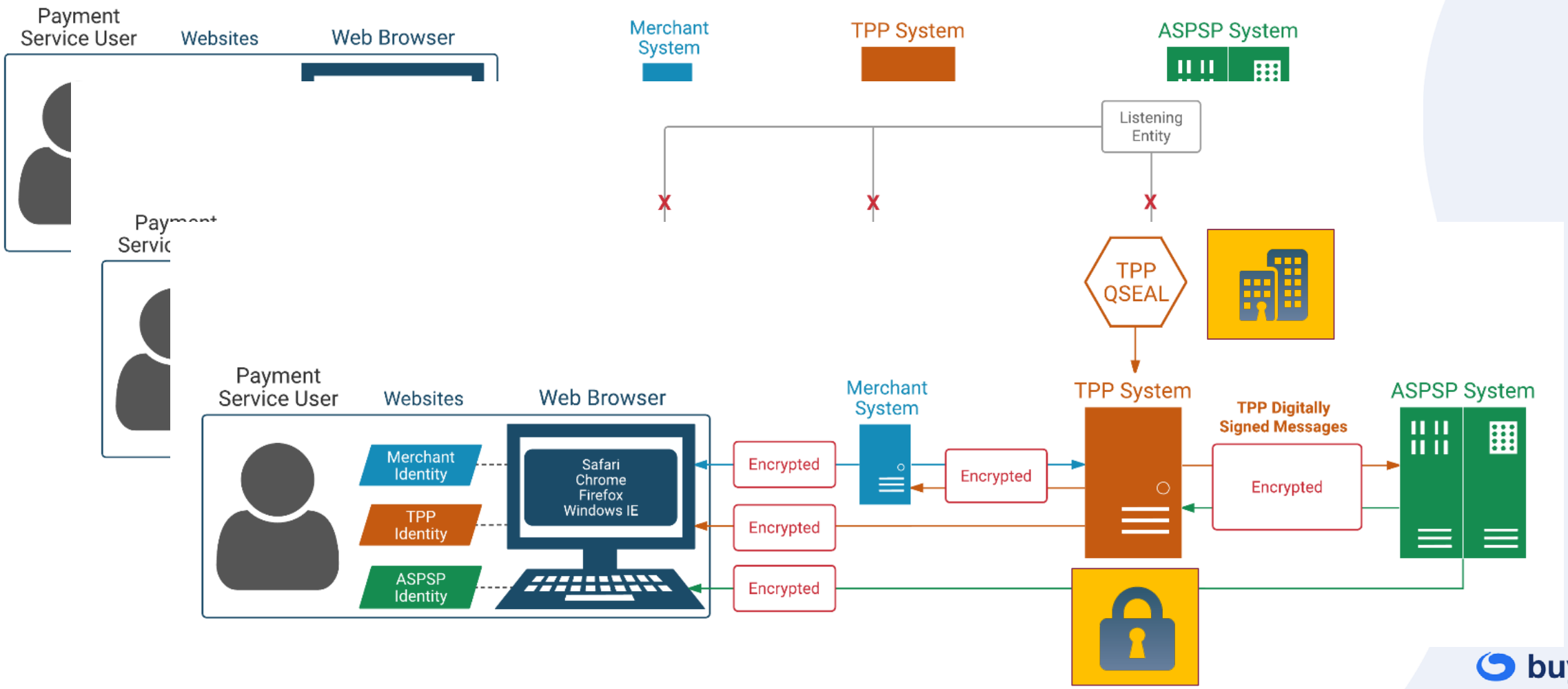
QSealC eller QWAC?

Feature	QSealC with Electronic Seal	QWAC with Transport Layer Security
Where is protection applied?	During communication and in storage	Just during communication
Is data protected when passed through intermediary?	Protection applies end-to-end, even if passed through intermediary	Only applied to direct peer-to-peer communications
What data is protected?	Specific data block	All data passing through channel
Evidential value?		
Type of protection?		



buypass

Bruk av QWAC og QC eSeal



buypass

EBA-Op-2018-7

10 December 2018

Opinion of t
on the use c
RTS on SCA

The opinion is addr
expectations it conv
technical service prov
interface) initiatives, t
as well as the establis

14. Taking into account the legal requirements of Article 34(1) and Article 35(1) of the RTS and the specificities of QSealCs and QWACs, the EBA has identified three possible alternatives for the use of QWACs and QSealCs by AISPs, PISPs and CBPIIs.

    a) *Parallel use of QWACs and QSealCs* – this will allow AISPs, PISPs and CBPIIs to identify themselves towards the ASPSPs and, at the same time, ensure that the communication is secure and that the data submitted originates from the PSP identified in the certificate.

    b) *Use of QWACs only* – this will allow AISPs, PISPs and CBPIIs to communicate securely with and identify themselves towards the ASPSP, but cannot provide evidence that the data submitted originates from the PSP identified in the certificate.

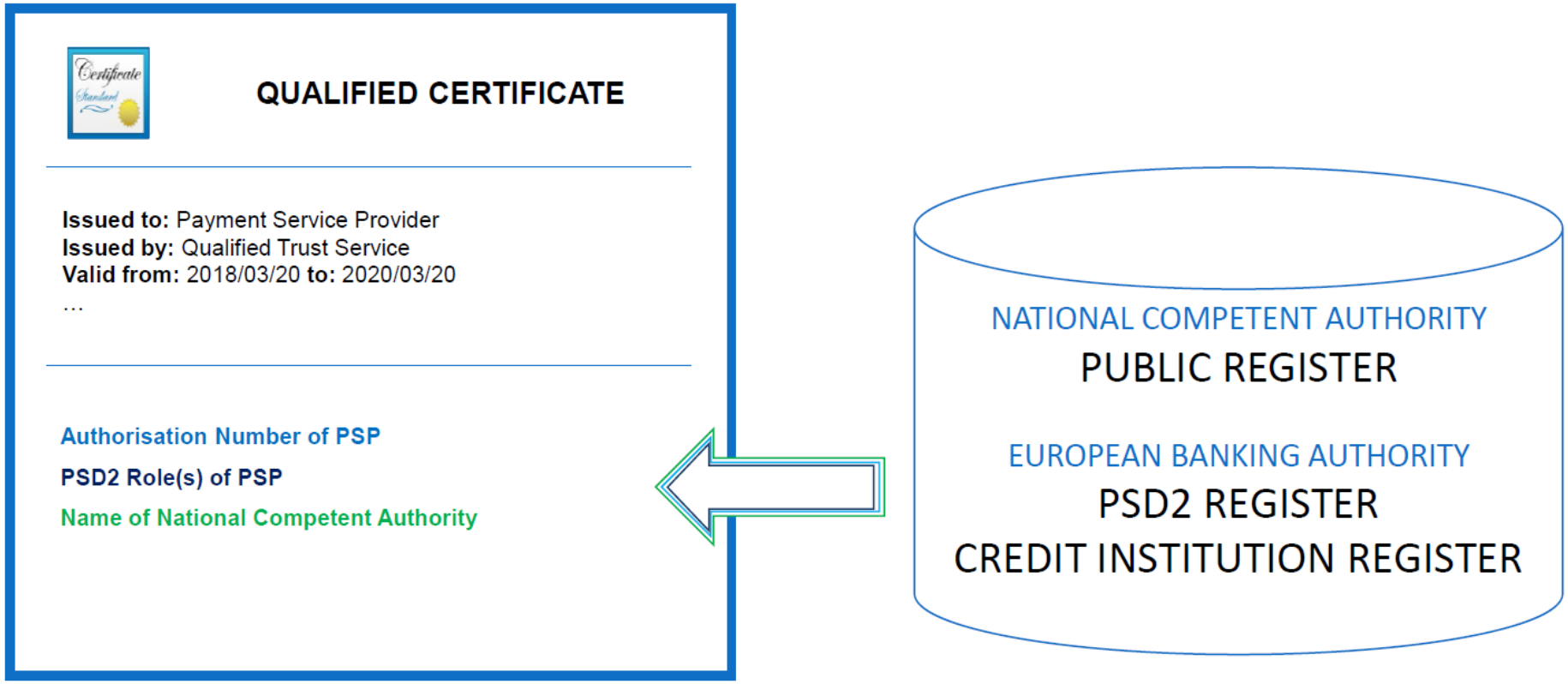
    c) *Use of QSealCs with an additional element that ensures secure communication* – QSealCs will allow AISPs, PISPs and CBPIIs to identify themselves towards the ASPSPs, but cannot ensure confidentiality during the communication session. Therefore, an additional element that ensures secure communication should be used in order to comply with the requirements of Article 35(1) of the RTS.

15. Although ASPSPs can choose any of the above three options, to ensure that (i) AISPs, PISPs and CBPIIs are able to identify themselves towards ASPSPs, (ii) AISPs, PISPs, CBPIIs and ASPSPs apply secure encryption throughout each communication session in order to safeguard the confidentiality and the integrity of the data and (iii) data provided are originated by the PSP identified in the certificate, the EBA recommends CAs to encourage ASPSPs to use both QWACs and QSealCs in parallel. However, the EBA reiterates that for establishing a secure

PSD2 attributter i sertifikater

buypass

Verifisering av PSD2 attributter



buypass

Registrering og utstedelse

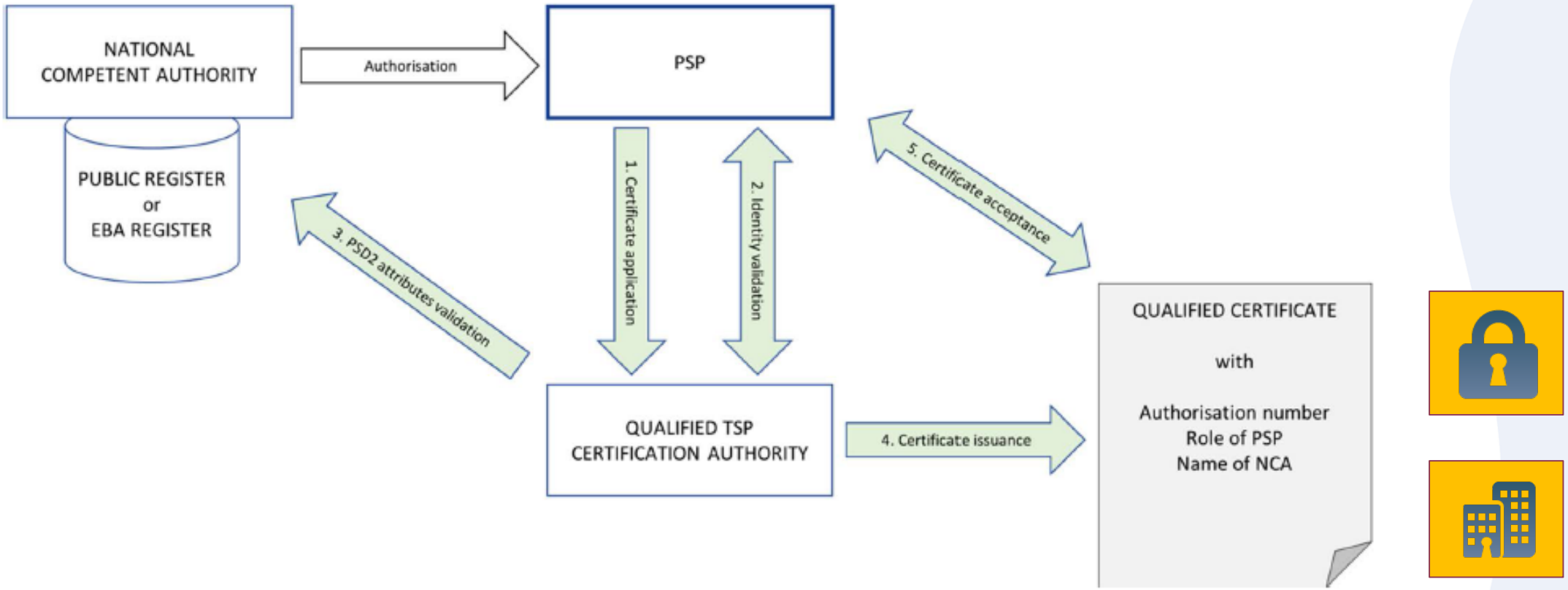


Figure 1: PSP Registration and certificate issuance

buypass

«PSD2 identitet» = Authorisation Number

organizationIdentifier

- "PSD"
- 2 character country code (NCA country)
- hyphen-minus "-"
- 2-8 character NCA identifier
- hyphen-minus "-"
- PSP identifier - authorisation number

PSDPL-PFSA-1234567890

buypass

PSP roller og NCA navn

PSD2 QCStatement

- ROLES:

(i) account servicing (**PSP_AS**);

(ii) payment initiation (**PSP_PI**);

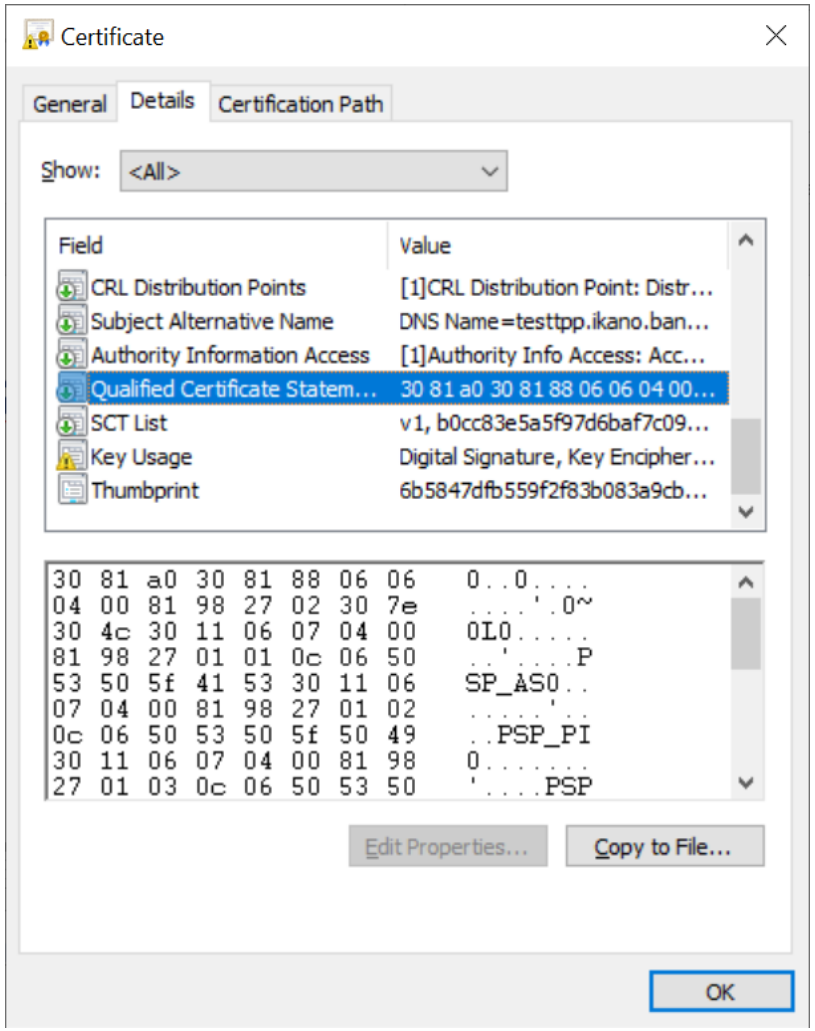
(iii) account information (**PSP_AI**);

(iv) issuing of card-based payment instruments (**PSP_IC**);

- NAME OF NCA (NATIONAL COMPETENT AUTHORITY)

buypass

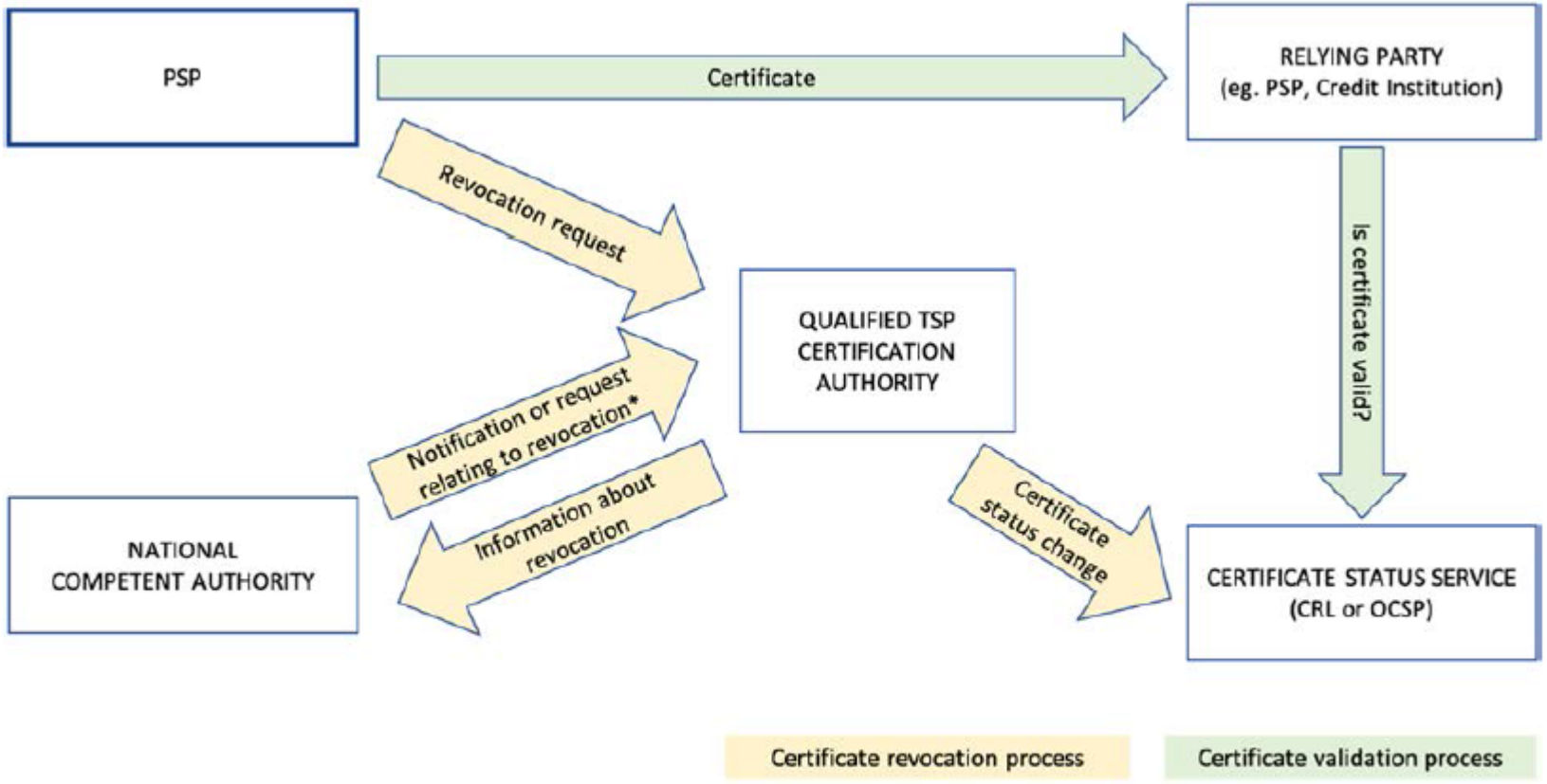
qcStatements i Buypass testsertifikater




```
1012  194:         SEQUENCE {
1015    8:           OBJECT IDENTIFIER qcStatements (1 3 6 1 5 5 7 1 3)
1025  181:           OCTET STRING, encapsulates {
1028  178:             SEQUENCE {
1031   98:               SEQUENCE {
1033    6:                 OBJECT IDENTIFIER '0 4 0 19495 2'
1041   88:                 SEQUENCE {
1043   38:                   SEQUENCE {
1045   17:                     SEQUENCE {
1047    7:                       OBJECT IDENTIFIER '0 4 0 19495 1 2'
1056    6:                       UTF8String 'PSP_PI'
              :                       }
1064   17:                     SEQUENCE {
1066    7:                       OBJECT IDENTIFIER '0 4 0 19495 1 3'
1075    6:                       UTF8String 'PSP_AI'
              :                       }
              :                     }
1083   39:                   UTF8String 'Swedish Financial Supervision Authority'
1124    5:                   UTF8String 'SE-FI'
              :                   }
              :                 }
1131   19:               SEQUENCE {
1133    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 6'
1141    9:                 SEQUENCE {
1143    7:                   OBJECT IDENTIFIER '0 4 0 1862 1 6 2'
              :                   }
              :                 }
1152   55:               SEQUENCE {
1154    6:                 OBJECT IDENTIFIER '0 4 0 1862 1 5'
1162   45:                 SEQUENCE {
1164   43:                   SEQUENCE {
1166   37:                     IA5String 'https://www.buypass.no/pds/pds_en.pdf'
1205    2:                     PrintableString 'en'
              :                     }
```

buypass

Revokering av sertifikater



NOTE: The present document does not place any specific requirements on the NCA regarding revocation.

Figure 2: Illustration of PSP Certificate validation and revocation

buypass

Validering av sertifikatene

When a party uses a PSD2 Qualified Certificate to identify another party, they will want to check that the certificate is 'valid'. This check generally involves checks on the following aspects of a certificate:

What to Check	How to Check it
That the Trust Service Provider (TSP) is Qualified	EU Trusted Lists
That the certificate is technically correct and has not expired	A raft of standards and practices in current use today
That the certificate is Qualified	*QCStatement* marking certificate as Qualified, etc.
That the certificate contains the required PSD2 information	Checking against ETSI TS 119 495
That the certificate has not been revoked since it was issued	Certificate Revocation List (CRL) / Online Certificate Status Protocol (OCSP) checks

Note these checks confirm the validity of the certificate and the identity authentication supported by the certificate. However, it does not necessarily confirm that the authorisations for the PSP are up-to-date (please see 5.4 Are PSP Authorisation & Roles updates synchronised with certificates? on page 14).

buypass

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.

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

buypass

Preta: Open Banking Europe Community

Competent Authorities & Associations

Get support for Regulatory Data Standards reviews & engage with EU dialogue on NCA data exchange procedures

ASPSPs

Join fellow ASPSPs as a stakeholder, to design and implement pan-EU PSD2 access to account services.

Third Party Providers

Sign-up to give early input to Identity and data mechanisms that will help smooth XS2A across the EU.

Qualified Trust Service Providers

Sign-up to engage with PSD2 Certificate issues and show the market that there are services available.

Solution Providers

Become a directory distributor for client deployments across the EU.

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

OPEN BANKING EUROPE

Preta: Open Banking Europe (OBE)

"Working. Together."

16th November 2018

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

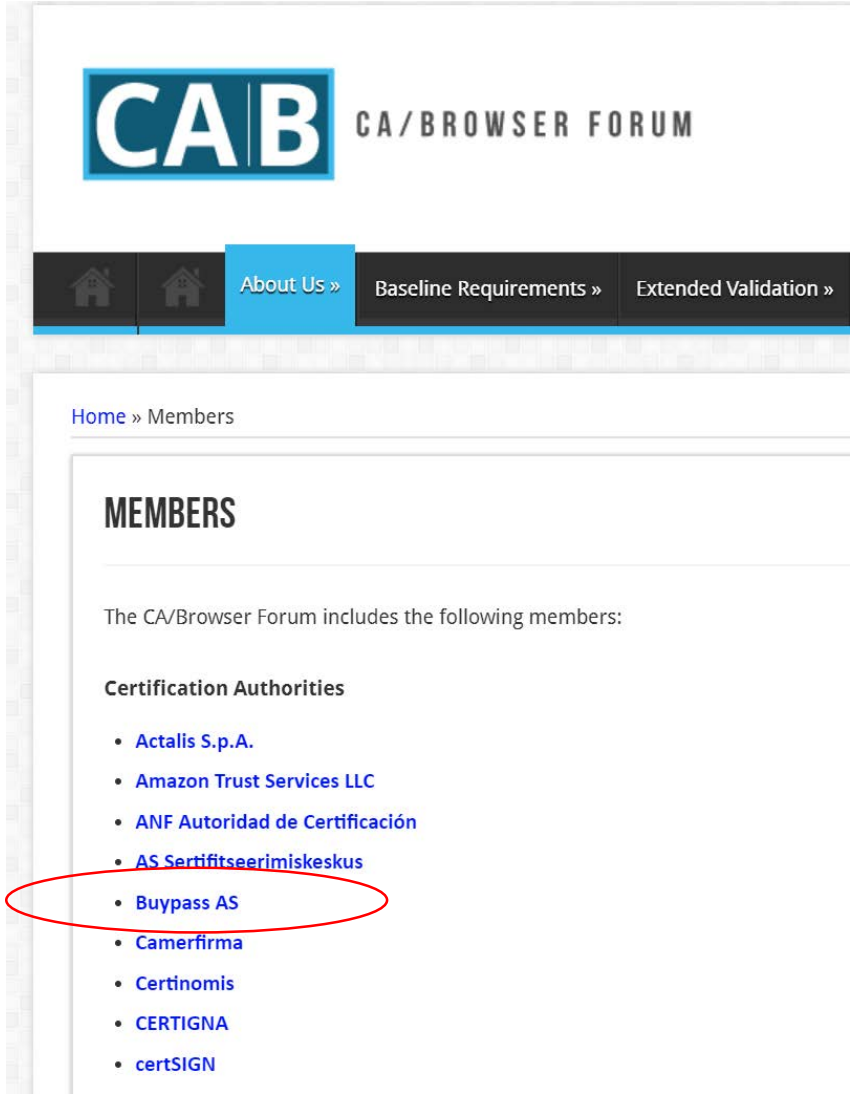
buypass

Participants

QTSP	Country
Aruba	Italy
Buypass	Norway
CertEurope	France
CertSign	Romania
D-Trust & (Bundesdruckerei)	Germany
Firmaprofesional	Spain
Global Sign	Belgium
Harica	Greece

QTSP	Country
Infocert	Italy
LuxTrust	Luxembourg
Microsec	Hungary
Multicert	Portugal
Namirial	Italy
SwissCom	Austria (Switzerland)
Trans Sped	Romania
Quovadis (Wisekey)	Netherlands (France)

CA/Browser Forum (cabforum.org)



buypass

PDS2-sertifikater for Test

- **Buypass kan levere test PSD2-sertifikater både for QWAC og QC eSeal**
- **Vi trenger følgende informasjon:**
  - Organisasjonsnummer (og navn)
  - Kontaktinformasjon
  - PSD2-attributter
    - Authorization Number – tildelt av NCA (for eksempel Finanstilsynet)
    - NCA informasjon – land (og identifikator og navn)
    - PSP-roller – vilkårlig kombinasjon av 4 definerte roller
- **Tilleggsinformasjon**
  - For QWAC:
    - CSR som inneholder offentlig nøkkel og domenenavn
  - For QC eSeal:
    - Buypass kan generere nøkkel => distribueres som PKCS#12-fil og aktiveringskode
    - Kunde kan generere nøkkel -> registrere CSR med offentlig nøkkel sammen med bestilling
- **Ta kontakt med Salg (salg@buypass.no) for mer informasjon**

buypass

PSD2-sertifikater i Produksjon

- **Krever noe mer informasjon:**
  - Kontraktsignerer – autorisert representant for virksomheten
  - Strengere valideringskrav:
    - Virksomhetens identitet må valideres mot godkjente registre (som Brønnøysundregistrene)
    - PSD2-attributter må verifiseres mot godkjente registre (NCA/EBA)
    - Personlig fremmøte
    - Signatur på abonnentavtale
- **Vi jobber med systemløsning for PSD2-sertifikater slik at kunde kan bestille selv via Web**
- **Planlagt ferdig Q2 - mai 2019**
  - Manuelle rutiner inntil dette er på plass, må avtales spesielt

buypass

Mer informasjon

- https://www.buypass.com/products/eseal--and-enterprise-certificate/eidas-qualified-certificates
- https://www.openbankingeurope.eu/resources/public-resources/
- https://www.openbankingeurope.eu/qtsps-and-eidas/
- https://www.openbankingeurope.eu/national-registers/
- https://portal.etsi.org//TBSiteMap/ESI/ESIActivities.aspx
- https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/

buypass

Spørsmål?