Nedenfor følger en oppsummering av seminaret 02.04.2019. Tre spørsmål kom opp i etterkant av seminaret. Spørsmålene og svarene er inkludert i denne oppsummeringen.

Innledning ved Finanstilsynet

1. Hvor finnes informasjon om foretak som har lisens som betalingsforetak?
2. Hvordan går foretakene frem for å få utstedt sertifikat?
3. Prosessen når det gjelder testsertifikater og produksjonssertifikater
4. Validering av sertifikater
5. Tilbakekalling av sertifikater – fullmakter, dokumentasjon, kommunikasjon
6. Sertifikater for sikker kommunikasjon vs. sertifikater for signering av transaksjoner
7. Hvem er ansvarlig for å signere hva på transaksjonsnivå (applikasjonslaget)?

1. Hvor finnes informasjon om foretak som har lisens som betalingsforetak?

Det kan ikke legges til grunn at noen av foretakstype (bank, kredittforetak, betalingsforetak eller e-pengeforetak) har tillatelse til å yte de nye tjenestene uten videre. QTSP må sjekke hvilke tjenester foretaket har tillatelse til å yte. Dette vil fremgå slik i Finanstilsynets konsesjonsregister:

Betalingsforetak/e-pengeforetak/ opplysningsfullmektig
For betalingsforetak/ e-pengeforetak/ opplysningsfullmektig vil det under kategorien tjenester/klasser fremgå konkret at foretaket kan yte tjeneste/klasse:

1) betalingsfullmakttjenester
eller
2) kontoinformasjonstjenester
Eventuelt begge

Se eksempel her på et utenlandsk foretak som er oppført med slik tillatelse på grensekryssende basis:

https://www.finanstilsynet.no/konsesjonsregisteret/detail/?id=200786

Oppføringen for CBPII tjenester vil være noe annerledes. Her vil foretaket være oppført med tjeneste/ klasse:

c) Utstedelse og innløsning av betalingstransaksjoner

I tillegg må det etterspørres bekreftelse på at foretaket har meldt og fått godtatt av Finanstilsynet at det skal yte CBPII tjenester. En indikasjon på at dette ikke er tilfellet er at foretaket ikke er oppført i EBAs Payment Institution Register, ettersom kun betalingsforetak/ e-pengeforetak/ opplysningsfullmektig som oppfyller aktuelle krav i PSD 2 vil være oppført her.

Per i dag er det ingen norske betalingsforetak eller e-pengeforetak som har tillatelse til å yte noen av de nye tjenestene (CBII, AIS, PIS) på bakgrunn av tillatelse fra Finanstilsynet. Det er heller ingen norske foretak med konsesjon som opplysningsfullmektig.

Banker
Konsesjonsregisteret angir ikke hvilke spesifikke betalingstjenester en bank kan yte, men kun at banken kan yte tjeneste/klasse "betalingsformidling". I utgangspunktet kan det antas at slik oppføring dekker alle de nye tjenestene.

Kredittforetak
Konsesjonsregisteret angir ikke hvilke spesifikke betalingstjenester et kredittforetak kan yte, men kun at kredittforetaket kan yte tjeneste/klasse "ytelse av betalingstjenester". I utgangspunktet kan det antas at slik oppføring dekker alle de nye tjenestene.

Det fremgår eksplisitt av Finanstilsynets nettsider at det tas forbehold om feil i konsesjonsregisteret. Vi vil anbefale QTSP å innhente fra foretaket dokumentasjon som viser at foretaket har nødvendig tillatelser.

2. Hvordan går foretakene frem for å få utstedt sertifikat?

Exemption til fallback forutsetter 3 måneder utstrakt bruk før 14. september. Da må foretakene ha installert og testet med produksjonssertifikater før 14. juni. De vil trenge minst 2 uker for å bestille og installere og teste prodsertifikatene. Og QTSP-en må ha laget sertifikatene. Informasjon om foretakene som skal inn i sertifikatet henter QTSP-en fra Finanstilsynets register. QTSP-en bør i tillegg be foretaket dokumentere som viser at foretaket har nødvendige tillatelser.

Foretak i prosess med å søke om tillatelse, kan be Finanstilsynet om bekreftelse på at de er i prosess. Bekreftelsen kan foretaket benytte overfor QTSP, som i sin tur kan utstede sertifikat til foretaket.

3. Prosessen når det gjelder testsertifikater og produksjonssertifikater

Vi viser til pkt. 2 og til foredraget som Buypass holdt på seminaret. Kopi av lysbildene ligger på Finanstilsynets nettsider
https://www.finanstilsynet.no/contentassets/b1101e98baf84ab1a4700f3a3a2b6bf4/psd2-eidas-sertifikater---buypass.pdf

4. Validering av sertifikater

Sertifikatene valideres mot såkalte Trusted Lists. Dette er lister over sertifikatutstedere og rotsertifikater. Vi viser for øvrig til foredraget som Buypass holdt. Kopi av lysbildene ligger på Finanstilsynets nettsider.
https://www.finanstilsynet.no/contentassets/b1101e98baf84ab1a4700f3a3a2b6bf4/psd2-eidas-sertifikater---buypass.pdf

5. Tilbakekalling av sertifikater

TPP-er plikter å meldt til QTSP dersom sertifikatet ikke lenger er gyldig. Finanstilsynet kan anmode QTSP om å tilbakekalle et sertifikat. Finanstilsynet må dokumentere årsaken til tilbakekallingen.

6. Sertifikater for sikker kommunikasjon vs. sertifikater for signering av transaksjoner

QWACS benyttes for sikker kommunikasjon. Den gir gjensidig autentisering av partene som kommuniserer og beskyttelse mot uautorisert innsyn i kommunikasjonen mellom dem. QSEALS benyttes for signering av transaksjoner og sikrer at innholdet i transaksjonen ikke endres.

7. Hvem er ansvarlig for å signere hva på transaksjonsnivå (applikasjonslaget)?

Dynamic linking innebærer at transaksjoner signeres og at signaturen speiler brukeren, betalingsmottakeren og transaksjonsbeløpet. RTS stiller krav om Dynamic linking. Dynamic linking kan skje hos TPP-en eller hos ASPSP.

8. Status

RTS (ny forskrift) art. 30 – krever at kontotilbyder skal gjøre tilgjengelig ett grensesnitt for tredjeparter, slik at disse kan identifisere seg overfor kontotilbyder og kommunisere sikkert med formål å yte betalingstjenesten.

Forskrift om systemer for betalingstjenester § 8, siste ledd stiller krav til at også kontotilbyder skal kommunisere med betalingstjenestetilbydere på en sikker måte. Dette betyr i praksis at kontotilbyder skal identifisere seg med et EIDAS sertifikat i kommunikasjonen med TPP-ene.

Kunden skal oppleve betalingstjenestene og kontoopplysningstjenestene som leveres fra kontotilbyder som like hensiktsmessige som tilsvarende tjenester som leveres fra TPP-ene. Finanstilsynet vil i denne sammenhengen vurdere oppetid, svarstider, kundestøtte, enkelhet, informasjonsrikdom, meldinger om transaksjonsforløp, feilmeldinger. Det vil si at hele kundereisen skal oppleves som like god for de to grensesnittene.

Det er brukeropplevelsen når det gjelder brukerens tilgang til brukerens kontoer i dag som er målestokken. Om bruker går gjennom en tredjepart, skal det oppleves likt.

Sterk kundeautentisering – kan skje på ulike måter;

1. Redirect (mest bruk, BankID, banktjenestetilbyder venter på svar, får tilbake signert identifiserings objekt. Hver bank er ansvarlig for å implementere. Må sammenlikne med egen bank sitt grensesnitt. Må ikke sammenlikne med andre banker)
2. Embedded (opprinnelig tanke fra EBA, integrert i dialog med kunden, ga sine credentials i samme sesjon.)
3. Decoupled (autentiseringstjenesten til Yahoo, eller Facebook, eller Microsoft benyttes såfremt de tilfredsstiller kravene til SCA i RTS-en. BankID på mobil kan være et eksempel på en nasjonal decoupled løsning for norske brukere)

Reserveløsning, RTS nr. 33.

Betalingstjenestetilbyder skal kunne bruke eksisterende grensesnitt som brukeren sedvanlig bruker som nettbank etc., art. 33 nr. 4.

Art. 33 nr .5
Unntak fra reserveløsning forutsetter, i tillegg til de generelle kravene i art. 32, at grensesnittet har vært i utstrakt bruk – "widely used".

Det følger av dette et aktivitetskrav på tjenestetilbyder, ASPSP og brukere. Det er et krav at alle parter er aktive med tanke på å få løsningene i bruk.

Det følger av aktivitetskravet at kontotilbyder skal aktivt oppsøke TPP-er og oppfordre disse til å teste og pre-pilotere løsningen til kontotilbyder så snart kontotilbyder er klar med grensesnittet.

Dette møtet som arrangeres av Finanstilsynet i dag er ment å få i gang en dialog mellom partene, slik at det åpnes opp for test og pilotering mellom aktørene.

Dersom kontotilbydere også opererer som TPP-er, vil test mellom disse kunne telle med ved vurderingen av om 3-måneders kravet og utstrakt bruk er oppfylt.

Dersom det ikke er mulig å få realisert utstrakt bruk av løsningen i 3 måneder, så anses dette som en indikasjon på at løsningen ikke er hensiktsmessig. I denne situasjonen skal betalingstjenestetilbyder kunne bruke eksisterende grensesnitt som brukeren sedvanlig bruker som for eksempel nettbank etc., art. 33 nr. 4.

9. Spørsmål fra salen

Spørsmål: Solaris opererer som Software As A Service leverandør. Har ikke sluttbrukere. Er Solaris forpliktet til å tilby et PSD-grensesnitt?
Finanstilsynet er av den oppfatning at leverandører av betalingstjenester som benytter Solaris sin løsning må ha et eget grensesnitt, eller henvise til Solaris sitt eget grensesnitt.

Sp. fra salen: Bør banken endre dagens grensesnitt (nettbank, brettbank, mobilbank) slik at TPP-er som benytter fall-back kun får tilgang til kundens betalingskontoer?
I en situasjon der ASPS-en må tilby fall-back løsning, dvs. nettbank, brettbank og mobilbank, vil TPP-en få tilgang til mer informasjon enn den skal ha tilgang til etter PSD2. Dette fordi bankens grensesnitt i disse kanalene ikke er laget slik at tilgang kan avgrenses til kundens betalingskontoer eller til 90-dagers historikk.

Finanstilsynet mener at bankene bør ha funksjonalitet slik at tilgang kan avgrenses til bestemte av kundens kontoer. Videre bør tilgang kunne avgrenses til å gjelde kun lesetilgang.

Sp. fra salen: Bør banken endre dagens grensesnitt (nettbank, brettbank, mobilbank) slik at TPP-er som benytter fall-back kan autentiseres i disse kanalene?
Tjenestetilbyder vil i denne situasjonen typisk søke å bli identifisert med EIDAS sertifikat. Finanstilsynet mener at bankene må kunne autentisere TPP-ene i disse grensesnittene.

Spørsmål fra salen: Hva gjelder for etablerte fullmaktsløsninger og disposisjonsforhold?
Introduksjonen av tredjepart endrer ikke på brukers fullmakter eller disposisjonsforhold. Brukeren må kunne benytte fullmaktsforholdet og disposisjonsforholdet via TPP-ene.

Men disposisjonsforholdet må etableres hos ASPSP.

Spørsmål om utstrakt bruk og dokumentasjon i denne forbindelse
Kan man i forbindelse med søknaden (innen fristen 15. juni) opplyse hvordan banken tenker å oppfylle vilkåret om utstrakt bruk, og deretter ettersende dokumentasjon på hvordan dette er gjennomført (etter fristen)?

Finanstilsynet svarte at ja, man kan ettersende dokumentasjon på gjennomføring av testingen.

Spørsmål: Hvordan skal ASPSP forholde seg til screen scraping før 14. september
Finanstilsynet opplyste at ifølge EBA kan TPP-er, som benyttet screen scraping før ikrafttredelse av PSD2, fortsette å benytte screen scraping frem til ikrafttredelse av RTS-en, dvs. 14. september 2019.

Spørsmål: Hvordan vet man at sertifikatet er gyldig til enhver tid
Bakgrunnen for spørsmålet er for eksempel at tillatelser er trukket tilbake, og at det er administrative forsinkelser som gjør at det ikke har vært mulig å revokere sertifikatet umiddelbart.

Innehaver av sertifikatet, dvs. tjenestetilbyder, plikter å melde endring av sin status til QTSP umiddelbart. Finanstilsynet plikter å videreformidle endringer til sentralt EBA- register innen utgangen av arbeidsdagen da endringen trådte i kraft.

Dette skiller seg i prinsipp ikke fra sedvanlig endring av bankkonsesjon og andre former for konsesjon når det gjelder tid for saksbehandling og oppdateringer.

Spørsmål fra salen om ASPSP-ens autentisering av TPP
Eksempel: En tysk tilbyder ber om tilgang til kontoinformasjon hos norsk ASPSP. Er det tilstrekkelig å sjekke sertifikatet?

Det er tilstrekkelig at kontotilbyder sjekker sertifikatet – kontotilbyder skal ikke behøve å gjøre andre kontroller av TPP-en. Se her:

https://eba.europa.eu/single-rule-book-qa?p_p_id=questions_and_answers_WAR_questions_and_answersportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_pos=1&p_p_col_count=2&_questions_and_answers_WAR_questions_and_answersportlet_jspPage=%2Fhtml%2Fquestions%2Fviewquestion.jsp&_questions_and_answers_WAR_questi

ons_and_answersportlet_viewTab=1&_questions_and_answers_WAR_questions_and_answersportlet_questionId=2539903&_questions_and_answers_WAR_questions_and_answersportlet_statusSearch=1

Spørsmål fra salen vedr. søknad om fallback
Skal bankene forholde seg til Guideline eller listen som er presentert på finanstilsynet.no.

Bankene må svare opp alle kravene i Guideline. Listen på 11 punkter er et forsøk fra Finanstilsynet på å konkretisere innholdet i begrepet "widely used".

Spørsmål fra salen: Kommer Finanstilsynet til å lage et søknadsskjema?
Finanstilsynet kommer ikke til å lage noe søknadsskjema. Finanstilsynet antar at søknadene vil bli følge systematikken i Guidelines og svare opp kravene der.

Spørsmål: For fellesløsninger når det gjelder grensesnitt – er det tilstrekkelig at widely used rapporteres for fellesløsningen og bare denne?
Nei. De 11 punktene må besvares individuelt med bakgrunn i hva den enkelte bank har gjort for å sikre utstrakt bruk i sitt marked. Det påligger et betydelig aktivitetskrav på hver bank med hensyn til å bidra til aktiv bruk i sitt marked / segment. Men banker kan sammen utarbeide enkelte felles aktiviteter som de så tar "hjem" og anvender i sitt marked.

Spørsmål knyttet til kredittkort. Er de underliggende kredittkort-kontoene omfattet av PSD2, og må være tilgjengelig via PSD2-apiet dersom kontoene vises i bankens nettbank?
Kontoer som benyttes til betalinger skal vises. Dette gjelder uavhengig av om det er snakk om kredittkortkontoer eller andre kontoer.

Noen banker har en løsning slik at de kan betale regning med direkte belastning av et kredittkort i nettbanken. Noen oppfatter at PISP-rollen skal ha mulighet til å initiere en betaling på konto, og ikke på kredittkort. Er regningsbetaling fra et kredittkort omfattet av det PSD2-apiet som en PISP skal gi tilgang til?
Finanstilsynet: Ja dette synes å være dekket, jf. teksten nedenfor:

ANNEX I

PAYMENT SERVICES

(as referred to in point (3) of Article 4)

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:

   (a) execution of direct debits, including one-off direct debits;

   (b) execution of payment transactions through a payment card or a similar device;

   (c) execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a payment service user:

   (a) execution of direct debits, including one-off direct debits;

   (b) execution of payment transactions through a payment card or a similar device;

   (c) execution of credit transfers, including standing orders.

5. Issuing of payment instruments and/or acquiring of payment transactions.

6. Money remittance.

7. Payment initiation services.

8. Account information services.

Presentasjon fra Buypass v/Mads Henriksveen
https://www.finanstilsynet.no/contentassets/b1101e98baf84ab1a4700f3a3a2b6bf4/psd2-eidas-sertifikater---buypass.pdf

Presentasjon fra BITS v/Brynjel Jonsen
https://www.finanstilsynet.no/contentassets/b1101e98baf84ab1a4700f3a3a2b6bf4/berlin-group-presentasjon-bits.pdf

Presentasjon fra Open Banking v/
https://www.finanstilsynet.no/contentassets/b1101e98baf84ab1a4700f3a3a2b6bf4/open-banking-europe.pdf