FINANSTILSYNET

NOTAT

Finanstilsynet

Senest opdateret 10. februar 2025

God praksis for PSD2-API'er

Indledning og baggrund

Med det andet betalingstjenestedirektiv (EU) 2015/2366 (PSD2) blev kontoførende betalingstjenesteudbydere (account servicing payment service providers, ASPSP) forpligtet til at sikre, at udbydere af tredjepartstjenester (third party payment service providers, TPP) kan tilgå oplysninger og funktioner fra en brugers online betalingskonti på sikker og effektiv vis. Formålet med reglerne er at fremme konkurrence og innovation på betalingsområdet indenfor EU.

Kommissionens delegerede forordning (EU) 2018/389 om stærk kundeautentifikation og fælles og sikre åbne standarder for kommunikation (forordningen) regulerer måden, hvorpå tredjepartsudbydere tilgår oplysningerne og funktionerne fra brugernes online betalingskonti. Forordningen fastsætter nærmere bestemt, at denne adgang som udgangspunkt skal gives gennem et API[1], også kaldet et *dedikeret interface*, der stilles til rådighed for TPP'erne af ASPSP'erne. Den Europæiske Banktilsynsmyndighed (EBA) har derudover i en række udtalelser, vejledninger og Q&As uddybet indholdet af forordningen.

På trods af disse supplerende fortolkningsbidrag fra EBA af både bindende og mere vejledende karakter, opstår der fortsat løbende fortolkningsspørgsmål mellem ASPSP'er og TPP'er relateret til PSD2-API'erne i praksis, som reguleringen ikke forholder sig klart til. Finanstilsynet nedsatte derfor i efteråret 2021 API Forum, hvor ASPSP'er og TPP'er mødes og drøfter disse praktiske udfordringer sammen med Finanstilsynet. Formålet er i fællesskab at nå til enighed om mulige løsninger og god praksis for udvikling og brug af PSD2-API'er.

Bankdata, BEC, SDC, Danske Bank, Nordea[2] og Lunar deltager som ASPSP'er og datacentraler på møderne, mens Aiia, Kontolink, Loyal

[1] Application Programming Interface, API, er en softwaregrænseflade, der tillader et stykke software at interagere med andet stykke software. Et API gør det muligt at tilbyde tjenester, herunder visning af data, i et system fra et andet system.
[2] Nordea Danmark er under tilsyn af det finske finanstilsyn, men har deltaget i forummet grundet Nordeas tilstedeværelse i Danmark.

Solutions, Subaio, Mastercard Payment Services, Moneycapp, Monthio, Nets, Symblepay og Noitso deltager som TPP'er. Finans Danmark og Forsikring & Pension deltager som observatører. Finanstilsynet vil løbende overveje medlemssammensætningen af forummet, i takt med, at markedet udvikler sig.

Dette "god praksis papir" opsummerer konklusioner på fire overordnede emner, som medlemmerne har drøftet på møderne i API Forum siden forummets opstart. Finanstilsynet skriver på sin hjemmeside, at "God praksis-papirer indeholder generelle, foreløbige og uformelle forventninger til virksomhederne, som gælder på tidspunktet for papiret"[3]. Indholdet i papiret vil dermed ikke indgå som element i Finanstilsynets løbende tilsynsaktivitet, og er alene en gengivelse af, hvad forummets medlemmer er blevet enige om at kunne forvente af hinanden. Såfremt det videre arbejde med at identificere praktiske problemstillinger og i fællesskab opnå god praksis for løsninger giver anledning til det, vil papiret blive revideret eller suppleret med nye papirer.

For hvert emne herunder fremgår der indledningsvist en redegørelse af det retlige grundlag efterfulgt at et kort oprids af drøftelserne i forummet. Hvert afsnit afrundes med en liste over de løsninger, som forummet i fællesskab er kommet frem til som god praksis på de drøftede udfordringer.

Videre arbejde

Finanstilsynet vil fortsætte drøftelserne med medlemmerne af API Forum for at følge op på, hvordan og i hvilket omfang ovennævnte god praksis kan implementeres hos markedsdeltagerne, og sikre en god dialog mellem medlemmerne. API Forum vil dermed fortsætte drøftelserne om god praksis for implementering af de overordnede emner i dette papir. Finanstilsynet forventer derudover, at deltagerne løbende vil identificere yderligere punkter, som forummet kan drøfte og hvor muligt etablere god praksis på. Finanstilsynet forventer, at dette god praksis-papir i fremtiden vil blive revideret eller suppleret på baggrund af de fortsatte drøftelser i API Forum.

[3] https://www.finanstilsynet.dk/om-os/finanstilsynets-opgaver/kommunikationsformater

Varsling af ændringer i API'erne

Gældende ret og behov for fælles forståelse
Det fremgår af artikel 30, stk. 4, i forordningen, at ASPSP'er skal varsle ændringer i API'erne tre måneder før, at ændringerne implementeres. Af samme artikel fremgår det, at implementering af ændringer kan ske med kortere varsel i såkaldt "kritiske situationer". Lovgivningen præciserer dog ikke nærmere, hvad en kritisk situation er, eller hvordan ASPSP'er skal varsle ændringer.

Drøftelser i forummet
Medlemmerne i API Forum er generelt enige om, at det er vigtigt at rette fejl i API'erne løbende og hurtigt. Derfor er det i praksis ikke altid hensigtsmæssigt, at ændringer skal varsles tre måneder før, at de må træde i kraft. Det kan skabe en unødig forsinkelse af nyttige eller sikkerhedskritiske ændringer. Der kan derfor være behov for, at ændringer kan træde i kraft hurtigere.

TPP'erne foretrækker generelt, at ændringer i API'er bliver lagt med en regelmæssig frekvens. Til dette anfører ASPSP'erne, at ændringer i API'erne ofte sker som afledt effekt af ændringer i bagvedliggende systemer, hvorfor det ikke er muligt at opdatere med en regelmæssige frekvens. Dette ønske kan derfor ikke imødekommes i praksis.

Medlemmerne drøftede i stedet muligheden for at varsle forskelligt alt efter hvilken type ændring, der er tale om. Ifølge artikel 30, stk. 4, i forordningen er det alene ændringer i "kritiske situationer", der kan implementeres med kortere varsel end tre måneder. Da det ikke er præciseret nærmere, hvad der betragtes som "kritiske situationer", har medlemmerne skelnet mellem forskellige typer af ændringer med henblik på at opnå en fælles forståelse for hvor langt varsel, der er behov for. Et forslag er, at varsling af tiltag, der ændrer i eksisterende funktioner, med fordel kan ske i god tid, dvs. tre måneder inden ikrafttrædelse som forudsat i artikel 30, stk. 4, i forordningen. Varsling af fejlrettelser eller udvikling af nye funktioner behøver derimod ikke nødvendigvis at ske, før de implementeres, såfremt ændringerne ikke har betydning for eksisterende løsninger. Der er i disse tilfælde ikke nødvendigvis tale om "kritiske situationer", men i praksis er der ikke behov for varsel på tre måneder.

API Forum har arbejdet videre med en klassificering af forskellige typer ændringer. Det er god praksis at inddele ændringer i "breaking changes", "mindre ændringer, herunder nye funktioner" og "fejlrettelser[4]". Varslingsperioden for "breaking changes" er som udgangspunkt altid tre måneder, mens mindre ændringer kan have kortere eller slet ingen varsel. Det vil være op til den enkelte ASPSP at vurdere hvilket varsel, der er hensigtsmæssigt for en konkret ændring. er det god praksis, at vælge en tilgang med øget varsling.

[4] Denne tilgang er valgt da den lægger sig op ad gængse klassificering af ændringer i "major", "minor" og "bug fixes".

For så vidt angår spørgsmålet om, hvordan ASPSP'er skal varsle ændringer overfor TPP'erne, er der som udgangspunkt metodefrihed for ASPSP'erne. Medlemmerne er generelt enige om, at det ikke udelukkende bør foregå via ASPSP'ernes developer portaler eller hjemmesider, da TPP'erne i så fald risikerer at overse kommende ændringer. Medlemmerne er enige om, at det er fordelagtigt, hvis ASPSP'erne aktivt kan sende såkaldte push-notifikationer med information om ændringer ud til TPP'erne, f.eks. via et nyhedsbrev på e-mail. Der er en fælles forståelse for, at TPP'erne selv er ansvarlige for at tilmelde sig sådanne nyhedsbreve hos ASPSP'erne samt selv at sørge for, at den kontaktinformation, som TPP'en har oplyst ASPSP'en, er opdateret. Finanstilsynet forstår, at alle ASPSP'er i Danmark pr. september 2022 aktivt sender push-notifikationer med information om ændringer i API'erne ud til de TPP'er, der har registreret sig hos dem.

I forhold til den besked som TPP'erne modtager fra ASPSP'erne om varsling af ændringer, foretrækker TPP'erne, at den gives i et maskinlæsbart format. Medlemmerne er dog enige om, at sådan en løsning har stor kompleksitet. For nuværende er det derfor fordelagtigt at fokusere på at forbedre informationsniveauet med andre typer løsninger, f.eks. e-mails.

TPP'erne fremhæver derudover et ønske om adgang til historik over ændringer, eventuelt struktureret med nøgleord. API Forum er enig i, at ASPSP'er bør føre en changelog hvor det løbende vil fremgå hvilke ændringer der er foretaget til API'et.

God praksis for varsling af ændringer i API'erne indebærer, at:

- ASPSP'er varsler ændringer i API'erne med en passende varslingsperiode på baggrund af ændringens karakter.
- ASPSP'er aktivt sender push-notifikationer med information om ændringer i API'erne ud til TPP'erne, f.eks. på e-mail.
- TPP'er tilmelder sig selv hos ASPSP'er, og sørger for at opdatere deres kontaktinformation for at kunne modtage push-notifikationer.
- ASPSP'er fører en changelog som løbende beskriver forandringer foretaget til API'et.

Information om driftshændelser og support til fejlrettelse

Gældende ret og behov for fælles forståelse
Det fremgår af artikel 32, stk. 1, i forordningen, at ASPSP'er er forpligtet til at yde samme support på PSD2-API'erne som på de såkaldte brugervendte interfaces såsom mobilbank og netbank. Dette indebærer, at ASPSP'erne skal sikre, at PSD2-API'erne har samme tilgængelighed og ydeevne, herunder support, som de brugervendte interfaces. PSD2-API'erne skal dermed generelt behandles på linje med de brugervendte interfaces i ASPSP'ens beredskabsplan. Det er dog ikke nærmere specificeret, hvordan ASPSP'er skal informere TPP'er om driftshændelser, eller hvordan supporten til TPP'er ved fejlrettelser skal ydes.

Drøftelser i forummet
Med henblik på at forbedre processerne for information om driftshændelser og support til fejlrettelser ønsker TPP'erne, at de efter indrapportering af et problem modtager bekræftelse fra ASPSP'erne om, at en opgave er modtaget og vil blive løst, samt så snart det er muligt, hvornår en løsning forventes implementeret. For at kunne imødekomme disse ønsker har ASPSP'erne tilsvarende behov for, at TPP'erne indberetter de mest nødvendige oplysninger. API Forum har udarbejdet en skabelon[5] der indeholder de mest basale og nødvendige informationer, som TPP'en bør medsende. API Forum besluttede også, at Finanstilsynet offentliggør skabelonen på sin hjemmeside. Formålet med skabelonen er at danne et ensartet udgangspunkt for efterfølgende dialog mellem TPP og ASPSP.

Ved akutte problemer, herunder uventet nedetid, finder TPP'erne det nyttigt, hvis ASPSP'erne af egen drift kan sende push-notifikationer med information om dette direkte til TPP'erne ligesom ved varsling af ændringer i API'erne. Det vil forbedre TPP'ernes fejlsøgning, hvis noget går galt, og gøre det nemmere for TPP'erne at reagere hurtigt på problemer. Det er Finanstilsynets indtryk, at flertallet af ASPSP'erne i Danmark pr. september 2022 aktivt sender push-notifikationer med information om driftsmæssige problemer i API'erne til de TPP'er, der har registreret sig hos ASPSP'en. Nogle ASPSP'er sender dog ikke information om disse hændelser direkte til TPP'erne. I disse tilfælde skal TPP'erne selv checke ASPSP'ernes developer portaler for at undersøge, om et problem skyldes et generelt nedbrud. Finanstilsynet finder, at ovenstående type af aktiv videndeling via eksempelvis push-notifikationer fra ASPSP til TPP kan forbedre processerne ved fejlrettelser og potentielt nedbringe TPP'ernes behov for at indrapportere fejl til ASPSP'erne.

Flere TPP'ere ønsker også at modtage information om planlagt nedetid af PSD2-API'erne. Det blev på API Forum drøftet om dette var muligt samt hvor

[5] Links:
Dansk version: https://www.finanstilsynet.dk/Media/APIhenvendelsestemplate_150224.pdf
Engelsk version: https://www.finanstilsynet.dk/Media/APIInquiryTemplate_150224.pdf

lang tid i forvejen nedetid kunne forventes at være planlagt og dermed potentielt kunne kommunikeres. Forummet konkluderede, at en hensigtsmæssig tidsramme kunne være 2 døgn før den planlagte nedetid. Det blev samtidig drøftet, om nedetid med fordel kunne lægges på særlige tider af døgnet. Her var der generel enighed om, at nattetimerne var mest oplagte i det omfang det var muligt for ASPSP'en i det konkrete tilfælde. TPP'erne ønskede også for planlagt nedetid at modtage push notifikationer.

Lovgivningen specificerer ikke, hvordan kommunikationen skal foregå mellem ASPSP'erne og TPP'erne. Det kan eksempelvis være via e-mail, ligesom ved varsling af ændringer i API'erne. Emnet skal drøftes nærmere på kommende møder i API Forum med henblik på at finde frem til god praksis.

ASPSP'erne er forpligtet til at yde samme support på PSD2-API'erne som på de brugervendte interfaces såsom mobilbank og netbank. Medlemmerne er dog enige om, at denne forpligtelse ikke umiddelbart giver mening i praksis. En TPP er ofte en specialiseret teknologivirksomhed, der har behov for en anden type support end en banks privatkunder, der benytter sig af mobil- eller netbank. API Forum er enige om, at ASPSP'er skal dedikere ressourcer til besvarelse af TPP'ers API-relaterede henvendelser, hvor spørgsmål om f.eks. generelle bankrelaterede emner kan afvises. TPP'erne opfordres herudover til ikke at kontakte ASPSP'ernes øvrige supportfunktioner, for at få svar på API-relaterede spørgsmål. Derudover er der enighed om, at TPP'er bør undersøge muligheden for i større omfang at kunne supportere brugere, så disse ikke i første omgang henvender sig hos ASPSP'en. Emnet forventes drøftet nærmere på kommende møder i API Forum med henblik på at undersøge, om der kan opnås yderligere enighed om god praksis for, hvilken type support TPP'er kan forvente fra ASPSP'erne sammenlignet med supporten på de brugervendte interfaces.

I tillæg hertil har TPP'erne et ønske om adgang til et centralt register eller lignende, hvor samlet information om API'ers driftsmæssige problemer fremgår. API Forum vil forventeligt drøfte muligheden herfor, samt hvad god praksis er på området.

God praksis for information om driftshændelser og support til fejlrettelse indebærer, at:

- TPP'er efter bedste evne medsender de informationer som er angivet i skabelonen for TPP-henvendelser.
- ASPSP'er bekræfter TPP'ers indberetning og følger hurtigst muligt op med oplysninger om, hvorvidt opgaven forsøges løst, samt så snart det er muligt, hvornår en løsning forventes implementeret.

- ASPSP'er, i det omfang det er muligt, informerer om planlagt nedetid. Informationen bør i udgangspunktet være tilgængelig for TPP'er senest to døgn før selve nedetiden indtræffer.

- ASPSP'er aktivt sender push-notifikationer med information om akutte driftshændelser, planlagt nedetid og fejl i API'erne ud til TPP'erne, eventuelt på e-mail.

- TPP'er tilmelder sig selv hos ASPSP'er, og sørger for at opdatere deres kontaktinformation for at kunne modtage push-notifikationerne.

- TPP'er kun benytter ASPSP'ers API-support til API-relaterede henvendelser, og ikke kontakter ASPSP'ers andre supportfunktioner for at få svar på API-relaterede henvendelser.

- TPP'er i større udstrækning søger at supportere egne brugere.

Håndtering af certifikater

Gældende ret og behov for fælles forståelse
Forordningen fastslår i artikel 30, stk. 1, litra a, at ASPSP'er skal stille et interface til rådighed, som giver TPP'er mulighed for at identificere sig overfor ASPSP'en, når TPP'er skal tilgå brugeres online betalingskonti hos ASPSP'en. Forordningen specificerer i artikel 34, at denne identifikation og kommunikation mellem ASPSP'er og TPP'er skal ske ved brug af kvalificerede certifikater, også kaldet eIDAS[6]-certifikater. Ved at benytte eIDAS-certifikater kan en TPP påvise overfor en hvilken som helst ASPSP, at TPP'en har ret til at tilgå data fra brugernes online betalingskonti via ASPSP'ens PSD2-API. Dette forudsætter også, at TPP'en har indhentet brugerens udtrykkelige samtykke.

TPP'er og ASPSP'er udveksler eIDAS-certifikater som en del af onboardingprocessen. Lovgivningen specificerer dog ikke yderligere, hvordan denne onboarding af TPP'er skal foregå. Det giver anledning til forskellig praksis blandt ASPSP'erne.

Herudover udløber et eIDAS-certifikat efter få år og skal derfor jævnligt fornyes. Lovgivningen specificerer ikke en nærmere proces for fornyelse af eIDAS-certifikater, hvilket giver anledning til problemstillinger i praksis.

Drøftelser i forummet
TPP'erne fremhæver, at de enkelte ASPSP'er har forskellige procedurer for onboarding og fornyelse af certifikater. TPP'er opfordrer til i videst muligt omfang at ensarte praksis på tværs af ASPSP'erne. ASPSP'erne har forklaret, at forskelle i processerne blandt andet skyldes, at de bagvedliggende systemer er forskellige. Det er derfor for nuværende ikke muligt at imødekomme ønsket om ensartede onboardingprocesser mellem ASPSP'erne. TPP'erne opfordrer herudover ASPSP'erne til at stille klare oplysninger til rådighed om deres respektive procedurer. ASPSP'erne er enige i, at der er behov for at øge niveauet for vejledning i disse procedurer og derved stille nødvendige oplysninger til rådighed for TPP'er.

TPP'erne oplever, at processen ved onboarding og fornyelse af eIDAS-certifikater er besværlig. TPP'erne fremhæver særligt, at der er en udpræget grad af manuelle processer, som ikke for dem virker nødvendige. TPP'erne har fremhævet, at man med fordel kan tænke fornyelse af certifikater ind i det grundlæggende design af API'erne. Der er generelt et ønske hos både ASPSP'er og TPP'er om yderligere at automatisere processerne ved registrering og udskiftning af certifikater, da manuelle procedurer er ressourcekrævende for alle parter, øger risikoen for fejl og skaber usikkerhed om driftsstabiliteten hos TPP'erne. Det vil løbende blive drøftet i API Forum, hvordan dette kan gøres bedst.

[6] Kravene til disse certifikater er nærmere specificeret i forordning 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked.

ASPSP'erne opfordrer generelt TPP'erne til at igangsætte processen i god tid, når TPP'erne ønsker at udskifte deres certifikat, eller når en TPP ønsker at skifte certifikatudbyder. Denne varsling skal sikre, at ASPSP'en bedre kan assistere, hvis der skulle opstå behov herfor.

TPP'erne fremhæver herudover et behov for at kunne anvende mere end ét certifikat ad gangen, så der er et back-up certifikat, hvis der opstår problemer med det ene certifikat. Det vil også give mulighed for, at en TPP kan aktivere et nyt certifikat forud for deaktivering af et andet certifikat, der snart udløber. Flere ASPSP'er understøtter pr. september 2022 anvendelsen af to eller flere certifikater samtidigt. Andre ASPSP'er har udfordringer med, at deres systemer ikke for nuværende understøtter anvendelsen af flere certifikater samtidigt. Det vil derfor ikke være muligt at tilbyde TPP'er at anvende flere certifikater, før de eksisterende systemer udskiftes eller fundamentalt ændres. Efter indgående diskussioner i forummet er medlemmerne blevet enige om, at det er god praksis at tilstræbe enten en fuldt automatiseret proces ved udskiftning af certifikater eller at tillade mere end ét aktivt certifikat ad gangen. Der er dermed to tilgange, som begge fungerer tilstrækkeligt.

God praksis for håndtering af certifikater indebærer, at:

- ASPSP'er stiller klar information om deres procedurer for onboarding og fornyelse af eIDAS-certifikater til rådighed for TPP'er på eksempelvis APSPS'ens developer portal.
- ASPSP'er i videst muligt omfang automatiserer processer i forbindelse med onboarding og fornyelse af eIDAS-certifikater og derigennem nedbringer behovet for manuelle processer.
- TPP'er igangsætter processen for udveksling af certifikater eller skift af certifikatudbyder i god tid, før et certifikat udløber.
- ASPSP'er tilstræber enten en fuldt automatiseret proces for udskiftning af certifikater, eller at TPP'er kan anvende mere end ét certifikat ad gangen.

Opkaldsbegrænsninger

Gældende ret og behov for fælles forståelse
PSD2-API'erne skal have samme tilgængelighed og ydeevne som de brugervendte interfaces såsom mobilbank og netbank. Det fremgår af artikel 32, stk. 1, i forordningen. På trods af denne forpligtelse er det tydeligt, at brugsscenarierne i praksis for en bruger af f.eks. netbank og en TPP ikke er de samme. En TPP vil eksempelvis ofte have brug for at tilgå mange betalingsoplysninger fra mange brugeres forskellige betalingskonti indenfor meget kort tid, mens det ikke på samme måde er relevant for den enkelte slutbruger. Det er derfor ikke meningsfuldt direkte at sammenligne ydeevne mellem de brugervendte interfaces og PSD2-API'erne.

Drøftelser i forummet
ASPSP'er fremhæver, at de pågældende interfaces og underliggende systemer er bygget til at håndtere datatrafik forbundet med almindelig drift. Det kan derfor være nødvendigt at begrænse meget ressourcekrævende forespørgsler fra TPP'er for at sikre, at systemerne fungerer hensigtsmæssigt for øvrige brugere af samme infrastruktur.

TPP'erne er enige med ASPSP'erne i, at det kan være legitimt at sætte begrænsninger på API-kald for at sikre hensigtsmæssig drift af API'erne. TPP'erne vil generelt gerne forpligte sig til at bruge API'erne på en hensigtsmæssig måde, eksempelvis ved at sprede deres API-kald ud over dagen.

TPP'erne har fremhævet, at det er essentielt for brugeroplevelsen ikke at opleve begrænsninger hvor en slutbruger er aktiv og f.eks. udfører en konkret handling på TPP'ens app. Omvendt kan kald, hvor en slutbruger ikke er aktiv, nedprioriteres til en vis grad hvis der skulle opstå situationer hvor en prioritering er nødvendig. Dette gælder f.eks. indhentning af historiske transaktionsdata, som ofte vil kunne ske løbende uden at forringe servicen til slutbrugeren Det har på API Forum været drøftet, om ASPSP'erne kan udvikle en løsning, så en ASPSP sender push-notifikationer med information til TPP'en om eksempelvis nye transaktioner på en given online betalingskonto, som TPP'en har ret til at tilgå og modtage data fra. På den måde kan ASPSP'en begrænse unødig trafik, da TPP'en ikke løbende skal kalde API'et for at finde ud af, om der er kommet ny data. For nuværende vurderer API Forum, at den bedste løsning er, at TPP'en fortsat løbende kalder API'et for at afdække, om der er sket ændringer siden foregående kald. API Forum kan vælge at tage emnet op i fremtiden.

God praksis for opkaldsbegrænsninger indebærer, at:

- ASPSP'er gør gennemskuelig information om eventuelle API opkaldsbegrænsninger tilgængelig for TPP'er. God praksis for opkaldsbegrænsninger skal drøftes nærmere i API Forum

- TPP'er fordeler så vidt muligt sine API-kald ud over dagen på en måde, som mindsker spidsbelastning af API'er