P R O M E M O R I A

Datum 2018-12-03
Författare **Finansinspektionen**

FI Dnr 18-9872

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Finansinspektionens syn på frågor om det andra betaltjänstdirektivet som diskuterades på branschmöte

Bakgrund

Finansinspektionen (FI) redogör i detta dokument för hur myndigheten ser på de frågor om det andra betaltjänstdirektivet, PSD 2, som diskuterades på rundabordssamtalet med finansiella företag, branschföreningar och myndigheter i juni 2018. Totalt medverkade 18 aktörer.

Syftet med samtalet var att identifiera frågor och potentiella hinder som de olika aktörerna på finansmarknaden upplever till följd av det nya betaltjänstregelverket, men även att diskutera vilka konsekvenser som utmaningarna kan medföra och branschens förslag på lösningar. FI ger nu sin syn på de frågor som diskuterades under mötet.

Tidigare har FI publicerat minnesanteckningar från rundabordssamtalet[1].

Allmänt om frågor om andra betaltjänstdirektivet och de tekniska standarder som reglerar området

Med anledning av genomförandet av det andra betaltjänstdirektivet har Europeiska Bankmyndigheten (EBA) utfärdat ett antal riktlinjer, och tekniska standarder (RTS)[2] från EU-kommissionen. Ytterligare ett antal riktlinjer från EBA är fortfarande under utveckling men väntas bli klara under hösten 2019[3].

FI har endast mandat att tillämpa regler som beslutas på EU-nivå. Men i vissa fall har myndigheten rätt att utfärda föreskrifter om dessa regler efter att ha fått bemyndigande från regeringen i lag eller förordning. Det pågår ett löpande arbete hos EBA för att förtydliga regelverket, ett arbete där även FI medverkar. EBA har på sin webbplats bland annat publicerat en sida[4] för frågor och svar (Single Rulebook, Q&A) som syftar till att förtydliga och svara på viktiga

[1] https://www.fi.se/sv/publicerat/nyheter/2018/anteckningar-fran-branschsamtal-om-andra-betaltjanstdirektivet/
[2] Genomförandeförordning (EU) 2018/389 om stark kundautentisering och säker kommunikation (RTS)
[3] https://www.fi.se/sv/bank/andra-betaltjanstdirektivet-psd-2/eu-regler-for-psd-2/
[4] http://www.eba.europa.eu/single-rule-book-qa/-/qna/search/legalAct/6

frågor. FI bistår i arbetet med att svara på frågor och granska inkomna förslag till svar från EBA eller andra medlemsstater.

Identifierade utmaningar:

Ansvar vid flerpartsförhållanden i fråga om kundens data

Det andra betaltjänstdirektivet öppnar för möjligheten att ge tredjepartsleverantörer tillgång till kunddata, men regelverket innehåller också begränsningar för hur tredjepartsleverantörerna får använda en betaltjänstanvändares data. Tredjepartsleverantörers skyldigheter i detta avseende regleras bland annat i betaltjänstlagens femte kapitel. En förutsättning för att en leverantör av en kontoinformationstjänst ska kunna tillhandahålla sin tjänst är att leverantören har betaltjänstanvändarens uttryckliga godkännande [5]. På motsvarande sätt för betalningsinitieringstjänster krävs samtycke från betalaren för att en betalningstransaktion ska få genomföras och betraktas som korrekt utförd[6].

Kontoförvaltande institut ska förlita sig på att en auktoriserad tredjepartsleverantör har inhämtat det samtycke som krävs. Vidare får leverantörer av betalningsinitieringstjänster och kontoinformationstjänster inte använda, ha tillgång till eller lagra uppgifter om betaltjänstanvändaren för andra ändamål än för att tillhandahålla tjänsten[7].

Det finns också bestämmelser om hur leverantörer av betalningsinitieringstjänster ska skydda information om betaltjänstanvändaren som leverantören har fått i samband med tillhandahållandet av tjänsten. För att en leverantör ska få lämna ut sådan information till betalningsmottagaren krävs även här användarens uttryckliga godkännande.[8]

Detta kan komma att bli föremål för FI:s löpande tillsyn, och myndigheten kommer att samråda med Datainspektionen.

Stark kundautentisering och omdirigering

Metod för stark kundautentisering

Ett av de krav som återfinns i de tekniska standarder (RTS) som träder i kraft 14 september 2019, berör vilka metoder för genomförande av kundautentisering som ett kontoförvaltande institut måste tillhandahålla åt en tredjepartsbetaltjänstleverantör. Vilken autentiseringsmetod, eller kombination av metoder, det kontoförvaltande institutet behöver tillhandhålla beror på

[5] 5 kap. 15 § 1 lag (2010:751) om betaltjänster (LBT).
[6] 5 kap. 3 § LBT.
[7] 5 kap. 8 § 4 LBT och 5 kap. 15 § 3 LBT.
[8] 5 kap. 9 § 2 LBT.

vilken autentiseringsmetod det kontoförvaltande institutet tillhandhåller åt sina egna betaltjänstanvändare[9].

Vidare ska det kontoförvaltande institutet när det utvecklar sina särskilda gränssnitt skapa en autentiseringslösning som gör det möjligt för leverantören av betalningsinitieringstjänster och leverantören av kontoinformationstjänster att förlita sig på de autentiseringsförfaranden som det kontoförvaltande institutet tillhandahåller betaltjänstanvändaren[10].

Kan omdirigering ses som ett otillåtet hinder?

Så kallad omdirigering har varit en omdiskuterad företeelse. I artikel 32.3 RTS nämns införande av omdirigeringar till den kontoförvaltande betaltjänstleverantörens autentisering eller andra funktioner som något som kan tänkas utgöra ett otillåtet hinder beroende på dess utformning. Omdirigering behöver inte utgöra ett hinder i sig. Däremot uttrycks det i RTS[11] att omdirigering *kan* anses utgöra ett hinder om det implementeras på ett sådant sätt att det utgör en begräsning eller ett hinder för tredjepartsleverantören.

Det kommer sannolikt att finnas ett visst utrymme för de nationella behöriga myndigheterna att göra olika bedömningar om vad som kan tänkas utgöra ett hinder. Det blir därmed en bedömning från fall till fall och FI kan komma att följa upp detta i sin löpande tillsyn.

Undantag från beredskapsmekanism och processer för att godkänna särskilda gränssnitt

Godkännande av särskilda gränssnitt

FI arbetar med att ta fram myndighetens interna process för godkännande av särskilda gränssnitt och undantag från beredskapsmekanism. Detta är något som har hög prioritet. Vi har som ambition att publicera hur dessa ansökningsförfaranden ska gå till i början av 2019.

Artikel 33.6 RTS anger vilka kriterier som ska vara uppfyllda för att det ska finnas förutsättningar att bevilja ett institut undantag från kravet på beredskapsmekanism. Det är dessa krav vi kommer att utgå från i bedömningen.

I fråga om hur kriteriet för undantag ”använts i stor utsträckning” ska tolkas enligt RTS 33.6 c), kommer denna fråga hanteras i riktlinjer som EBA avser att fastställa inom kort. Enligt de föreslagna riktlinjerna kommer det att finnas

[9] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC punkt 50
[10] Andra betaltjänstdirektivet artikel 97.5.
[11] Genomförandeförordning (EU) 2018/389 om stark kundautentisering och säker kommunikation (RTS) artikel 32.3

alternativa metoder för att visa på att kraven har uppfyllts som tar hänsyn till att det i vissa fall inte är möjligt att visa på ett faktiskt användande.

Även risken för att godkännanden och bedömningar av särskilda gränssnitt görs på olika sätt i olika medlemsstater har varit föremål för diskussion. Det kan noteras att denna fråga hanteras i de föreslagna riktlinjerna från EBA och att ambitionen är att bedömningarna mellan de olika medlemsstaterna ska skilja sig från varandra så lite som möjligt.

Undantag från beredskapsmekanism

Många frågor under rundabordssamtalet berörde undantag för ett kontoförvaltande institut att behöva tillhandahålla en beredskapsmekanism. I artikel 33.6 RTS beskrivs vilka förutsättningar som gäller för att ett kontoförvaltande institut ska kunna ansöka om möjlighet till undantag från att tillhandahålla en sådan. FI kan efter ansökan från ett kontoförvaltande institut bevilja undantag från att behöva tillhandahålla en beredskapsmekanism. Institutet måste i sin ansökan kunna styrka med underlag och data att det uppfyller de kriterier som ställs i artikel 33.6 och ange hur det har gjort bedömningen att de anses vara uppfyllda. Syftet med beredskapsmekanismen är att ge tredjepartsaktörer en möjlighet att fortsätta sin verksamhet även om de dedikerade gränssnitten har driftsstörning. Således måste institutet anpassa sina kundgränssnitt så att en tredjepart kan autentisera sig enligt artikel 34 även om inte institutet har beviljats undantag enligt 33.6.

Om FI återkallar ett beslut om undantag enligt 33.7 ska beredskapsmekanismen upprättas så snart som möjligt, dock senast inom två månader från beslut om återkallelse.

Verifiering av tredjepartsleverantörer

FI har i samarbete med EBA deltagit i arbetet med att ändra på standardiseringsorganet för telekommunikation i Europas, ETSI (European Telecommunications Standards Institute) standard som ska användas. Ändringen medför en standardisering av de uppgifter som ska finnas i det betrodda certifikatet som en tredjepartsleverantör ska använda vid autentisering. Dessa uppgifter kan ett kontoförvaltande institut använda för att verifiera om en tredjepartsleverantör har de tillstånd som krävs. Betrodda certifikat kan endast utfärdas av betrodda certifikatutställare[12] som står under tillsyn av behörig myndighet för eIDAS förordningen[13]. I Sverige är det Post- och Telestyrelsen (PTS) som är behörig myndighet och utövar tillsyn enligt denna förordning.

[12] https://webgate.ec.europa.eu/tl-browser/#/
[13] https://elegnamnden.se/eidas/omeidasforordningen.4.4498694515fe27cdbcf240.html

När en betrodd certifikatutställare utfärdar ett certifikat för en tredjepartsleverantör, ska den informera den behöriga tillsynsmyndigheten i det land tredjepartsleverantören är auktoriserad.

Såväl FI:s som EBA:s företagsregister visar aktuell information om vilka bolag som är auktoriserade. Kontoförvaltande institut uppmanas att regelbundet ta del av aktuell information om de bolag som är verksamma på den svenska marknaden.

Om FI återkallar en tredjepartsleverantörs tillstånd, eller om tredjepartsleverantören själv återkallar sitt tillstånd, kan myndigheten begära att den betrodda certifikatutställaren ogiltigförklarar det utfärdade certifikatet.

Avslutande diskussion

Flera delar av det andra betaltjänstdirektivet är redan i kraft i dag, medan en stor del, däribland RTS, börjar gälla nästa år. Vårt arbete med genomförandet pågår och kommer att fortsätta under 2019. FI eftersträvar att löpande utbyta information och kommunicera med branschen under genomförandet för att tillhandahålla vägledning i den mån det går. Vi har även som ambition att under våren 2019 bjuda in till ett nytt informationsmöte om PSD 2 som helhet, alternativt om specifika områden av genomförandet av regelverket och tillhörande tekniska standarder.