FI-FORUM

Nya regler för betaltjänster

FI-forum

7 juni 2018

FI-FORUM

Inledning

Stig Johansson

Senior finansinspektör, Marknadsuppförandetillsyn

Agenda

- Introduktion
- Vilka berörs
- Vad är nytt
- Nya betaltjänstlagen och GDPR
- Rapporteringskraven i praktiken
- Relaterade internationella regelverk
- Tredjepartsleverantörer – rättigheter och skyldigheter
- Krav på hantering av operativa risker och säkerhetsrisker
- Frågor

Varför PSD 2?

Syftet med direktivet

- Göra det enklare och säkrare att använda internetbaserade betaltjänster.
- Bättre konsumentskydd vid bedrägeri, missbruk och betalningsproblem.
- Främja innovativa mobila och internet baserade betaltjänster.
- Stärka konsumenters rättigheter.

Källa: EC sammanfattning av PSD 2

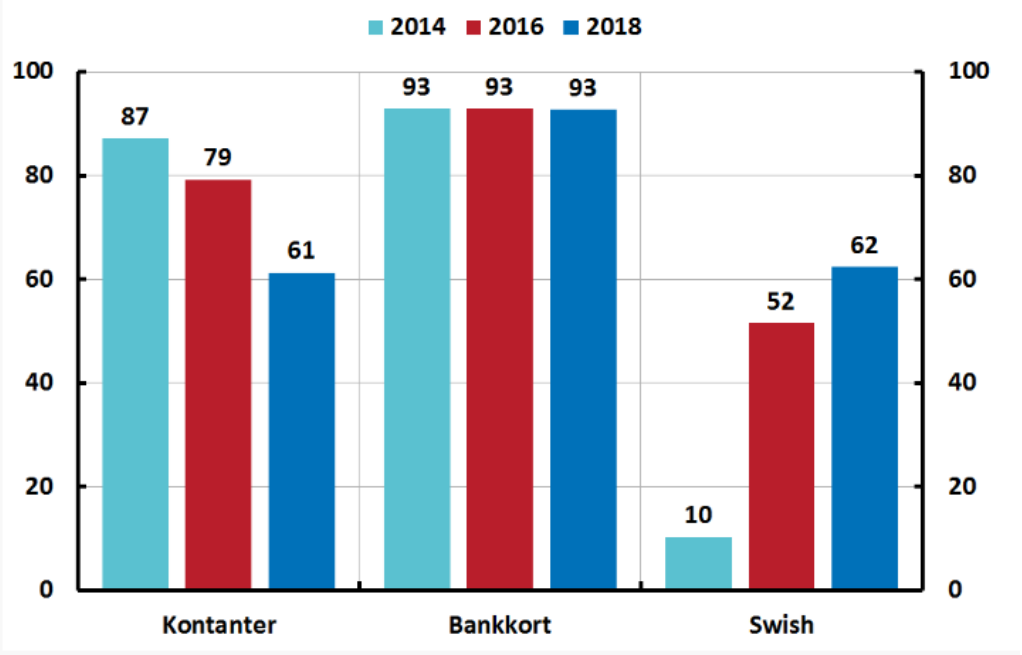
Konsumenters beteende…

…ändras

Betalningsstatistik

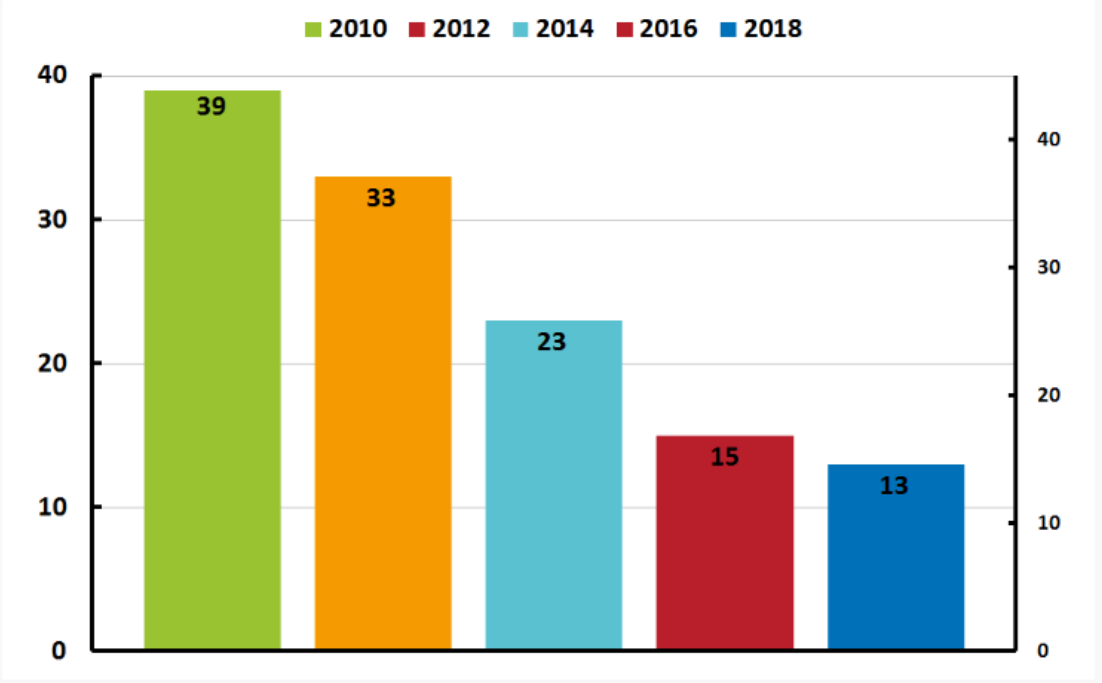
Vilka betalsätt har du använt under den senaste månaden?

Användningen av Swish har ökat oerhört snabbt under de senaste åren. Parallellt har andelen hushåll som uppger att de använt kontanter under den senaste månaden fortsatt att minska.



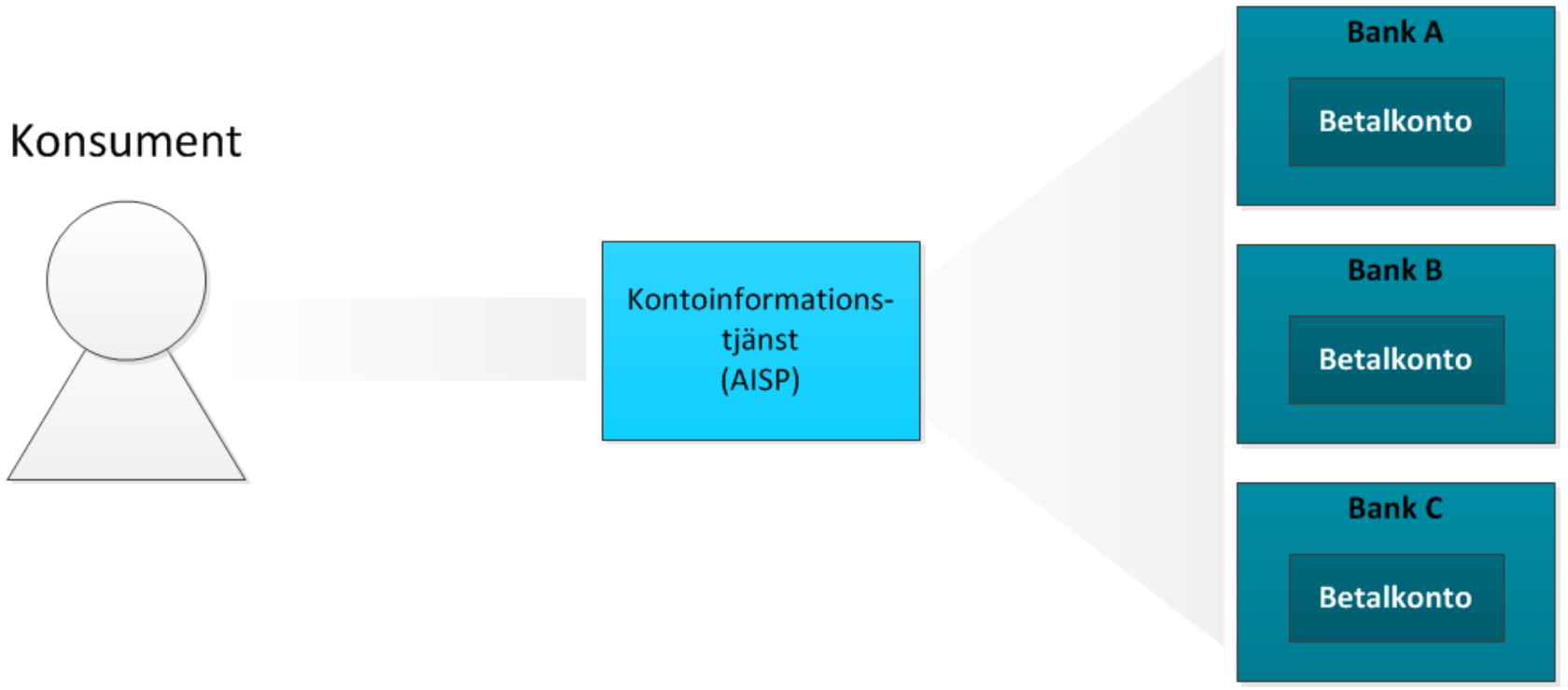
Andel som svarat att de betalade kontant vid sitt senaste köp

På åtta år har andelen svarande som betalat med kontanter vid sitt senaste köp minskat från cirka 40 procent till 13 procent.

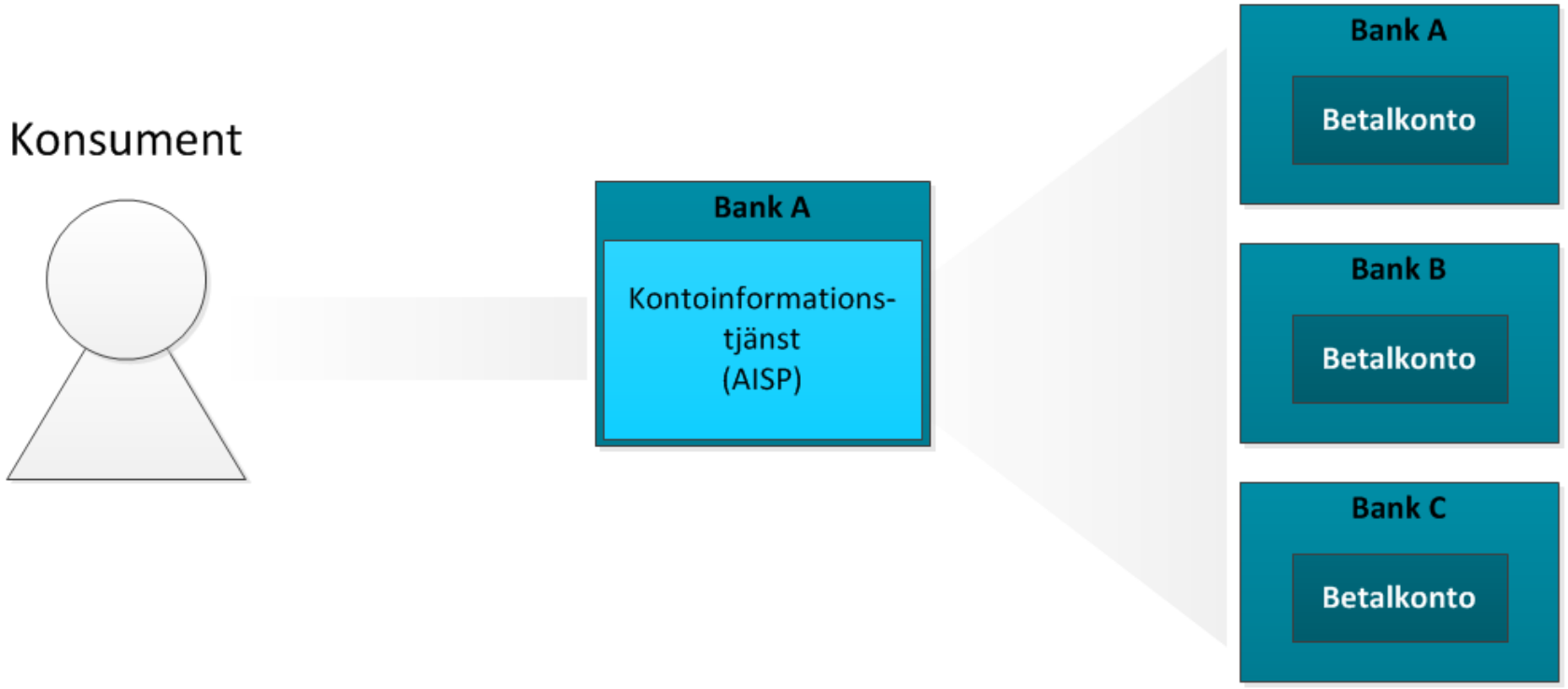


Källa: Riksbanken 2018, Betalningsstatistik

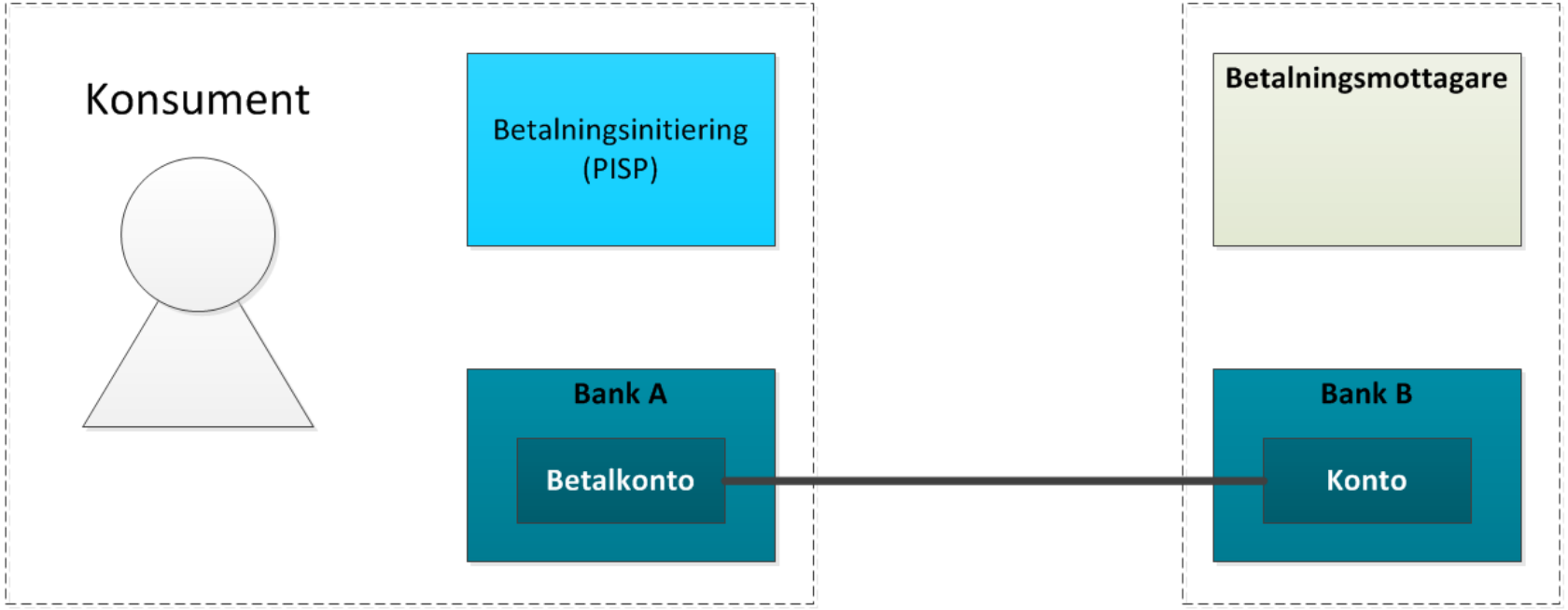
Kontoinformationstjänst



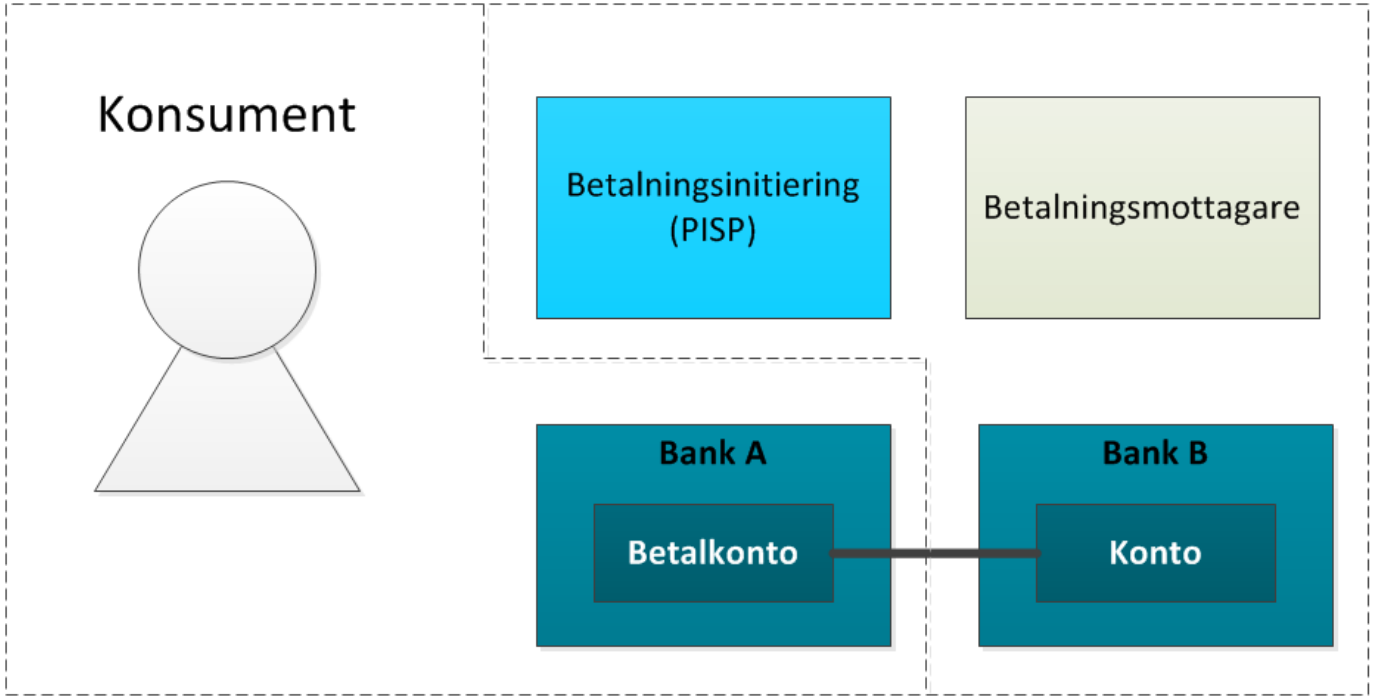
Kontoinformationstjänst



Betalningsinitiering



Betalningsinitiering



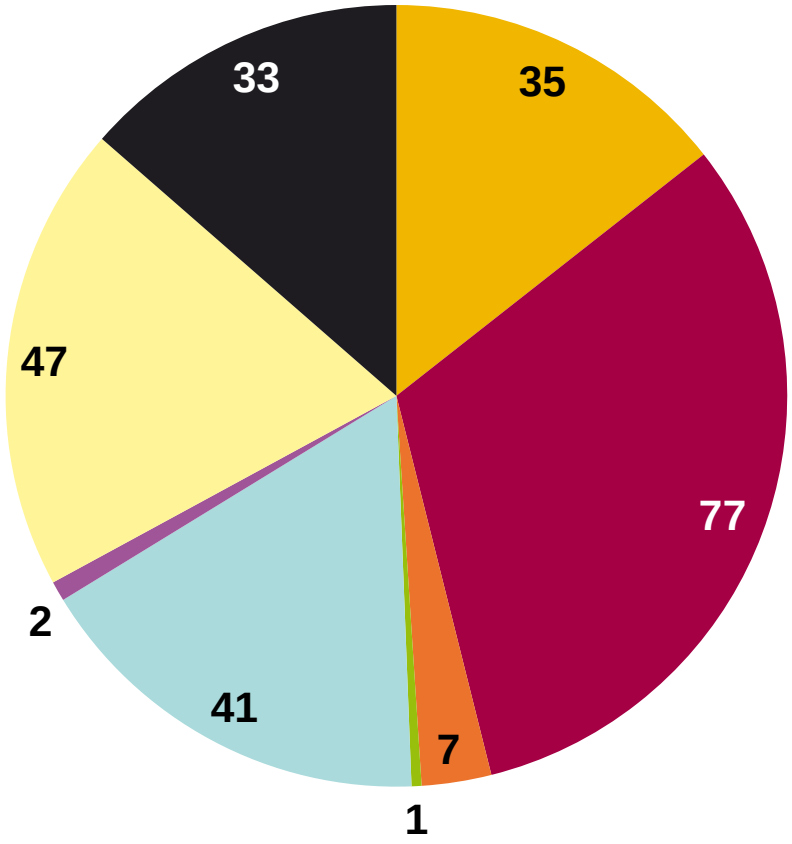
FI:s nya föreskrifter

David Lothigius

Jurist, Marknadsuppföranderätt


Nya regler från 1 maj

Vilka företag omfattas?

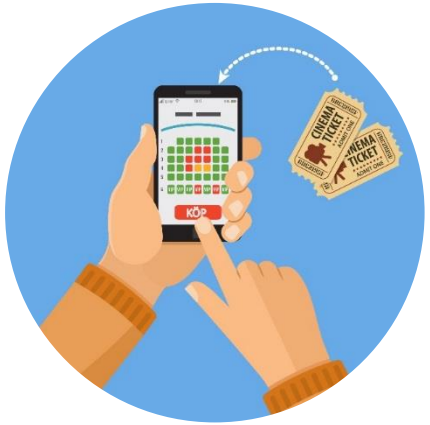


- Betalningsinstitut
- Registrerade betaltjänstleverantörer
- Institut för elektroniska pengar
- Registrerade utgivare av elektroniska pengar
- Banker
- Medlemsbanker
- Sparbanker
- Kreditmarknadsbolag

Anm: Diagrammet visar 242 betaltjänstleverantörer (mars 2018)

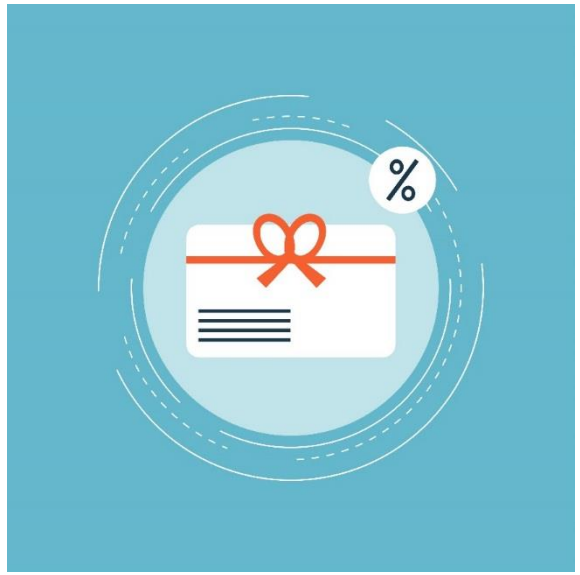
Anmälningsskyldig verksamhet

Kundkort med betalfunktion



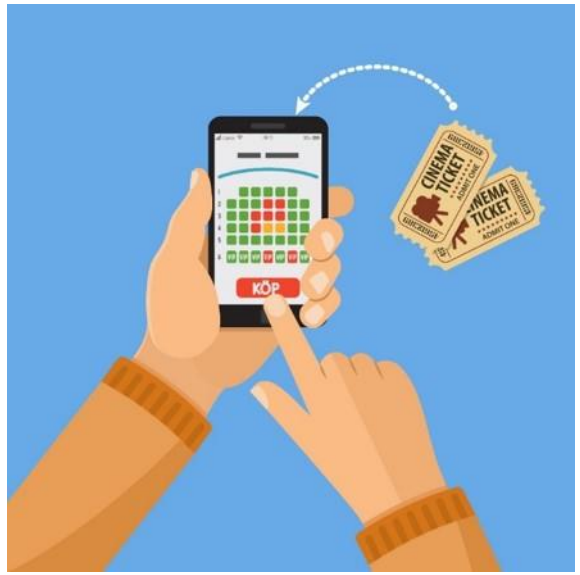
Premiumtjänster

Kundkort med betalfunktion



- Tjänster som baseras på ***betalningsinstrument*** som enbart kan utnyttjas inom ett ***begränsat nätverk*****.**
  - Presentkort, bränslekort, medlemskort, busskort, rabattkuponger för måltider
- Anmälningsskyldighet vid en omsättning som motsvarar minst 1 miljon euro.
- Vid anmälan ska företaget redogöra för var instrumentet kan användas och vilka varor eller tjänster som kan köpas.

Premiumtjänster



- Tjänster som genomförs via en leverantör av elektroniska nätverk (operatörsfakturering).
  - Digitalt innehåll och röstbaserade tjänster (filmklipp, musik, spel, omröstningar)
- Anmälningsplikt från första kronan.
- Takbelopp på 50 euro per inköp eller 300 euro per månad.
- FI har infört krav på årligt revisorsintyg.

Nya tredjepartsleverantörer

Betalnings-
initieringstjänster

Konto-
informationstjänster

Betalningsinitieringstjänster

- Måste vara ett företag med tillstånd (kan inte ansöka om undantag).
- Krav på ansvarsförsäkring.
- Startkapitalkrav och kapitalkrav motsvarande minst 50 000 euro.

Kontoinformationstjänster

- ”Registrerad betaltjänstleverantör” räcker.
- Inget kapitalkrav.
- Får gränsöverskrida inom EES direktiv, genom ombud eller filial.

FI:s nya föreskrifter och allmänna råd

- **FFFS 2018:4** om verksamhet för betaltjänstleverantörer
  - Ny föreskrift
  - Gäller för alla betaltjänstleverantörer oavsett typ.
- **FFFS 2018:6** (ändringsföreskrift)
  - Ändrar FFFS 2010:3 om betalningsinstitut och registrerade betaltjänstleverantörer.
- **2018:7** (ändringsföreskrift)
  - Ändrar FFFS 2011:49 om institut för elektroniska pengar och registrerade utgivare.
- **FFFS 2018:5** allmänt råd om rapportering av väsentlig betydelse
  - Nytt allmänt råd
  - Gäller *inte* för betaltjänstleverantörer i deras betaltjänstverksamhet (2015:15 upphör att gälla)

Nya FFFS 2018:4

- Nya regler om rapportering till FI.
- Nya regler om krav på system för operativa risker och säkerhetsrisker.
- Från FFFS 2017:1 om vissa betalkonton har vi överfört följande delar:
  - information till konsumenter
  - byte av betalkonto
  - rapportering till FI
- Nya regler om klagomålshantering.

Nya rapporteringskrav

Nya rapporteringskrav

- Periodisk rapportering
- Händelsestyrd rapportering
- Hanteringen på FI
- Översikt kommer publiceras på **fi.se/psd2**

Operativa risker och säkerhetsrisker

- Rapportera en gång per år.
- Första rapporteringstillfället är senast den 21 februari 2019.

1. Ge en aktuell och övergripande bedömning av operativa risker och säkerhetsrisker.
2. Beskriva vilka säkerhetsåtgärder som finns för att hantera dessa risker.
3. Lämna en bedömning av hur lämpliga säkerhetsåtgärderna är.

- Bör skickas i krypterat mejl till finansinspektionen@fi.se

Statistik om svikliga förfaranden

- Rapportera första gången 21 augusti 2019.
- Därefter två gånger per år senast den 21 februari och 21 augusti.
  – Undantag: registrerade betaltjänstleverantörer och registrerade utgivare av elektroniska pengar ska endast rapportera en gång per år, 21 februari.
- Vad ska rapporteras och vad ingår i svikliga förfaranden?

  Betalningstransaktioner som
  – inte auktoriserats av betalaren,
  – betalaren nekar till att denne har auktoriserat, eller
  – genomförts genom att betalaren manipulerats.
- Riktlinjer för rapportering av statistiska uppgifter om svikliga förfaranden – under utveckling

Rapporteringskrav för betalkonton

Situation	Regel / undantag	Förutsättningar	Rapporteras
ASPSP återställer inte betalkonto	Omedelbar återställning. Vid misstanke om behörighet ges skälig utredningstid	Anledning att misstänka att transaktionen är behörig	Rapporteras krypterat till finansinspektionen@fi.se FI Dnr 18-8618
TPP vägras åtkomst till kundens betalkonto	ASPSP ska ge TPP tillträde. Vid misstanke om obehörig åtkomst eller initiering får TPP vägras åtkomst.	Objektivt motiverade och tillräckligt underbyggda skäl	Rapporteras krypterat till finansinspektionen@fi.se FI Dnr 18-8619
TPP vägras åtkomst till kreditinstituts betalkontotjänster	ASPSP ska ge TPP tillgång till betalkontotjänster. KI som nekar ska underrätta FI.	Tillgång på objektiva, icke-diskriminerande och proportionella grunder. Samma krav för alla.	Rapporteras krypterat till finansinspektionen@fi.se FI Dnr 18-8620

Incidentrapportering

Vad?	När?	Hur?
Allvarliga incidenter och säkerhetsincidenter.	Inom max fyra (4) timmar – enlig lagen ” snart det kan ske”.	Krypterad e-post till FI via särskild mejl incidentrapportering.betaltjanster@fi.se Särskild blankett på fi.se *I vissa fall ska betaltjänstleverantörerna informera användarna.*
Exempel: En tredje-partsleverantör kan inte komma in via bankens eller kreditinstitutets gränssnitt.	Därefter rapportering vid förändringar, men senast inom tre dagar från det att inledande rapport har skickats in.	Formulär A-del Formulär B-del
Nedtrappning: Hur rapporteras en incident som inte blev ”allvarlig”, men som kunde blivit det?	Avslutande rapport skickas in senast två veckor efter det att driften kan anses vara normal igen.	Riktlinje 2.21 Kryssa i att incidenten har omkategoriserats på försättsbladet och ange skälen i C-delen.

Kriterier för incidentrapportering

Exempel på bedömningskriterier

- Berörda transaktioner
- Berörda betaltjänstanvändare
- Driftavbrott
- Ekonomiska effekter
- Hög intern upptrappningsnivå
- Andra betaltjänstleverantörer eller relevant infrastruktur som kan beröras
- Effekter på anseendet

Anm: EBA/GL/2017/17

Bedömningskriterier och trösklar

Kriterier	Lägre effektnivå		Högre effektnivå
Berörda transaktioner	> 10 % av betaltjänstleverantörerns normala transaktionsnivå (vad gäller antalet transaktioner) **och** 100 000 euro	>	> 25 % av betaltjänstleverantörens normala transaktionsnivå (vad gäller antalet transaktioner) **eller** > 5 miljoner euro
Berörda betaltjänstanvändare	> 5000 **och** 10 % av betaltjänstleverantörens betaltjänstanvändare	>	> 50 000 **eller** > 25 % av betaltjänstleverantörens betaltjänstanvändare
Driftavbrott	> 2 timmar		Ej tillämpligt
Ekonomiska effekter	Ej tillämpligt		> Max. (0,1 % av primärkapitalet, * 200 000 euro) **eller** > 5 miljoner euro
Hög upptrappningsnivå	Ja		Ja, och krisläge (eller liknande) kommer sannolikt att utlysas
Andra betaltjänstleverantörer eller relevanta infrastrukturer som kan beröras	Ja		Ej tillämpligt
Effekter på anseendet	Ja		Ej tillämpligt

Anm: Se EBA/GL/2017/17 riktlinje 1 s. 10.

Betaltjänster och dataskydd

Personuppgifter och tillgång till data

- Betaltjänstdirektivet sätter inte dataskyddsförordningen ur spel när det gäller personuppgifter.
- Bägge regelverken ställer krav på att det krävs samtycke för att få hantera kundernas personuppgifter.
- Principen om dataminimering: den data som tredjepartsleverantörerna hanterar ska vara relevant och begränsad till vad som är nödvändigt för att kunna utföra den aktuella betaltjänsten.
- Tillgång till kontoinformation – stöd i bägge regelverken.


Gällande EU-regler

EBA:s standarder och riktlinjer

Riktlinjer och tekniska standarder under PSD 2	Benämning på engelska	Förkortning	Artikel	Länk	Status
Tekniska standarder för underrättelser om gränsöverskridande verksamhet	Regulatory Technical Standards (RTS) on Passporting Notifications under PSD2	RTS(EU)2017/2055	28.5	http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELE	Ikraft
Riktlinjer för fastställande av minimibelopp för ansvarsförsäkring eller annan jämförbar garanti	Guidelines on Professional Indemnity Insurance under PSD2 (PII)	EBA/GL/2017/08	5.4	https://www.eba.europa.eu/documents/10180/1956339/Guidelines+on+PII+under+PSD2+	Ikraft
Riktlinjer för rapportering vid allvarliga incidenter	Guidelines on Incident Reporting	EBA/GL/2017/10	96.3	https://www.eba.europa.eu/documents/10180/2066978/Gui	Ikraft
Riktlinjer för auktorisation och registrering	Guidelines on Authorisation of payment institutions	EBA/GL/2017/09	5.5	https://www.eba.europa.eu/documents/10180/2015792/Guidelines+on+Authorisations+o	Ikraft
Riktlinjer för klagomålshantering vid påstådda överträdelser	Guidelines on Complaints Procedures by Competent Authorities	EBA/GL/2017/13	100.6	https://www.eba.europa.eu/documents/10180/2053197/Guidelines+on+complaint+proce	Ikraft
Tekniska standarder för stark kundautentisering och säker kommunikation	Regulatory Technical Standards (RTS) on strong customer authentication and secure communication	RTS(EU)2018/839	98.1	http://ec.europa.eu/info/law/better-regulation/initiatives/c-2017-7782_en	Ikraft
Riktlinjer för säkerhetsåtgärder för operativa risker och säkerhetsrisker	Guidelines on Operational and Security Measures	EBA/GL/2017/17	95.3	https://www.eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+me	Ikraft
Tekniska standarder för central kontaktpunkt	RTS on Central Contact Points	EBA/RTS/2017/09	29.5	http://www.eba.europa.eu/regulation-and-policy/payment-	Under utveckling
Tekniska standarder för tillsyn och genomförande om format, struktur och information i register hos EBA	Regulatory and Implementing Technical Standards (RTS and ITS) on Technical Requirements for a Central Register	EBA/RTS/2017/10	15.4-5	http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/technical-standards-	Under utveckling
Riktlinjer för rapportering av statistiska uppgifter om svikliga förfaranden	Guidelines on fraud reporting	EBA/GL/2018/XX	96.6	http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-	Under utveckling
Tekniska standarder för tillsyn över betalninsginstitut som tillhandahåller gränsöverskridande betaltjänster	Regulatory Technical Standards on home-host coordination	EBA/RTS/2018/XX	29.6	http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/rts-on-home-host-	Under utveckling

RTS = Regulatory Technical Standards - tekniska standarder för tillsyn (artikel 10 i Ebaförordningen)
GL = Guidelines - riktlinjer

Föreskrifter och allmänna råd

Föreskrifter	Allmänna råd	Upphäver eller ändrar
2018:4 om verksamhet för betaltjänstleverantörer		Upphäver FFFS 2017:1 om vissa betalkonton
	2018:5 om rapportering av händelser av väsentlig betydelse	Ersätter 2015:15 om rapportering av väsentlig betydelse
2018:6 Ändringsföreskrift		Ändrar 2010:3 om betalningsinstitut och registrerade betaltjänst-leverantörer
2018:7 Ändringsföreskrift		Ändrar 2011:49 om institut för elektroniska pengar och registrerade utgivare

Operativa risker – tillämpning av föreskrifter

Maximilian Görtz

Riskexpert, Kredit och operativa risker

Fyra riskområden

Struktur

Riskidentifiering

Kommunikation

Riskhantering
och kontroll

Snarlik men inte identisk

Text FFFS 2018:4	FFFS 2018:4	FFFS 2014:1	FFFS 2014:4	FFFS 2014:5
1. definiera och tilldela de ansvarsfunktioner som leverantören bedömer är nödvändiga för att genomföra säkerhetsåtgärderna,	5 kap. 1 § 1 p.	2 kap. 1 § 3 p	-	2 kap. 3 §
2. fastställa processer, rutiner och system för att identifiera, mäta, övervaka och hantera riskerna som är förknippade med leverantörens betaltjänstverksamhet,	5 kap. 1 § 2 p.	5 kap. 1-3 §§	2 kap. 2 § 3 kap. 2 §	2 kap. 7 §
3. göra en riskbedömning av betaltjänsterna och ta fram en beskrivning av de säkerhetsåtgärder som ska skydda betaltjänstanvändarna mot de risker som identifierats, bland annat mot bedrägerier och olaglig användning av känsliga uppgifter och personuppgifter,	5 kap. 1 § 3 p.	5 kap. 10-11 §§	3 kap. 1-3 §§	2 kap. 6 §
4. ha en intern nivåbaserad modell för att hantera och kontrollera risker i betaltjänstverksamheten,	5 kap. 1 § 4 p.	5 kap. 1-2 §§	-	-
5. ta fram en beskrivning av hur leverantören säkerställer att de operativa riskerna och säkerhetsriskerna hanteras när den uppdrar åt någon annan att utföra en del av betaltjänstverksamheten,	5 kap. 1 § 5 p.	10 kap. 2-7 §§	2 kap. 3 §	3 kap. 6 §
6. fastställa en riskaptit för betaltjänstverksamheten samt inventera, klassificera och riskbedöma affärsfunktioner, processer och tillgångar som anses kritiska för verksamheten,	5 kap. 1 § 6 p.	2 kap. 3 §	2 kap. 1 § 5 kap. 1, 7-8 §§	2 kap. 5 §
7. ta fram säkerhetsåtgärder som hanterar konfidentialitet, integritet och tillgänglighet för data och it-system, samt fysisk säkerhet och åtkomstkontroll,	5 kap. 1 § 7 p.	2 kap. 2 §	5 kap. 8-9 §§	2 kap. 8 §
8. se till att verksamheten övervakas för att identifiera oplanerade händelser som leder till operativa eller säkerhetsrelaterade incidenter samt hantera, följa upp och rapportera incidenterna,	5 kap. 1 § 8 p.	5 kap. 5 §	3 kap. 5-6 §§	2 kap. 7 § Inkl. *Allmänna råd*
9. ta fram en plan för kontinuitetshantering, som innefattar en beskrivning av hur verksamheten ska upprätthållas i olika scenarier och hur leverantören ska kommunicera i händelse av kris, testa kontinuitetsplanerna årligen och vid behov uppdatera dem,	5 kap. 1 § 9 p.	2 kap. 9 §	5 kap. 15-23	-
10. ta fram och regelbundet testa kontrollrutiner som säkerställer att säkerhets–åtgärderna är uppdaterade och effektiva,	5 kap. 1 § 10 p.	3 kap. 4 §	-	2 kap. 8 §
11. ta fram en hotbildsanalys för betaltjänstverksamheten och regelbundet utbilda personalen om hur den ska använda beredskapsplaner, kontinuitetsplaner och återställningsplaner och	5 kap. 1 § 11 p.	2 kap. 9 §	5 kap. 21 §	-
12. ta fram och vid behov genomföra processer och rutiner för att vägleda och informera betaltjänstanvändarna om säkerhetsrisker och felmeddelanden som är relaterade till de tillhandahållna betaltjänsterna och betaltjänstanvändarnas möjligheter att avaktivera specifika betalningsfunktioner.	5 kap. 1 § 12 p.	-	-	-


Struktur

Vilka risker finns i din verksamhet?

Riskhantering och kontroll

Kommunikation till kund

FI-FORUM

Teknisk standard (RTS SCA och CSC)

Stig Johansson

Senior finansinspektör, Marknadsuppförandetillsyn

Teknisk standard (RTS SCA och CSC)

- Antagen av EU parlamentet 13 mars 2018.
- Träder i kraft 21 september 2019.
- Särskild gränssnitt för tredjepartsaktörer (Art 32).
- Ansökan om undantag från skyldigheten att upprätta beredskapsmekanism (Art 33.6).
- Certifikat för betrodda tjänster (Art 34).
- Två-faktor autentisering (Stärk kundautentisering).

Nästa steg

- Rundabordssamtal 18 juni
- Podd innan midsommar
- FI återkopplar på rundabordssamtalet under hösten
- Förtydligande via EBA under hösten gällande teknisk standard (RTS SCA och CSC)

Frågor?

Förkortningar

- AISP (Account Information Service Provider) = Kontoinformationstjänst
- ASPSP (Account Servicing Payment Service Provider) = Kontoförvaltande institut
- ITS (Implementing Technical Standards) = Tekniska standarder för genomförande
- PISP (Payment Initiation Service Provider) = Betalningsinitieringstjänst
- PSP (Payment Service Provider) = Betaltjänstleverantör
- PSU (Payment Service User) = Betaltjänstanvändare
- RTS (Regulatory Technical Standards) = Tekniska standarder för tillsyn
- TPP (Third Party Provider) = Tredjepartsbetaltjänstleverantör

Följ oss på fi.se och i sociala medier

twitter.com/finansinsp

soundcloud.com/fipodden

youtube.com/finansinspektionen

flickr.com/finansinspektionen

linkedin.com/company/finansinspektionen

FI-FORUM