EBA/GL/2014/12_Rev1

19 december 2014

Riktlinjer

om säkerhet vid betalningar på internet

Innehåll

Riktlinjer om säkerhet vid betalningar på internet

Riktlinjernas status

Detta dokument innehåller riktlinjer som utfärdats i enlighet med artikel 16 i Europaparlamentets och rådets förordning (EU) nr 1093/2010 av den 24 november 2010 om inrättande av en europeisk tillsynsmyndighet (Europeiska bankmyndigheten), om ändring av beslut nr 716/2009/EG och om upphävande av kommissionens beslut 2009/78/EG (nedan kallad *EBA-förordningen*). I enlighet med artikel 16.3 i EBA-förordningen ska de behöriga myndigheterna och finansinstituten försöka följa riktlinjerna med alla tillgängliga medel.

I riktlinjerna ger Europeiska bankmyndigheten (EBA) sin syn på vad som är lämplig tillsynspraxis inom det europeiska systemet för finansiell tillsyn och på hur unionslagstiftningen bör tillämpas inom ett visst område. EBA förväntar sig därför att alla berörda behöriga myndigheter och finansinstitut följer riktlinjerna. De behöriga myndigheter som omfattas av riktlinjerna bör följa dem genom att på lämpligt sätt införliva dem i sin tillsyn (t.ex. genom att ändra sin rättsliga ram eller sina tillsynsrutiner). Detta gäller även när riktlinjerna främst riktar sig till institutioner.

Rapporteringskrav

I enlighet med artikel 16.3 i EBA-förordningen ska de behöriga myndigheterna underrätta EBA om huruvida de följer eller tänker följa riktlinjerna. I annat fall ska de ange skälen till att inte följa riktlinjerna. Myndigheterna ska underrätta EBA senast den 5 maj 2015. Om de berörda myndigheterna inte underrättat EBA inom denna tidsfrist anser EBA att de inte följer riktlinjerna. Underrättelserna bör ske på formuläret i avsnitt 5 och skickas till compliance@eba.europa.eu. Ange referensnummer EBA/GL/2014/12. Underrättelserna bör skickas av personer med lämplig behörighet att för den behöriga myndighetens räkning rapportera att riktlinjerna följs.

Underrättelserna offentliggörs på EBA:s webbplats i enlighet med artikel 16.3.

Kapitel I – Tillämpningsområde och definitioner

Tillämpningsområde

1. I dessa riktlinjer fastställs en uppsättning av minimikrav inom området säkerhet vid betalningar på internet. Riktlinjerna bygger på reglerna i direktiv 2007/64/EG ([1]) (betaltjänstdirektivet) som gäller informationskraven vid betaltjänster och skyldigheterna för betaltjänstleverantörer i samband med tillhandahållandet av betaltjänster. I artikel 10.4 i direktivet föreskrivs att betalningsinstituten ska inrätta en effektiv styrning och tillfredsställande rutiner för intern kontroll.

2. Riktlinjerna gäller vid tillhandahållande av betaltjänster via internet av betaltjänstleverantörer enligt artikel 1 i betaltjänstdirektivet.

3. Riktlinjerna riktar sig till finansiella institut enligt definitionen i artikel 4.1 i förordning (EU) nr 1093/2010 och till behöriga myndigheter enligt definitionen i artikel 4.2 i förordning (EU) nr 1093/2010. Behöriga myndigheter i de 28 medlemsstaterna i Europeiska unionen bör säkerställa att betaltjänstleverantörer under deras tillsyn tillämpar dessa riktlinjer.

4. Dessutom får de behöriga myndigheterna besluta att kräva att betaltjänstleverantörer rapporterar till den behöriga myndigheten att de följer riktlinjerna.

5. Dessa riktlinjer påverkar inte giltigheten för Europeiska centralbankens ”Recommendations for the security of internet payments” (”rapporten”) ([2]). Framför allt fortsätter rapporten att utgöra det dokument mot vilket centralbanker i sin tillsynsfunktion över betalningssystem och instrument bör bedöma efterlevnaden avseende säkerhet vid betalningar på internet.

6. Riktlinjerna utgör de lägstaförväntningarna. De påverkar inte betaltjänstleverantörernas ansvar att övervaka och bedöma riskerna i sin betalningsverksamhet, utveckla sina egna detaljerade säkerhetsregler och genomföra tillräckliga åtgärder vad gäller arbete med säkerhet-, beredskaps-, incident- och kontinuitetsskydd som står i proportion till de risker som är förenade med de inneboende riskerna med erbjudna betaltjänster.

7. Syftet med riktlinjerna är att fastställa de lägsta gemensamma kraven för de betaltjänster på internet som anges nedan, oavsett vilket inloggningsverktyg som används:

> [kort] utförandet av kortbetalningar på internet, bland annat virtuella kortbetalningar, samt registrering av kortuppgifter för användning i ”plånbokslösningar”,
>
> [betalningar] genomförandet av betalningar på internet,

([1]) Europaparlamentets och rådets direktiv 2007/64/EG av den 13 november 2007 om betaltjänster på den inre marknaden och om ändring av direktiven 97/7/EG, 2002/65/EG, 2005/60/EG och 2006/48/EG samt upphävande av direktiv 97/5/EG, EUT L 319, 5.12.2007,

([2]) http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

[e-uppdrag] utgivning och ändring av elektroniska uppdrag för autogireringar,

[e-pengar] överföringar via internet av elektroniska pengar mellan två konton för elektroniska pengar.

8. När riktlinjerna anger ett resultat kan resultatet uppnås genom olika metoder. Utöver de krav som anges nedan ger dessa riktlinjer även exempel på bästa praxis (i bilaga 1), som betaltjänstleverantörer uppmuntras att följa, men inte är skyldiga att följa.

9. Om tillhandahållandet av betaltjänster och instrument erbjuds genom ett betalningssystem (t.ex. kortbetalningssystem, girosystem, autogiro, etc.), bör behöriga myndigheter och den relevanta centralbanken med tillsynsfunktion över betalningsinstrument samarbeta för att säkerställa att de aktörer som är ansvariga för driften av systemet tillämpar riktlinjerna konsekvent.

10. Betalningsintegratörer ([3]) som tillhandahåller tjänster för att initiera betalningar betraktas antingen som behandlare av betaltjänster på internet (och därmed som betaltjänstleverantörer) eller som externa leverantörer av tekniska tjänster för de berörda systemen eller betaltjänstleverantörerna. I det senare fallet bör betalningsintegratörerna vara avtalsmässigt skyldiga att följa riktlinjerna.

11. Undantagna från tillämpningsområdet för riktlinjerna är

andra internettjänster som tillhandahålls av en betaltjänstleverantör via dennes betalningswebbplats (t.ex. e-mäkleri, onlinekontrakt),

betalningar där instruktioner skickas med post, telefonorder, röstbrevlåda eller med sms-baserad teknik,

mobilbetalningar som inte är webbläsarbaserade betalningar,

betalningar där en tredje part har åtkomst till kundens betalkonto,

betalningstransaktioner som görs av ett företag via särskilt nätverk avsett för ändamålet,

kortbetalningar med hjälp av anonyma och icke-uppladdningsbara fysiska eller virtuella kontantkort, när det inte finns något pågående förhållande mellan kortutgivaren och kortinnehavaren,

clearing och avveckling av betalningstransaktioner.

([3]) Betalningsintegratörerna förser betalningsmottagaren (dvs. e-handlaren) med ett standardiserat gränssnitt till tjänster för initiering av betalningar, som tillhandahålls av betaltjänstleverantörer.

Definitioner

12. För dessa riktlinjer, och utöver definitionerna i PSD, gäller följande definitioner:

Autentisering innebär ett förfarande som gör det möjligt för en betaltjänstleverantör att kontrollera en kunds identitet.

Stark kundautentisering är, i dessa riktlinjer, ett förfarande som bygger på användning av två eller flera av följande element – kategoriserade som kunskap, ägande och tillhörighet: i) något som enbart användaren känner till, t.ex. statiskt lösenord, kod, personligt id-nummer, ii) något som enbart användaren innehar, t.ex. säkerhetsdosa, smartkort, mobiltelefon, iii) något som användaren är, t.ex. biometriska kännetecken, såsom fingeravtryck. Dessutom måste de element som valts vara oberoende av varandra, d.v.s. brott mot ett äventyrar inte de(t) andra. Minst en av faktorerna bör vara icke-återanvändbar och icke-replikerbar (utom för tillhörighet), och inte kunna bli stulen i smyg via internet. Det starka autentiseringsförfarandet bör utformas på ett sådant sätt att det skyddar sekretessen för autentiseringsuppgifter.

Godkännande innebär ett förfarande som kontrollerar om en kund eller betaltjänstleverantör har rätt att utföra en viss handling, till exempel rätten att överföra medel, eller att få tillgång till känsliga uppgifter.

Säkerhetsuppgifter innebär information – i allmänhet konfidentiell – som tillhandahålls av en kund eller betaltjänstleverantör för autentisering. Säkerhetsuppgifterna kan också innebära innehav av ett fysiskt verktyg som innehåller information (t.ex. engångslösenordsgenerator, smartkort), eller något användaren memorerar eller representerar (t.ex. biometriska kännetecken).

Väsentlig säkerhetsincident vid betalning: innebär en incident som har eller kan ha en väsentlig inverkan på säkerheten, integriteten eller kontinuiteten för betaltjänstleverantörens betalningsrelaterade system och/eller säkerheten för känsliga uppgifter om betalningar eller medel. Vid bedömningen av väsentlighet bör hänsyn tas till antalet potentiellt berörda kunder, det belopp som är i riskzonen samt påverkan på andra betaltjänstleverantörer eller andra betalningsinfrastrukturer.

Riskanalys för transaktion innebär att risken i samband med en specifik transaktion utvärderas med hänsyn till kriterier som till exempel kundbetalningsmönster (beteende), värdet på den relaterade transaktionen, typen av produkt och betalningsmottagarens profil.

Virtuella kort innebär en kortbaserad betalningslösning där ett alternativt, tillfälligt kortnummer med en begränsad giltighetstid, begränsad användning och en fördefinierad köpgräns genereras, som kan användas för köp via internet.

Plånbokslösningar innebär lösningar som tillåter en kund att registrera uppgifter om ett eller flera betalningsinstrument för att göra betalningar med flera e-handlare.

Kapitel II – Riktlinjer om säkerhet vid betalningar på internet

Allmän kontrollmiljö

Styrning

1. Betaltjänstleverantörer bör införa en formell säkerhetspolicy för betaltjänster på internet. Denna bör regelbundet utvärderas.

    1.1 Säkerhetspolicyn bör dokumenteras och regelbundet utvärderas och vid behov uppdateras (i enlighet med riktlinje 2.4) samt fastställas av styrelsen eller den verkställande direktören. Den bör definiera mål för arbetet med säkerhet och riskaptiten.

    1.2 Säkerhetspolicyn bör definiera roller och ansvar, inkluderat den riskkontrollfunktion som rapporterar direkt till styrelsen, och rapporteringsvägar för tillhandahållna betaltjänster på internet, inklusive hantering av riskbedömning, kontroll och begränsning avseende känsliga uppgifter om betalningar. .

Riskbedömning

2. Betaltjänstleverantörer bör genomföra och dokumentera noggranna riskbedömningar avseende säkerheten vid betalningar på internet och relaterade tjänster, både före tillhandahållandet av tjänsten/tjänsterna och regelbundet därefter.

    2.1 Betaltjänstleverantörer bör genom sin riskkontrollfunktion genomföra och dokumentera detaljerade riskbedömningar för betalningar på internet och tillhörande tjänster. Betaltjänstleverantörer bör beakta resultaten av den pågående övervakningen av säkerhetshot som rör de betaltjänster på internet som de erbjuder eller planerar att erbjuda, med hänsyn till: i) de tekniska lösningar som de använder, ii) de tjänster som läggs ut på uppdragstagare, och iii) kundernas tekniska miljö. Betaltjänstleverantörer bör överväga de risker som är förknippade med valda teknikplattformar, systemarkitektur, programmeringstekniker och rutiner både hos dem själva ([4]) och hos deras kunder ([5]), samt resultaten från processen för övervakning av säkerhetsincidenter (se riktlinje 3).

    2.2 På grundval av detta bör betaltjänstleverantörer avgöra om och i vilken utsträckning förändringar kan vara nödvändiga för befintliga säkerhetsåtgärder, den teknik som används och de rutiner eller tjänster som erbjuds.

([4]) Såsom systemets känslighet för kapning av betalningssessioner, SQL-injektioner, cross-site scripting, buffertspill, etc.

([5]) Såsom risker i samband med användning av multimedieprogram, insticksprogram för webbläsare, ramar, externa länkar osv.

Betaltjänstleverantörer bör ta hänsyn till den tid som krävs för att genomföra förändringarna (inklusive introduktion för kunder) och vidta tillfälliga lämpliga åtgärder för att hantera säkerhetsincidenter och bedrägerier, samt potentiellt störande effekter.

2.3 I riskbedömningen bör inkluderas behovet av att skydda och säkra känsliga uppgifter om betalningar.

2.4 Betaltjänstleveratörer bör göra en översyn av riskscenarier och befintliga säkerhetssåtgärder efter väsentliga incidenter som påverkat deras tjänster, innan en större förändring av infrastruktur eller rutiner och när nya hot identifierats genom omvärldsbevakning. Dessutom bör en allmän utvärdering av riskbedömningen genomföras minst en gång per år. Resultaten av dessa riskbedömningar och utvärderingar bör fastställas av styrelsen eller den verkställande direktören.

Incidentövervakning och rapportering

3. Betaltjänstleverantörer bör säkerställa en konsekvent och sammanhållen övervakning, hantering och uppföljning av säkerhetsincidenter, inklusive säkerhetsrelaterade kundklagomål. Betaltjänstleverantörerna bör fastställa en rutin för att rapportera sådana incidenter till ledningen och, i händelse av väsentliga säkerhetsincidenter vid betalning, de behöriga myndigheterna.

3.1 Betaltjänstleverantörer bör ha en process på plats för att övervaka, hantera och följa upp säkerhetsincidenter och säkerhetsrelaterade kundklagomål och rapportera sådana händelser till ledningen.

3.2 Betaltjänstleverantörer bör ha en rutin för att omedelbart meddela de behöriga myndigheterna (d.v.s. tillsyns- och dataskyddsmyndigheter), om sådana finns, i händelse av väsentliga säkerhetsincidenter vid betalningar, med avseende på de betaltjänster som tillhandahålls.

3.3 Betaltjänstleverantörer bör ha en rutin för att samarbeta med relevanta brottsbekämpande myndigheter i händelse av väsentliga säkerhetsincidenter vid betalning, däribland dataintrång.

3.4 De betaltjänstleverantörer som inlöser transaktionsbelopp där ett betalningsinstrument har använts bör avtalsmässigt kräva att e-handlare som lagrar, behandlar eller överför känsliga uppgifter om betalningar samarbetar både med dem och berörda brottsbekämpande myndigheter, i händelse av väsentliga säkerhetsincidenter vid betalning, däribland dataintrång. Om en betaltjänstleverantör får kännedom om att en e-handlare inte samarbetar enligt avtalet, bör betaltjänstleverantören vidta åtgärder för att verkställa denna avtalsförpliktelse eller upphäva avtalet.

Riskkontroll och begränsning

4. Betaltjänstleverantörer bör införa säkerhetsåtgärder i linje med sin respektive säkerhetspolicy för att begränsa identifierade risker. Dessa åtgärder bör innehålla flera lager av säkerhetsåtgärder, där misslyckande vid en säkerhetsåtgärd fångas upp av nästa säkerhetsåtgärd (’defence in depth’).

    4.1 Vid design, utveckling och underhåll av betaltjänster på internet, bör betaltjänstleverantörer ägna särskild uppmärksamhet åt att funktioner i informationstekniska miljöer (IT-miljöer) (t.ex. utvecklings-, test- och produktionsmiljöer) är tillräckligt separerade och att principerna om uppgiftsdelning, och ”lägsta privilegium” ligger till grund för en sund identitets- och åtkomsthantering. ([6]).

    4.2 Betaltjänstleverantörer bör ha lämpliga säkerhetslösningar för att skydda nätverk, webbplatser, servrar och kommunikationslänkar mot missbruk eller attacker. Betaltjänstleverantörer bör ta bort alla överflödiga funktioner från servrarna för att skydda (härda) dem och eliminera eller minska sårbarheter i program som är i riskzonen. De olika programmens åtkomst till de uppgifter och resurser som krävs bör hållas till ett minimum efter principen ”lägsta privilegium”. För att begränsa användningen av ”falska” webbplatser (som liknar webbplatserna för legitima betaltjänstleverantörer), bör transaktionswebbplatser som erbjuder betaltjänster på internet identifieras genom utökade valideringscertifikat som upprättats i betaltjänstleverantörens namn eller genom andra liknande autentiseringsmetoder.

    4.3 Betaltjänstleverantörer bör ha lämpliga rutiner på plats för att övervaka, spåra och begränsa åtkomsten till: i) känsliga uppgifter om betalningar, och ii) logiska och fysiska kritiska resurser, såsom nätverk, system, databaser, säkerhetsmoduler etc. Betaltjänstleverantörer bör skapa, lagra och analysera lämpliga loggar och verifieringskedjor.

    4.4 Vid design ([7]), utveckling och underhåll av betaltjänster på internet, bör betaltjänstleverantörer säkerställa att dataminimering ([8]) är en viktig del av kärnfunktionerna: insamling, transport, bearbetning, lagring och/eller arkivering och att visualisering av känsliga uppgifter om betalningar bör hållas på en absolut miniminivå.

([6]) ”Varje program och varje privilegierad användare av systemet ska använda det lägsta privilegium som krävs för att utföra jobbet.” Se Saltzer, J.H. (1974), ‘Protection and the Control of Information Sharing in Multics’, Communications of the ACM, Vol. 17, No 7, p. 388.

([7]) Inbyggt integritetsskydd (privacy by design)

([8]) Dataminimering syftar på policyn att samla den minsta mängden personlig information som är nödvändig för att utföra en viss funktion.

4.5 Säkerhetsåtgärderna för betaltjänster på internet bör testas under övervakning av riskkontrollfunktionen för att säkerställa dess robusthet och effektivitet. Alla ändringar bör omfattas av en formell process för ändringshantering, som säkerställer att förändringar planeras, testas, dokumenteras och godkänns på ett ändamålsenligt sätt. På grundval av de ändringar som gjorts och de säkerhetshot som observeras, bör testerna upprepas regelbundet och omfatta scenarier av relevanta och kända potentiella attacker.

4.6 Betaltjänstleverantörers säkerhetsåtgärder för betaltjänster på internet bör regelbundet granskas så att deras stabilitet och effektivitet säkerställs. Genomförandet av betaltjänster på internet och deras funktion bör också granskas. Hur ofta sådana granskningar ska göras och vad de ska vara inriktade på bör ta hänsyn till och stå i proportion till aktuella säkerhetsrisker. Betrodda och oberoende (interna eller externa) experter bör utföra granskningarna. De bör inte på något sätt vara inblandade i utveckling, införandet eller den operativa förvaltningen av de erbjudna betaltjänsterna på internet.

4.7 När betaltjänstleverantörer lägger ut funktioner relaterade till säkerheten för betaltjänster på internet på uppdragstagare, bör avtalet innehålla bestämmelser om krav på efterlevnad av de principer och riktlinjer som anges i dessa riktlinjer.

4.8 Betaltjänstleverantörer som erbjuder inlösentjänster bör kräva att e-handlare som hanterar (dvs. lagrar, bearbetar eller skickar) känsliga uppgifter om betalningar genomför säkerhetsåtgärder i sin IT-infrastruktur, i linje med riktlinjerna 4.1–4.7, för att undvika stöld av dessa känsliga uppgifter om betalningar genom deras system. Om en betaltjänstleverantör får kännedom om att en e-handlare inte har de nödvändiga säkerhetsåtgärderna på plats, bör betaltjänstleverantören vidta åtgärder för att verkställa denna avtalsförpliktelse eller upphäva avtalet.

Spårbarhet

5. Betaltjänstleverantörer bör ha rutiner som säkerställer att alla transaktioner samt processflödet för e-uppdrag kan härledas.

5.1 Betaltjänstleverantörer bör säkerställa att deras tjänster innehåller säkerhetsmekanismer för detaljerad loggning av transaktioner och uppgifter om e-uppdrag, däribland löpnummer för transaktion, tidsstämplar för transaktionsdata, förändringar av parametrar samt tillgång till data om transaktioner och e-uppdrag.

5.2 Betaltjänstleverantörer bör införa loggfiler som gör det möjligt att härleda eventuella tillägg, ändringar eller borttag av data om transaktioner och e-uppdrag .

5.3 Betaltjänstleverantörer bör analysera datan om transaktioner och e-uppdrag samt säkerställa att de har verktyg för att kunna utvärdera loggfilerna. Endast behörig personal bör ha tillgång till respektive verktyg. Särskilda kontroller och säkerhetsåtgärder för betalningar på internet

Inledande kundidentifiering, kundinformation

6. Kunder ska vara ändamålsenligt identifierade i enlighet med den europeiska lagstiftningen om åtgärder mot penningtvätt[9] och bekräfta sin vilja att göra betalningar via internet med hjälp av tjänster innan de beviljas tillgång till dessa tjänster. Betaltjänstleverantörer bör tillhandahålla adekvat ”förhands-”, ”vanlig” eller, i förekommande fall, ”ad hoc”-information till kunden om de nödvändiga kraven (t.ex. utrustning, rutiner) för att utföra säkra internetbetalningstransaktioner och de inneboende riskerna.

6.1 Betaltjänstleverantörer bör säkerställa att kunden har genomgått rutiner för kundkontroll och har uppvisat adekvata identitetshandlingar ([10]) och lämnat relaterad information innan de beviljas tillgång till betaltjänster på internet ([11]).

6.2 Betaltjänstleverantörer bör säkerställa att förhandsinformationen ([12]) som lämnas till kunden innehåller specifika detaljer som rör betaltjänsterna på internet. Dessa bör lämpligen omfatta:

- tydlig information om eventuella krav på kundutrustning, programvara eller andra nödvändiga verktyg (t.ex. antivirusprogram, brandväggar),
- riktlinjer för en korrekt och säker användning av personliga säkerhetsuppgifter,
- en steg-för-steg-beskrivning av hur kunden går till väga för att lämna och godkänna en betalningstransaktion och/eller få information, inbegripet konsekvenserna av varje åtgärd,
- riktlinjer för en korrekt och säker användning av all maskinvara och programvara som tillhandahålls till kunden,

([9]) Exempelvis Europaparlamentets och rådets direktiv 2005/60/EG av den 26 oktober 2005 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt och finansiering av terrorism. EUT L 309, 25.11.2005, s. 15–36. Se även kommissionens direktiv 2006/70/EG av den 1 augusti 2006 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv 2005/60/EG beträffande definitionen av ”person i politiskt utsatt ställning”, samt de tekniska kriterierna för förenklade förfaranden för kundkontroll och för undantag på grund av en finansiell verksamhet som drivs tillfälligt eller i mycket begränsad omfattning. EUT L 214, 4.8.2006, s. 29–34.

([10]) Till exempel pass, nationellt identitetskort eller avancerad elektronisk signatur.

([11]) Kundidentifieringsprocessen påverkar inte eventuella undantag i befintlig lagstiftning mot penningtvätt. Betaltjänstleverantörer behöver inte genomföra en separat kundidentifieringsprocess för betaltjänster på internet, förutsatt att en sådan kundidentifiering redan har gjorts, till exempel för andra befintliga betalningsrelaterade tjänster eller vid öppnandet av ett konto.

([12]) Denna information kompletterar artikel 42 i betaltjänstdirektivet som anger vilka uppgifter som betaltjänstleverantören måste lämna till betaltjänstanvändaren innan ett avtal ingås om tillhandahållande av betaltjänster.

- rutiner som ska tillämpas i händelse av förlust eller stöld av de personliga säkerhetsuppgifterna eller kundens maskinvara eller programvara för att logga in eller utföra transaktioner,

- rutiner som ska följas om missbruk upptäcks eller misstänks,

- en beskrivning av betaltjänstleverantörens och kundernas ansvar och skyldigheter avseende användningen av internetbetaltjänsten.

6.3 Betaltjänstleverantörer bör säkerställa att ramavtalet med kunden anger att betaltjänstleverantören kan blockera en specifik transaktion eller betalningsinstrumentet ([13]) på grundval av säkerhetsskäl. Metoden och villkoren för underrättelse av kunden bör fastställas, liksom hur kunden kan kontakta betaltjänstleverantören för att få betalningstransaktionen på internet eller tjänsten ”återaktiverad” i linje med betaltjänstdirektivet.

Stark kundautentisering

7. Initiering av internetbetalningar, samt tillgång till känsliga uppgifter om betalningar, bör skyddas av en stark kundautentisering. Betaltjänstleverantörer bör ha en rutin för stark kundautentisering som är i linje med definitionen i dessa riktlinjer.

7.1 [betalningar/e-uppdrag/e-pengar] Betaltjänstleverantörer bör utföra stark kundautentisering för kundens godkännande av betalningstransaktioner på internet (däribland buntbetalningar) och utgivning eller ändring av elektroniska autogirouppdrag. Betaltjänstleverantörerna kan överväga alternativa åtgärder för kundautentisering gällande:

- utbetalningar till betrodda mottagare som ingår i tidigare fastställda vitlistor för den kunden,

- transaktioner mellan två konton som tillhör samma kund och som finns hos samma betaltjänstleverantör,

- överföringar inom samma betaltjänstleverantör som motiveras av en transaktionsriskanalys,

- betalningar som avser låga belopp, enligt vad som anges i betaltjänstdirektivet ([14]).

7.2 Att få tillgång till eller ändra känsliga uppgifter om betalningar (inklusive att skapa och ändra vitlistor) kräver stark kundautentisering. Om en betaltjänstleverantör erbjuder rent konsultativa tjänster, utan att visa känslig kund- eller betalningsinformation som till exempel betalkortsuppgifter, som lätt kan

([13]) Se artikel 55 i PSD om begränsningar av användningen av betalningsinstrument.

([14]) Se definitionen av betalningsinstrument som avser låga belopp i artiklarna 34.1 och 53.1 i PSD.

missbrukas för att begå bedrägeri, kan betaltjänstleverantören anpassa sina autentiseringskrav på grundval av sin riskbedömning.

7.3 [kort] För korttransaktioner bör alla betaltjänstleverantörer som utfärdar kort stödja stark autentisering av kortinnehavaren. Alla kort som utfärdas måste vara tekniskt redo (registrerade) för att användas med stark autentisering.

7.4 [kort] Betaltjänstleverantörer som erbjuder inlösentjänster bör stödja teknik som gör det möjligt för kortutgivaren att utföra en stark autentisering av kortinnehavaren för kortbetalningssystem där köparen deltar.

7.5 [kort] Betaltjänstleverantörer som erbjuder inlösentjänster bör kräva att deras e-handlare stöder lösningar som gör det möjligt för kortutgivaren att utföra stark autentisering av kortinnehavaren för korttransaktioner via internet. Att använda alternativa autentiseringsåtgärder kan övervägas för på förhand identifierade kategorier av lågrisktransaktioner, till exempel sådana som är baserade på en transaktionsriskanalys eller som innefattar betalningar som avser låga belopp, enligt vad som anges i betaltjänstdirektivet.

7.6 [kort] För kortbetalningssystem som godtagits av tjänsten, bör leverantörer av plånbokslösningar kräva att kortutgivaren använder stark autentisering när den rättmätige innehavaren först registrerar kortuppgifter.

7.7 Leverantörer av plånbokslösningar bör stödja stark kundautentisering när kunderna loggar in på plånboksbetaltjänster eller utför korttransaktioner via internet. Att använda alternativa autentiseringsåtgärder kan övervägas för på förhand identifierade kategorier av lågrisktransaktioner, till exempel sådana som är baserade på en riskanalys av transaktionen eller som innefattar betalningar som avser låga belopp, enligt vad som anges i betaltjänstdirektivet.

7.8 [kort] För virtuella kort bör den första registreringen ske i en trygg och pålitlig miljö ([15]). Stark kundautentisering bör krävas för processen för generering av virtuella kortuppgifter, om kortet är utfärdat i internetmiljön.

7.9 Betaltjänstleverantörer bör säkerställa en korrekt bilateral autentisering vid kommunikation med e-handlare för att inleda betalningar via internet och för att få tillgång till känsliga uppgifter om betalningar.

Registrering för och tillhandahållande av autentiseringsverktyg och/eller programvara som levereras till kunden

([15]) Miljöer under betaltjänstleverantörers ansvar, där det säkerställs en tillräcklig autentisering av kunden och av betaltjänstleverantörerna som erbjuder tjänsten och skyddet av konfidentiell/känslig information, innefattar: i) betaltjänstleverantörers lokaler, ii) internetbanken eller en annan säker webbplats, till exempel där GA erbjuder jämförbara säkerhetsfunktioner, bland annat enligt riktlinje 4, eller iii) tjänster avseende bankomat (ATM). (I fallet med bankomater krävs stark kundautentisering. Denna autentisering tillhandahålls vanligen genom chip och PIN-kod eller chip och biometri).

8. Betaltjänstleverantörer bör säkerställa att kundens anmälan till och nyanskaffning av autentiseringsverktyg som krävs för att använda internetbetalning och/eller leverans av betalningsprogramvara till kunder sker på ett säkert sätt.

8.1 Registrering för och tillhandahållande av verifieringsverktyg och/eller betalningsprogramvara som levereras till kunden bör uppfylla följande krav.

- De relaterade rutinerna bör genomföras i en säker och pålitlig miljö samtidigt som hänsyn tas till möjliga risker som härrör från enheter som inte står under betaltjänstleverantörens kontroll.

- Effektiva och säkra rutiner bör finnas på plats för leveransen av personliga säkerhetsuppgifter, betalningsprogramvara och alla personliga enheter för internetbetalningar. Programvara som levereras via internet bör också signeras digitalt av betaltjänstleverantören för att kunden ska kunna verifiera dess äkthet och att den inte har manipulerats.

- [kort] Vid korttransaktioner bör kunden ha möjlighet att registrera sig för stark autentisering oberoende av ett specifikt internetköp. Om aktivering under handel på internet erbjuds bör detta ske genom att kunden dirigeras om till en säker och pålitlig miljö.

8.2 [kort] Kortutgivaren bör aktivt uppmuntra kortinnehavarens registrering för stark autentisering och låta sina kortinnehavare kringgå registreringen endast i ett exceptionellt och begränsat antal fall där detta motiveras av risken i samband med den specifika korttransaktionen.

Inloggningsförsök, timeout för session, giltigheten för autentisering

9. Betaltjänstleverantörer bör begränsa antalet inloggnings- eller autentiseringsförsök, definiera regler för ”time out” av sessioner vid tillhandahållandet av betaltjänster på internet samt fastställa autentiseringarnas giltighetstid.

9.1 När man använder ett engångslösenord för autentiseringsändamål, bör betaltjänstleverantörer säkerställa att giltighetstiden för sådana lösenord är begränsad till det strikta minimum som krävs.

9.2 Betaltjänstleverantörer bör fastställa det maximala antalet misslyckade inloggnings- eller autentiseringsförsök efter vilka tillgången till betaltjänsten på internetär (tillfälligt eller permanent) blockerad. De bör ha en säker rutin för att återaktivera blockerade betaltjänster på internet.

9.3 Betaltjänstleverantörer bör fastställa den längsta tiden efter vilken inaktiva sessioner av betaltjänster på internet avslutas automatiskt.

Transaktionsövervakning

10. Mekanismer för transaktionsövervakning som syftar till att förebygga, upptäcka och blockera bedrägliga betalningstransaktioner bör köras innan betaltjänstleverantörer ger sitt slutliga godkännande. Misstänkta transaktioner eller högrisktransaktioner bör bli föremål för en särskild kontroll- och utvärderingsrutin. Likvärdiga mekanismer för säkerhetsövervakning och godkännande bör också vara på plats för utgivning av e-uppdrag.

    10.1 Betaltjänstleverantörer bör använda system för att upptäcka och förebygga bedrägeri, så att de kan identifiera misstänkta transaktioner innan betaltjänstleverantören slutligen godkänner transaktioner eller e-uppdrag. Sådana system bör till exempel bygga på parametriserade regler (till exempel svarta listor över äventyrade eller stulna kortuppgifter), och övervaka onormala beteendemönster hos kunden eller kundens enhet för kommunikation (till exempel byte av internetprotokolladress (IP-adress)([16]) eller IP-intervallet under sessionen för betaltjänsten på internet, ibland identifierat genom IP-kontroller för geolokalisering ([17]), otypiska kategorier av e-handlare för en viss kund eller onormala transaktionsuppgifter m.m.). Sådana system bör också kunna upptäcka tecken på infektion med sabotageprogram i sessionen (till exempel via skript gentemot manuell validering) och kända bedrägeriscenarier. Omfattning, komplexitet och flexibilitet för övervakning bör, samtidigt som de efterlever relevant dataskyddslagstiftning, stå i proportion till resultatet av riskbedömningen.

    10.2 De betaltjänstleverantörer som inlöser transaktionsbelopp där ett betalningsinstrument har använts bör ha system för att upptäcka och förebygga bedrägerierför att övervaka e-handlares aktiviteter.

    10.3 Betaltjänstleverantörer bör granska och utvärdera transaktioner inom en lämplig tidsperiod, för att inte i onödan fördröja inledandet och/eller utförandet av den berörda betaltjänsten.

    10.4 Om betaltjänstleverantören, i enlighet med dess riskpolicy, beslutar att blockera en betalningstransaktion som har identifierats som potentiellt bedräglig, bör betaltjänstleverantören behålla spärren under så kort tid som möjligt fram till det att säkerhetsaspekterna har klargjorts.

Skydd av känsliga uppgifter om betalningar

11. Känsliga uppgifter om betalningar bör skyddas vid lagring, bearbetning eller överföring.

    11.1 Alla uppgifter som används för att identifiera och autentisera kunder (till exempel vid inloggning, vid initiering av betalningar på internet, samt vid utfärdande, ändring eller annullering av e-uppdrag) samt kundgränssnittet

([16]) En IP-adress är en unik numerisk kod som identifierar varje dator som är ansluten till internet.

([17]) En ”Geo-IP”-kontroll verifierar om det utfärdande landet motsvarar IP-adressen från vilken användaren inleder transaktionen.

(betaltjänstleverantörens eller e-handlarens webbplats), bör vara lämpligt skyddade mot stöld och obehörig åtkomst eller förändring.

11.2 När betaltjänstleverantörerutbyter känslig betalningsinformation via internet, bör de säkerställa att säker ”end-to-end” kryptering ([18]) tillämpas mellan de kommunicerande parterna under respektive kommunikations session, för att skydda konfidentialiteten och riktigheten hos dessa uppgifter med hjälp av starka och allmänt etablerade krypteringstekniker.

11.3 Betaltjänstleverantörer som erbjuder inlösentjänster bör uppmuntra sina e-handlare att inte lagra känsliga uppgifter om betalningar. För den händelse att e-handlare hanterar, dvs. lagrar, bearbetar eller överför känsliga uppgifter om betalningar, bör sådana betaltjänstleverantörer avtalsmässigt kräva att e-handlarna har nödvändiga åtgärder på plats för att skydda dessa uppgifter. Betaltjänstleverantörer bör genomföra regelbundna kontroller, och om en betaltjänstleverantör får kännedom om att en e-handlare hanterar känsliga uppgifter om betalningar utan att ha de nödvändiga säkerhetsåtgärderna på plats, bör de vidta åtgärder för att verkställa denna avtalsförpliktelse eller upphäva avtalet.

Kundernas medvetenhet, utbildning och kommunikation

Kundutbildning och kommunikation med kunden

12. Betaltjänstleverantörer bör, vid behov, ge stöd och vägledning till kunder när det gäller säker användning av betaltjänster på internet. Betaltjänstleverantörerna bör kommunicera med sina kunder på ett sådant sätt som försäkrar kunderna om att de meddelanden som mottagits är äkta.

12.1 Betaltjänstleverantörer bör tillhandahålla åtminstone en säker kanal ([19]) för den löpande kommunikationen med kunder angående hur betaltjänsten på internet används säkert och korrekt. Betaltjänstleverantörer bör informera kunderna om denna kanal och förklara att meddelanden på betaltjänstleverantörens vägnar som sker på något annat sätt, till exempel via e-post, och som gäller säker och korrekt användning av betaltjänsten på internet, inte är tillförlitlig. Betaltjänstleverantören bör förklara:

- hur kunderna går till väga för att rapportera till betaltjänstleverantören (misstänkta) bedrägliga betalningar, misstänkta incidenter eller avvikelser under

([18]) End-to-end kryptering avser kryptering i eller i anslutning till datas inmatning, med motsvarande avkryptering inom eller i direkt anslutning till det mottagande systemet

ETSI EN 302 109 V1.1.1. (2003-06

([19]) Såsom en särskild postlåda på betaltjänstleverantörens webbplats eller en säker webbplats.

sessioner på internetbetaltjänster och/eller eventuella försök till ”social engineering” ([20]) ;

- nästa steg, dvs. hur betaltjänstleverantörer kommer att svara kunden;

- hur betaltjänstleverantören kommer att meddela kunden om (potentiella) bedrägliga transaktioner eller att de inte inletts, eller varna kunden om förekomsten av attacker (till exempel nätfiske via e-post).

12.2 Genom den säkra kanalen bör betaltjänstleverantören hålla kunderna informerade om uppdateringar av säkerhetsrutinerna för betaltjänster på internet. Eventuella varningar om väsentliga nya risker (till exempel varningar om ”social engineering”) bör också ges via den säkra kanalen.

12.3 Betaltjänstleverantörer bör tillhandahålla en kundtjänst för alla frågor, klagomål, ansökningar om stöd och anmälningar om avvikelser eller incidenter som gäller betalningar via internet och relaterade tjänster, och kunderna bör bli informerade på ett adekvat sätt om hur en sådan tjänst kan erhållas.

12.4 Betaltjänstleverantörer bör initiera utbildnings- och medvetenhetsprogram för kunder för att säkerställa att kunderna åtminstone som ett minimum förstår behovet

- av att skydda sina lösenord, säkerhetsdosor, personuppgifter och annan konfidentiell uppgifter,

- att hantera säkerheten för den personliga enheten (till exempel en dator) korrekt genom att installera och uppdatera säkerhetskomponenter (virusskydd, brandväggar, säkerhetsfixar),

- att överväga väsentliga hot och risker i samband med nedladdning av programvara via internet, om kunden inte kan vara rimligt säker på att programvaran är äkta och inte har manipulerats,

- att använda den äkta webbplatsen för betalning på internet som tillhör betaltjänstleverantören.

12.5 De betaltjänstleverantörer som inlöser transaktionsbelopp där betalningsinstrument har använts bör kräva att e-handlarna tydligt skiljer betalningsrelaterade processer från nätbutiken för att göra det lättare för kunder att identifiera när de kommunicerar med betaltjänstleverantören och inte med betalningsmottagaren (till exempel genom att kunden omdirigeras och ett separat fönster öppnas så att betalningsprocessen inte visas i e-handlarens ram).

([20]) Social engineering i detta sammanhang betyder tekniker för att manipulera människor för att inhämta information (till exempel via e-post eller telefonsamtal), eller hämta information från sociala nätverk, i syfte att begå bedrägeri eller få obehörig tillgång till en dator eller ett nätverk.

Anmälningar, inställning av gränsvärden

13. Betaltjänstleverantörer bör sätta gränser för betaltjänster på internet och erbjuda sina kunder alternativ attytterligare begränsa riskerna inom dessa gränser. De kan också tillhandahålla varningar och möjligheter för kunder att hantera sina kundprofiler.

    13.1 Innan betaltjänstleverantörer tillhandahåller en kund betaltjänster på internet, bör de sätta gränser som ([21]) gäller för dessa tjänster (till exempel ett högsta belopp för varje enskild betalning eller ett sammanlagt belopp under en viss tidsperiod), och bör informera sina kunder om detta. Betaltjänstleverantörer bör ge kunderna möjlighet att avaktivera funktionen för betalning på internet.

Kundens tillgång till information om status för initiering och genomförande av betalning

14. Betaltjänstleverantörer bör bekräfta initieringen av en betalning till sina kunder och i god tid förse kunderna med den information som behövs för att kontrollera att en betalningstransaktion har initierats och/eller genomförts korrekt.

    14.1 [betalning/e-uppdrag] Betaltjänstleverantörer bör ge kunderna möjlighet att i nära realtid när som helst kontrollera statusen för genomförandet av transaktioner samt saldon ([22]) i en säker och pålitlig miljö.

    14.2 Alla detaljerade elektroniska utdrag bör göras tillgängliga i en säker och pålitlig miljö. När betaltjänstleverantörer informerar kunderna om tillgången till elektroniska utdrag (till exempel regelbundet när ett periodiskt e-utdrag har utfärdats, eller på ad hoc-basis efter att en transaktion genomförs) genom en alternativ kanal, såsom sms, e-post eller brev, bör känsliga uppgifter om betalningar inte ingå i sådana meddelanden. Om de ingår bör de maskeras.

Kapitel III – Slutbestämmelser och införande

15. Riktlinjerna ska tillämpas från och med den 01.08.2015.

([21]) Sådana begränsningar kan antingen gälla globalt (dvs. för alla betalningsinstrument som möjliggör betalningar via internet) eller individuellt.

([22]) Med undantag för när tjänsten undantagsvis är otillgänglig på grund av tekniskt underhåll eller till följd av en väsentlig incident.

Bilaga 1: Exempel på bästa praxis

Utöver de krav som anges ovan beskrivs i dessa riktlinjer den bästa praxis som betaltjänstleverantörer och relevanta marknadsaktörer uppmuntras att anta, men inte behöver anta. För tydlighet anges uttryckligen de kapitel som denna bästa praxis avser.

Allmän kontrollmiljö

Styrning

BP 1: Säkerhetspolicyn skulle kunna fastställas i ett särskilt dokument.

Riskkontroll och begränsning

BP 2: Betaltjänstleverantörer skulle kunna tillhandahålla säkerhetsverktyg (till exempel verktyg och/eller anpassade webbläsare, ordentligt säkrade) för att skydda kundens gränssnitt mot olaglig användning eller attacker (till exempel ”man-i-mitten” attacker).

Spårbarhet

BP 3: Betaltjänstleverantörer som erbjuder inlösentjänster skulle kunna kräva genom avtal att e-handlarna som lagrar betalningsinformation har lämpliga processer på plats för att underlätta spårbarheten.

Särskilda kontroller och säkerhetsåtgärder för betalningar på internet

Inledande kundidentifiering, kundinformation

BP 4: Kunden skulle kunna teckna ett särskilt tjänsteavtal för att genomföra betalningstransaktioner på internet, snarare än att ha villkoren inkluderade i ett bredare allmänt serviceavtal med betaltjänstleverantören.

BP 5: Betaltjänstleverantörer kan också se till att kunder får, på en pågående eller, i förekommande fall, ad hoc-basis, och via lämpliga medel (t.ex. broschyrer, webbsidor), med tydliga och enkla instruktioner förklarar sitt ansvar om en säker användning av tjänsten.

Stark kundautentisering

BP 6: [kort] E-handlarna skulle kunna stödja en stark autentisering av kortinnehavaren från kortutgivaren vid korttransaktioner via internet.

BP 7: För kundens bekvämlighet skulle betaltjänstleverantörer kunna överväga att använda ett enda starkt kundverifieringsverktyg för alla betaltjänster på internet. Detta skulle kunna göra kunderna mer benägna att acceptera lösningen och underlätta en korrekt användning.

BP 8: Stark kundautentisering kan inkludera element som kopplar autentiseringen till ett visst belopp och en viss betalningsmottagare. Detta skulle kunna ge kunderna ökad säkerhet när de godkänner betalningar. Tekniklösningen som gör att de starka autentiseringsuppgifterna och transaktionsuppgifterna kan kopplas bör vara säker mot manipulation.

Skydd av känsliga uppgifter om betalningar

BP 9: Det är önskvärt att e-handlarna som hanterar känsliga uppgifter om betalningar på lämpligt sätt utbildar sin personal som hanterar bedrägerier, och uppdaterar denna utbildning regelbundet för att säkerställa att innehållet fortfarande är relevant i en föränderlig säkerhetsmiljö.

Kundutbildning och kommunikation med kunden

BP 10: Det är önskvärt att betaltjänstleverantörer som erbjuder inlösen av transaktionsbelopp där ett betalningsinstrument har använts ordnar utbildningar om bedrägeribekämpning för sina e-handlare.

Anmälningar, inställning av gränsvärden

BP 11: Inom de fastställda gränserna skulle betaltjänstleverantörer kunna erbjuda sina kunder möjligheten att hantera begränsningar av betaltjänster på internet i en säker och pålitlig miljö.

BP 12: Betaltjänstleverantörer skulle kunna genomföra varningar för kunder, till exempel via telefonsamtal eller sms, vid misstänkta transaktioner eller vid transaktioner med hög risk, baserat på sin riskhanteringspolicy.

BP 13: Betaltjänstleverantörer skulle kunna göra det möjligt för kunderna att specificera allmänna, personliga regler som parametrar för sitt beteende när det gäller betalningar via internet och relaterade tjänster, till exempel att de bara kommer att inleda betalningar från vissa specifika länder och att betalningar som inleds från annat håll ska blockeras, eller att de kan inkludera specifika betalningsmottagare på vita eller svarta listor.