EBA/GL/2014/12
19 desember 2014

Endelige retningslinjer

for sikkerhet i internettbetalinger

Finanstilsynet, sept. 2015

Oversettelse i utdrag av:
Final guidelines on the security of internet payments
fra the European Banking Authority (EBA)

Innhold

Retningslinjer for sikkerhet i internettbetalinger

Status når det gjelder retningslinjene

Dette dokumentet inneholder retningslinjer i henhold til artikkel 16 i Forordning (EU) nr. 1093/2010 som definerer en europeisk tilsynsmyndighet (European Banking Authority (EBA)), og som endrer beslutning nr. 716/2009/EC og som opphever Kommisjonsbeslutning 2009/78/EC ("EBA-reguleringen"). Ifølge artikkel 16(3) i EBA-bestemmelsene må myndighetene og næringen gjøre sitt ytterste for å følge retningslinjene.

Retningslinjene definerer EBAs syn på hva som er riktig tilsynspraksis innenfor det europeiske finanstilsynssystemet, og hvordan EU-lover skal anvendes innenfor et bestemt område. EBA forventer at alle myndigheter og finansforetak som reglene gjelder for, følger disse. Relevante myndigheter skal etterleve retningslinjene ved å innarbeide dem i tilsynsvirksomheten (for eksempel ved å endre lovgivningen eller tilsynsmetodene), også der retningslinjene henvender seg primært til foretakene.

Rapportering

Ifølge artikkel 16(3) i EBA-bestemmelsene må myndighetene innen to måneder fra de oversatte retningslinjene er publisert, underrette EBA om de følger eller har til hensikt å følge retningslinjene, alternativt angi en grunn for at retningslinjene ikke følges. Dersom EBA ikke er underrettet innen fristen, vil EBA anta at den relevante myndigheten ikke følger retningslinjene. Underretning skjer ved å sende et utfylt skjema (kapittel 5)[1], til compliance@eba.europa.eu, merket med referansen "EBA/GL/2014/12". Underretningen skal sendes av en person med myndighet til å representere myndigheten.

Underretninger publiseres på EBAs nettsted i henhold til artikkel 16(3).

[1] Skjemaet står på side 42, bakerst i EBAs retningslinjer: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0

Kapittel 1 – Omfang og definisjoner

Omfang

1. Disse retningslinjene definerer et sett med minimumskrav når det gjelder sikkerhet for internettbetalinger. Retningslinjene bygger på direktiv 2007/64/EC ("Payment Services Directive", PSD) som omhandler krav til informasjon når det gjelder betalingstjenester og krav til foretak som tilbyr betalingstjenester (PSP-er) knyttet til tjenesten. I henhold til artikkel 10(4) i direktivet, skal foretakene ha gode opplegg for styring og kontroll.

2. Retningslinjene gjelder for betalingstjenester på Internett som tilbys av PSP-er i henhold til artikkel 1 i direktivet.

3. Retningslinjene retter seg til finansforetak som definert i artikkel 4(1) i Forordning (EU) nr. 1093/2010 og til myndigheter som definert i artikkel 4(2) i Forordning (EU) nr. 1093/2010. Myndigheter i de 28 medlemslandene i EU skal sikre at PSP-ene definert i artikkel 1 i direktivet følger retningslinjene.

4. I tillegg kan myndighetene vedta at PSP-ene skal avgi en erklæring til myndigheten om at de følger retningslinjene.

5. Disse retningslinjene endrer ikke gyldigheten av den europeiske sentralbankens "Recommendations for the security of internet payments" ("Rapporten"). Rapporten er fortsatt det dokumentet som sentralbankene skal benytte i sin oppsynsrolle når det gjelder internettbetalinger.

6. Retningslinjene utgjør minimum forventninger. Uavhengig av disse har PSP-ene ansvar for å overvåke og vurdere risikoene knyttet til betalingstjenestene, utvikle sine egne detaljerte sikkerhetspolicyer og implementere tilstrekkelig sikkerhet, beredskapsløsning, hendelseshåndtering og reserveløsninger som er tilpasset risikoene.

7. Hensikten med retningslinjene er å definere felles minimumskrav for internettbetalingene som er listet nedenfor, uansett hvilket utstyr som benyttes for tilgang til tjenesten:

    - [kort] utførelse av kortbetalinger på Internett, inkludert betalinger med virtuelle kort og registrering av kortbetalingsdata for bruk i "lommebokløsninger".
    - [kredittoverføringer] gjennomføring av kredittoverføringer (CT-er) på Internett
    - [elektroniske betalingsoppdrag] registrere og endre elektroniske oppdrag for direkte debitering
    - [e-penger] overføring av elektroniske penger mellom to e-pengekontoer via Internett

8. Der retningslinjene angir et utfall, kan dette oppnås på flere måter. Retningslinjene sammen med kravene som følger, utgjør eksempler på beste praksis (i "Annex 1" i EBAs retningslinjer), som PSP-er oppfordres til å følge, men som de ikke er pålagt å følge.

9. Myndigheter og sentralbanken bør samarbeide for å sikre konsistent etterlevelse der betalingstjenestene og instrumentene tilbys gjennom en etablert ordning (f.eks. kortsystem, kredittoverføringssystem, debiteringssystem etc.).

10. Betalingsintegratorer[2] som tilbyr tjenester for initiering av betaling blir sett på som enten innløsere av internettbetalinger (og således som PSP-er) eller som eksterne tjenestetilbydere til de relevante ordningene eller til PSP-en. I siste tilfelle bør integratoren være kontraktsforpliktet til å følge retningslinjene.

11. Unntatt fra retningslinjene er:

- andre internettjenester som tilbys av en PSP via betalingsnettsiden (f.eks. elektronisk megling, online-kontraktsinngåelse);
- betalinger der instruksjonene gis via post, telefon, såkalt "voice mail", eller SMS-basert teknologi;
- mobile betalinger som ikke er basert på nettleser;
- kredittoverføringer der en tredjepart kommer seg inn på kundens betalingskonto;
- betalingstransaksjoner utført av et foretak via dedikerte nettverk;
- kortbetalinger ved bruk av anonyme eller ikke-ladbare fysiske eller virtuelle forhåndsbetalte kort der det ikke er noe fast kundeforhold mellom utsteder og kortholder;
- avregning og oppgjør av betalingstransaksjoner.

Definisjoner

Følgende definisjoner anvendes i dette dokumentet, i tillegg til definisjonene i PSD.

Autentisering er en prosedyre som gjør PSP i stand til å verifisere en kundes identitet.

Sterk kundeautentisering er en prosedyre som bygger på to eller flere av følgende elementer – omtalt som kunnskap, eierskap eller egenskap: i) noe bare brukeren vet, f.eks. et statisk passord, kode, personnummer; ii) noe bare brukeren har, f.eks. kodekalkulator, smartkort, mobiltelefon; iii) noe brukeren er, eksempelvis biometri slik som f.eks. fingeravtrykk. I tillegg må elementene være gjensidig uavhengige – kompromittering av en av dem skal ikke kompromittere en av de andre. Minst ett av elementene bør være ikke gjenbrukbar og ikke kopierbar, og ikke kunne stjeles via Internett. En sterk autentiseringsprosedyre skal være konstruert slik at den beskytter konfidensialiteten til autentiseringsdata.

Autorisasjon er en prosedyre som kontrollerer om en kunde eller en PSP har rett til å utføre visse handlinger, f.eks. rett til å overføre midler, eller rett til tilgang til sensitive data.

Kjennetegn er informasjon – oftest hemmelig – som avgis av kunden eller PSP for autentiseringsformål. Kjennetegn kan også være besittelse av en fysisk redskap som inneholder

[2] Betalingsintegratorer tilbyr betalingsmottaker, dvs. brukerstedet, et standardisert grensesnitt til betalingstjenesten som tilbys av PSP-en.

informasjonen (f.eks. engangspassord-kalkulator, smartkort eller noe brukeren husker eller er (slik som biometriske kjennetegn).

Alvorlig sikkerhetshendelse er en hendelse som har eller kan ha en vesentlig konsekvens for sikkerheten, integriteten eller kontinuiteten til PSP-ens betalingsrelaterte systemer og/eller sikkerheten til sensitive betalingsdata eller midler. Vurdering av vesentlighet skal ta i betraktning potensielt antall kunder som kan bli berørt, potensielt tap og følgen for andre PSP-er eller andre betalingsinfrastrukturer.

Transaksjonsrisikoanalyse innebærer å vurdere risikoen knyttet til en spesifikk transaksjon der man tar i betraktning kriterier som, f.eks. kundens betalingsmønster, verdien på transaksjonen, type produkt og profilen til betalingsmottaker.

Virtuelt kort er en kortbasert betalingsløsning der et alternativt, midlertidig kortnummer med en redusert gyldighetsperiode, begrenset bruk og forhåndsdefinert beløpsgrense blir generert og som kan brukes til kjøp på Internett.

Lommebokløsning er en løsning som tillater kunden å registrere data knyttet til ett eller flere betalingsinstrumenter for å kunne betale hos flere brukersteder.

Kapittel 2 – Retningslinjer for sikkerhet i internettbetalinger

Overordnet kontroll og sikkerhet

Ledelse

1. PSP-ene bør implementere og jevnlig gå gjennom en formell sikkerhetspolicy for internettbetalinger.

    1.1. Policy bør være tilstrekkelig dokumentert, og jevnlig gjennomgått (i tråd med retningslinje 2.4) og godkjent av øverste ledelse. Den bør definere sikkerhetsmål og risikoappetitt.

    1.2. Policy bør definere roller og ansvar, herunder risikostyringsfunksjonen med en direkte rapporteringslinje til styrenivå, og rapporteringslinjene for internett-betalingstjenestene som tilbys, herunder kontroll over sensitive betalingsdata når det gjelder risikovurdering, kontroll og tiltak.

Risikovurdering

2. PSP-er bør gjennomføre og dokumentere grundige risikovurderinger når det gjelder sikkerheten i internettbetalinger og tilhørende tjenester, både før etablering av tjenesten(e) og jevnlig etter dette.

    2.1. Gjennom risikostyringsfunksjonen bør PSP-er gjennomføre og dokumentere i detalj risikovurderinger for internettbetalinger og tilhørende tjenester. PSP-er bør vurdere resultatene av fortløpende overvåking av sikkerhetstrusler relatert til internett-betalingstjenesten som de tilbyr eller planlegger å tilby, og at de tar i betraktning:

i) tekniske løsninger som er benyttet, ii) tjenester som er utkontraktert til eksterne leverandører og, iii) kundens tekniske miljø. PSP-er bør ta i betraktning risikoen knyttet til de valgte teknologiske plattformene, applikasjonsarkitektur, programmeringsteknikkene og rutinene både hos dem selv[3], hos kundene[4], så vel som resultatene av overvåkingen av hendelser.

2.2. Basert på dette bør PSP-ene avgjøre om det er behov for å endre eksisterende sikkerhetstiltak, teknologiene som er benyttet og prosedyrer og tjenester som tilbys. PSP-ene bør ta i betraktning tiden det tar å implementere endringene (herunder utrulling til kunder) og gjøre nødvendige midlertidige tiltak for å minimere sikkerhetshendelser og svindel, så vel som avbrudd.

2.3. Vurderingen av risiko bør inkludere behovet for å beskytte og sikre sensitive betalingsdata.

2.4. Etter vesentlige hendelser som har påvirket tjenesten, bør PSP-er gjennomgå risikoscenarier og eksisterende sikkerhetstiltak, før en eventuell endring i infrastrukturen eller prosedyrer finner sted. Tilsvarende må gjøres når risikoovervåkingen har avdekket nye trusler. I tillegg bør risikovurderingen være gjenstand for en generell gjennomgang minst én gang hvert år. Resultatet av risikovurderingene og gjennomgangene skal oversendes til toppledelsen for godkjenning.

Hendelsesovervåking og rapportering

3. PSP-er bør sikre konsistent og integrert overvåking, behandling og oppfølging av sikkerhetshendelser, inkludert sikkerhetsrelaterte kundeklager. PSP-er bør etablere prosedyrer for å rapportere slike hendelser til ledelsen og, dersom det skjer alvorlige sikkerhetshendelser knyttet til betalingstjenestene, til de kompetente myndigheter.

3.1. PSP-er bør ha på plass en prosess for å overvåke, håndtere og følge opp sikkerhetshendelser og sikkerhetsrelaterte kundeklager og rapportere slike hendelser til ledelsen.

3.2. PSP-er bør ha en prosedyre for raskt å informere kompetente myndigheter (som Finanstilsynet og Datatilsynet), hvis det skjer vesentlige sikkerhetshendelser knyttet til betalingstjenestene.

3.3. PSP-er bør ha på plass en prosedyre for å samarbeide med påtalemyndigheten ved alvorlige sikkerhetshendelser, herunder brudd på konfidensialitet.

3.4. PSP-er som er innløsere, bør kontraktsmessig forplikte brukersteder som lagrer, behandler eller overfører sensitive betalingsdata til å samarbeide med både PSP-en og relevant påtalemyndighet. Hvis en PSP blir oppmerksom på at et brukersted ikke samarbeider slik kontrakten forutsetter, skal PSP-en ta skritt for at det skjer, eller terminere kontrakten.

[3] Som f.eks. risikoen for sesjonskapring, SQL-injeksjon, såkalt "cross site scripting", "buffer overflow" etc.
[4] Som f.eks. risikoer knyttet til å bruke multimedia-applikasjoner, plug-ins til nettleser, rammer, eksterne lenker etc.

Risikokontroll og risikoreduksjon

4. For å redusere den identifiserte risikoen bør PSP-er implementere sikkerhetstiltak i tråd med sikkerhetspolicy. Tiltakene bør inneholde flere lag med sikkerhet, noe som vil øke sannsynligheten for at risikoen blir eliminert før det er skjedd skade ("dybdeforsvar").

   4.1. PSP-er bør ha spesiell oppmerksomhet på arbeidsdeling i IT-miljøet (f.eks. utviklings-, test- og produksjonsmiljøet) når betalingstjenestene blir utformet, utviklet og vedlikeholdt og implementere prinsippet om "minste privilegium" som basis for autentisering og aksesskontroll[5].

   4.2. PSP-er bør ha tilstrekkelige sikkerhetsløsninger på plass for å beskytte nettverk, nettsteder, servere og kommunikasjonslinjer mot misbruk og angrep. PSP-er bør ta bort all overflødig funksjonalitet fra serverne for å beskytte (herde) dem og fjerne eller redusere sårbarheter. Applikasjonenes tilgang til data og ressurser bør holdes på et minimum og følge prinsippet om "minste privilegium". For å begrense risikoen for falske nettsider bør nettsidene som tilbyr betalingstjenester, identifiseres med såkalte "extended validation certificates" utstedt til PSP-en, eller ved annen tilsvarende autentiseringsmetode.

   4.3. PSP-er bør ha egnede prosesser på plass for å overvåke, spore og begrense tilgang til i) sensitive betalingsdata, og ii) kritiske logiske og fysiske ressurser, som nettverk, systemer, databaser, sikkerhetsmoduler etc. PSP-er bør etablere, lagre og analysere logger og revisjonsspor.

   4.4. PSP-ene bør sikre at dataminimering[6] er en vesentlig komponent i kjernefunksjonaliteten ved utforming[7], utvikling og vedlikehold av betalingstjenestene: innsamling, ruting, behandling, lagring og/eller arkivering, og visualisering av sensitive betalingsdata bør holdes på et absolutt minimum.

   4.5. Testing av sikkerhetstiltak for internett-betalingstjenester bør skje under tilsyn av risikostyringsledelsen for å sikre at tiltakene er robuste og effektive. Alle endringer bør undergis en formell endringshåndtering som skal sikre at endringer er tilstrekkelig planlagt, testet, dokumentert og autorisert. Basert på endringene og observerte sikkerhetstrusler bør tester gjentas regelmessig og inkludere scenarier med relevante og kjente, potensielle angrep.

   4.6. PSP-ens sikkerhetstiltak for internett-betalingstjenester bør revideres periodisk for å sikre at de er robuste og effektive. Implementeringen og funksjonaliteten til betalingstjenestene bør også revideres. Frekvens og fokus bør ta hensyn til og stå i forhold til sikkerhetsrisikoen. Revisjonen bør gjennomføres av tiltrodde og uavhengige (interne eller eksterne) eksperter. De bør ikke på noen måte være involvert i utvikling, implementering eller ledelsen av drift av betalingstjenesten.

---

[5] "Alle programmer og privilegerte brukere av systemet bør ha færrest mulig privilegier for å gjøre jobben". Se Saltzer, J.H. (1974): "Protection and the Control of Information Sharing in Multics" i: *Communications of the ACM*, Vol. 17, nr. 7, s. 388.

[6] Dataminimering betyr å samle minst mulig personlig informasjon for å utføre en gitt funksjon.

[7] "Privacy by design"

4.7. Når PSP-en utkontrakterer funksjoner som kan påvirke sikkerheten i internett-betalingstjenesten, skal kontrakten inneholde bestemmelser som sikrer at prinsippene og retningslinjene her følges.

4.8. For å unngå tyveri av sensitive betalingsdata bør PSP-er som tilbyr innløsertjenester, kontraktsmessig kreve at brukersteder som behandler (dvs. lagrer, behandler eller overfører) sensitive betalingsdata, implementerer sikkerhetstiltak i sin infrastruktur i tråd med retningslinjene 4.1 til 4.7. Hvis en PSP blir klar over at et brukersted ikke har påkrevde sikkerhetstiltak på plass, bør PSP-en ta skritt for å sikre dette, eller terminere kontrakten.

Sporbarhet

5. PSP-er bør ha på plass prosesser som sikrer at alle transaksjoner og behandlingsflyt for elektroniske oppdrag er sporet.

5.1. PSP-er bør sikre at tjenesten inkluderer mekanismer for detaljert logging av transaksjoner og elektroniske oppdrag, inkludert transaksjonsserienummer, tidsstempel for transaksjonsdata, parameterendringer så vel som oppslag på transaksjonsdata og data som gjelder elektroniske oppdrag.

5.2. PSP-er bør implementere log-filer som gjør det mulig å spore nye data, endringer eller sletting av data når det gjelder transaksjoner og elektroniske oppdrag.

5.3. PSP-er bør spørre på og analysere data knyttet til transaksjoner og elektroniske oppdrag og sikre at de har verktøy for å vurdere loggfilene. Applikasjonene for dette skal være tilgjengelige bare for autorisert personell.

Spesifikke kontroller og sikkerhetstiltak for internettbetalinger

Innledende kundeidentifisering, informasjon

6. Kunder bør identifiseres i tråd med den europeiske anti-hvitvaskingslovgivningen[8] og bekrefte at de ønsker å gjøre internettbetalinger ved hjelp av tjenestene, før de gis tilgang til slike tjenester. PSP-er bør gi kunden tilstrekkelig informasjon, på forhånd, regelmessig eller ved behov, når det gjelder nødvendige forutsetninger (f.eks. utstyr, prosedyrer) for å utføre sikre internett-betalingstransaksjoner og den iboende risikoen.

6.1. PSP-er bør sikre at kunden har vært gjenstand for "kjenne din kunde"-prosedyrer, og at kunden har avgitt tilstrekkelige identitetsdokumenter[9] og relatert informasjon før kunden blir gitt tilgang til internett-betalingstjenesten.

6.2. PSP-er bør sikre at forhåndsinformasjon[10] som kunden har fått, inneholder nødvendig informasjon relatert til tjenesten. Informasjonen bør inkludere:

[8] For eksempel direktiv 2005/60/EC. Se også Kommisjonsdirektiv 2006/70/EC.
[9] For eksempel pass, nasjonalt ID-kort eller avansert elektronisk signatur.
[10] Informasjonen utfyller artikkel 42 i PSD som angir informasjon som PSP må gi til brukeren av betalingstjenesten før kontrakten med kunden inngås.

- tydelig informasjon om forutsetninger i form av kundeutstyr, programvare eller andre nødvendige hjelpemidler (f.eks. antivirus programvare, brannmur);
- retningslinjer for riktig og sikker bruk av sikkerhetskjennetegn;
- en skritt for skritt-beskrivelse av prosedyren for registrering og autorisering av betalinger og/eller innhenting av informasjon, herunder følgene av hver handling;
- retningslinjer for riktig og sikker bruk av all maskinvare og programvare som brukeren har fått;
- prosedyren som skal følges i tilfelle tyveri av sikkerhetskjennetegn eller kundens maskinvare eller programvare som benyttes for innlogging eller gjennomføring av betalinger;
- prosedyrene som skal følges hvis det oppdages misbruk eller mistanke om misbruk;
- en beskrivelse av PSP-ens og kundens ansvar og erstatning når det gjelder bruk av betalingstjenesten.

6.3. PSP-er bør sikre at rammeavtalen med kunden spesifiserer at PSP-en kan stoppe en bestemt transaksjon eller betalingsinstrumentet[11] ut ifra sikkerhetsbetraktninger. Den bør beskrive metode og vilkår når det gjelder melding til kunde, og hvordan kunden kan kontakte PSP-en for å åpne tjenesten eller betalingstransaksjonen igjen, i tråd med PSD.

Sterk kundeautentisering

7. Iverksetting av en internettbetaling, så vel som tilgang til sensitive betalingsdata, bør beskyttes av sterk kundeautentisering. PSP-er bør ha en prosedyre for sterk kundeautentisering i tråd med definisjonen i disse retningslinjene.

7.1. [KO/e-oppdrag/e-penger] PSP-er bør foreta sterk kundeautentisering når kunden godkjenner internettbetalinger (inkludert bunter med KO-er) og når kunden gir eller endrer oppdrag for direkte debitering. Men PSP-er kan vurdere å benytte alternative metoder for kundeautentisering for:

- utgående betalinger til tiltrodde mottakere som er inkludert i kundens hvitelister som er etablert tidligere;
- transaksjoner mellom to kontoer som tilhører samme kunde hos samme PSP;
- overføringer innen samme PSP i henhold til en risikovurdering;
- lav-verdi-transaksjoner[12], slik de er definert i PSD.

7.2. Tilgang til eller endring av sensitive betalingsdata (inklusive opprettelse eller endring av hvitelister) krever sterk kundeautentisering. Hvis PSP-en tilbyr utelukkende konsulenttjenester, uten å vise sensitive kunde- eller betalingsdata, slik som kortdata, som lett kunne vært misbrukt til svindel, kan PSP-en tilpasse autentiseringskravene til dette basert på en risikovurdering.

[11] Se artikkel 55 i PSD når det gjelder grenser for bruken av betalingsinstrumentet.
[12] Se definisjonen av lav-verdi-transaksjoner i artikkel 34(1) og 53(1) i PSD.

7.3. [kort] Alle utstedere bør støtte sterk kortholderautentisering for korttransaksjoner. Alle kort som utstedes, må være teknisk klargjort (registrert) for sterk kundeautentisering.

7.4. [kort] PSP-er som tilbyr innløsertjenester, bør støtte teknologier som gjør utsteder i stand til å foreta sterk kundeautentisering av kortholder for kortordningen som innløseren deltar i.

7.5. [kort] PSP-er som tilbyr innløsertjenester, bør kreve at brukerstedene støtter løsninger som gjør utsteder i stand til å foreta sterk kundeautentisering av kortholder for korttransaksjoner på Internett. Bruk av alternative autentiseringsmekanismer kan vurderes for predefinerte kategorier av lavrisiko-transaksjoner, eksempelvis basert på en transaksjonsrisikoanalyse, eller lav-verdi-betalinger, slik de er definert i PSD.

7.6. [kort] For kortordninger som tjenesten støtter, skal tilbydere av lommebokløsninger kreve sterk kundeautentisering av utsteder når brukeren første gang registrerer kortdata.

7.7. Tilbydere av lommebokløsninger bør støtte sterk kundeautentisering når kunden logger inn på lommeboken eller utfører korttransaksjoner på Internett. Bruk av alternative autentiseringsmekanismer kan vurderes for predefinerte kategorier av lavrisiko-transaksjoner, eksempelvis basert på en transaksjonsrisikoanalyse, eller lav-verdi-betalinger, slik de er definert i PSD.

7.8. [kort] For virtuelle kort bør førstegangs registrering skje i trygge og tiltrodde omgivelser[13]. Sterk kundeautentisering bør kreves for generering av kortdata hvis kortet utstedes på Internett.

7.9. PSP-er bør sikre gjensidige autentisering under kommunikasjon med brukersteder i den hensikt å igangsette internettbetalinger og aksessere sensitive betalingsdata.

Registrering og utstedelse av autentiseringsmekanismer og/eller programvare som leveres til kunden

8. PSP-er bør sikre at registrering og førstegangs utstedelse av autentiseringsmekanismer som kreves for å benytte betalingstjenesten på Internett og levering av betalingsrelatert programvare skjer på sikker måte.

8.1. Registrering og utstedelse av autentiseringsmekanismer og/eller betalingsrelatert programvare som leveres til kunden bør innfri følgende krav:

- Relaterte prosedyrer bør skje i trygge og tiltrodde omgivelser som tar hensyn til mulig risiko knyttet til enheter som ikke er under PSP-ens kontroll.

- Effektive og sikre prosedyrer bør være etablert når det gjelder levering av personaliserte sikkerhetskjennetegn, betalingsrelatert programvare og alle personaliserte enheter relatert til internettbetaling. Programvare som er levert over

[13] Omgivelser som PSP-en er ansvarlig for hvor autentisering av kunden og PSP-en skjer, og der konfidensielle/sensitive data skal være beskyttet. De inkluderer: i) PSP-ens lokaler, ii) internettbank og andre sikre nettsider, eller iii) minibanktjenester.

Internett, bør være digitalt signert av PSP-en slik at kunden kan verifisere avsender og kontrollere at programvaren ikke er endret av uvedkommende.

- [kort] For korttransaksjoner bør kunden kunne velge å registrere seg for sterk kundeautentisering uavhengig av et spesifikt internettkjøp. Dersom aktivering tilbys i tilknytning til netthandel, bør brukeren rutes til sikre og tiltrodde omgivelser.

8.2. [kort] Utstedere bør aktivt oppfordre til å registrere seg for sterk kundeautentisering og tillate kortholdere å omgå å registrere seg bare i spesielle og begrensede tilfeller som kan forsvares ut ifra risikoen knyttet til den spesifikke kort-transaksjonen.

Antall innloggingsforsøk, sesjonsvarighet, gyldighet av autentisering

9. PSP-er bør begrense antall innloggings- og autentiseringsforsøk, definere sesjonsvarighet for internett-betalingstjenester og begrense varigheten av autentiseringen.

9.1. Når engangspassord benyttes for autentisering bør PSP-er sikre at gyldigheten av passordet er begrenset til et absolutt minimum.

9.2. PSP-er bør definere maksimum antall feilede påloggingsforsøk eller autentiseringsforsøk som tillates før tilgangen til betalingstjenesten blir (midlertidig eller permanent) blokkert. De bør ha en sikker prosedyre for å reaktivere blokkerte tilganger.

9.3. PSP-er bør definere maksimum tid før en inaktiv betalingssesjon stenges ned automatisk.

Transaksjonsovervåking

10. Mekanismer for transaksjonsovervåking som skal hindre, avdekke og blokkere bedragerske betalinger bør ha kontrollert transaksjonen før PSP-en godkjenner den; mistenkelige eller høyrisikotransaksjoner bør være gjenstand for spesiell analyse og vurdering. Tilsvarende sikkerhetsovervåking og autorisasjonsmekanismer bør være på plass når det gjelder registrering av elektroniske oppdrag.

10.1. PSP-er bør benytte svindeloppdagende og avvergende systemer for å identifisere mistenkelige transaksjoner før PSP-en endelig godkjenner transaksjonen eller e-oppdraget. Slike systemer bør vært basert på eksempelvis parameteriserte regler (som svartelister over kompromitterte eller stjålne kort), og overvåking av unormal kundeatferd eller kundeterminal (som endring av IP-adresse eller IP-segment i løpet av betalingssesjonen, ved hjelp av såkalte geolokasjon-kontroller[14], brukersteder som kunden vanligvis ikke benytter eller unormale transaksjonsdata etc.). Systemene bør også kunne oppdage tegn på om sesjonen er infisert med ondartet kode (for eksempel om det er tegn på at registrering av betalingsdetaljer eller autentiseringsdetaljer blir registrert av et (svindlersk) program og ikke et menneske) og kjente svindelscenarier. Omfang, kompleksitet og anvendelse av overvåkingsløsningene må etterleve relevant databeskyttelseslovgivning og være tilpasset utfallet av risikoanalysen.

[14] Geolokasjon-kontroll verifiserer om utstederlandet korresponderer med IP-adressen til brukeren.

10.2. PSP-er som driver innløsning, bør overvåke brukerstedene ved hjelp av svindeloppdagende og avvergende systemer.

10.3. PSP-er bør gjøre transaksjonsanalyse og vurdering innenfor en tidsramme som gjør at igangsetting og utførelse av betalingstjenesten ikke utsettes unødvendig.

10.4. Der en PSP, i henhold til risikopolicy til PSP-en, har bestemt seg for å blokkere en transaksjon som er identifisert til å være en mulig bedragersk transaksjon, skal PSP-en opprettholde blokkeringen i så kort tid som mulig inntil sikkerhetsspørsmålet er avgjort.

Beskyttelse av sensitive betalingsdata

11. Sensitive betalingsdata bør beskyttes under lagring, bearbeiding og overføring.

11.1. All data som benyttes for å identifisere og autentisere kunden (f.eks. ved innlogging, ved oppstart av internettbetalinger, og under opprettelse, endring eller avslutning av e-oppdrag) og kundegrensesnittet (nettstedet til PSP-en eller brukerstedet), bør være beskyttet mot tyveri og uautorisert tilgang eller endring.

11.2. For å sikre konfidensialitet og integritet på dataene, bør PSP-ene sikre at ende-til-ende-kryptering[15] ved hjelp av sterke og anerkjente krypteringsmekanismer er etablert mellom de kommuniserende parter når sensitive betalingsdata utveksles over Internett.

11.3. PSP-er som tilbyr innløsertjenester bør oppfordre brukerstedene til ikke å lagre sensitive betalingsdata. I tilfelle brukerstedene behandler, dvs. lagrer, bearbeider eller overfører sensitive betalingsdata, bør PSP-en kontraktsmessig kreve at brukerstedet har nødvendige tiltak på plass for å beskytte dataene. PSP-ene bør foreta jevnlige kontroller, og hvis en PSP blir oppmerksom på at et brukersted som behandler sensitive betalingsdata ikke har foreskrevet sikkerhet på plass, så skal PSP-en ta skritt for å sikre dette eller terminere kontrakten.

Kundeatferd, kundeopplæring og kommunikasjon

Kundeopplæring og kommunikasjon

12. PSP-er bør tilby kundestøtte og kundeveiledning etter behov når det gjelder sikker bruk av betalingstjenesten. PSP-er bør kommunisere med kunden på en måte som gjør PSP-en sikker på ektheten av meldingene som mottas.

12.1. PSP-ene bør tilby minst én sikker kanal[16] for løpende kommunikasjon med kundene når det gjelder riktig og sikker bruk av betalingstjenesten. PSP-ene bør gi kundene informasjon om denne kanalen og forklare at all annen kommunikasjon, så som e-post, når det gjelder riktig og sikker bruk av betalingstjenesten, ikke er gyldig. PSP-en bør redegjøre for:

[15] Ende-til-ende-kryptering er kryptering som skjer i avsenders nettverk og der dekrypteringen skjer i mottakers nett.
[16] Som for eksempel en dedikert postkasse på PSP-ens webside eller en sikker webside.

- prosedyren som kundene skal benytte for å melde til PSP-en om bedragerske betalinger eller mistanke om slike, mistenkelige hendelser eller avvik i løpet av betalingssesjonen og/eller mulig forsøk på sosial manipulering;

- neste skritt, dvs. hvordan PSP-en vil svare kunden;

- hvordan PSP-en vil informere kunden om (potensielle) bedragerske transaksjoner eller avvisning av slike, eller advare kunden om angrep (f.eks. forsøk på nettfiske ved hjelp av e-post).

12.2. PSP-en bør informere kunden om alle endringer i sikkerhetsprosedyrer som gjelder betalingstjenesten via den sikre kanalen. Alle advarsler om gryende risikoer (f.eks. advarsler om sosial manipulering) bør også formidles via den sikre kanalen.

12.3. PSP-ene bør tilby kundestøtte når det gjelder spørsmål, klager, anmodning om støtte og meldinger om avvik eller hendelser knyttet til betalinger og tilknyttede tjenester, og kunden bør bli tilstrekkelig informert om hvordan hun kan få slik støtte.

12.4. PSP-er bør initiere kundeopplæring og bevisstgjøringsprogrammer som skal gjøre kunden i stand til, som et minimum:

- å beskytte passord, sikkerhetsmekanismer, personlige data og andre konfidensielle data;
- å administrere sikkerheten på maskinen sin (f.eks. PC) ved å installere og oppdatere sikkerhetskomponenter (antivirus, brannmur, oppdateringer);
- å vurdere den betydelige trusselen og risikoen det er å laste ned programvare via Internett uten å være tilstrekkelig sikker på at programvaren er ekte og ikke har blitt endret;
- å sikre at hun benytter PSP-ens nettside og ikke en falsk nettside.

12.5. PSP-er som gjør innløsning, skal kreve av brukerstedene at de klart skiller betalingsrelaterte prosesser fra butikktjenester for på den måten å gjøre det lettere for kunder å vite om de kommuniserer med PSP-en eller betalingsmottaker (f.eks. ved å rute om kunden og åpne et eget vindu slik at betalingsprosessen ikke skjer innenfor brukerstedets ramme).

Meldinger, grenser

13. PSP-er bør sette grenser[17] for internettbetalinger og kan gi kunden mulighet for å sette ytterligere grenser innenfor PSP-ens grenser. PSP-ene kan også tilby varslingstjenester og tjenester som gjør kunden i stand til å gjøre endringer på profilen sin.

13.1. Før kunden får tilgang til betalingstjenester, bør PSP-en sette grenser (f.eks. beløpsgrense for hver betaling eller en omsetningsgrense som gjelder for en periode) og bør informere kundene om disse. PSP-ene bør tillate kunden å skru av betalingstjenesten.

[17] Kan være globale grenser (for alle instrumenter som kan benyttes for internettbetalinger) eller individuelle grenser.

Kundens adgang til informasjon om status på igangsetting av betaling og utføring av den

14. PSP-er bør informere kunden om en betaling er påbegynt og i god tid gi kunden nødvendig informasjon slik at hun kan kontrollere at betalingen er gyldig iverksatt og/eller gjennomført.

    14.1. [KO/e-oppdrag] PSP-er bør tilby kunden en måte å sjekke status på behandlingen av en transaksjon i nær realtid og en måte å sjekke saldo på til enhver tid, i en sikker og tiltrodd omgivelse.

    14.2. Alle detaljerte elektroniske kontoutskrifter bør gjøre tilgjengelige i trygge og tiltrodde omgivelser. Hvis PSP-en gir melding over en alternativ kanal, for eksempel SMS, e-post eller brev, om at kontoutskrifter er tilgjengelige (for eksempel regelmessige elektroniske kontoutdrag eller ad hoc etter utføringen av en transaksjon), så skal sensitive betalingsdata ikke være med i meldingen, alternativt være maskert.

Kapittel 3 – Innføring

Disse retningslinjene gjelder fra 1.8.2015.