EBA/GL/2014/12_rev1

19. prosince 2014

# Obecné pokyny (konečné znění)

## k bezpečnosti internetových plateb

# Obsah

# Obecné pokyny k bezpečnosti internetových plateb

## Status těchto obecných pokynů

Tento dokument obsahuje obecné pokyny vydané v souladu s článkem 16 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (dále jen „nařízení o orgánu EBA“). V souladu s čl. 16 odst. 3 nařízení o orgánu EBA musí příslušné orgány a finanční instituce vynaložit veškeré úsilí, aby se těmito obecnými pokyny řídily.

Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by právní předpisy Unie měly být uplatňovány v konkrétní oblasti. Orgán EBA tudíž očekává, že se obecnými pokyny budou řídit všechny příslušné orgány a finanční instituce, kterým jsou obecné pokyny určeny. Příslušné orgány, na které se obecné pokyny vztahují, by se jimi měly řídit tak, že je náležitě začlení do svých postupů dohledu (např. změnou svého právního rámce nebo svých procesů dohledu), a to i tam, kde jsou obecné pokyny určeny primárně institucím.

## Oznamovací povinnost

V souladu s čl. 16 odst. 3 nařízení o orgánu EBA musí příslušné orgány do 5. května 2015 oznámit orgánu EBA, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Nebude-li do tohoto termínu podáno žádné oznámení, bude mít orgán EBA za to, že se příslušné orgány těmito pokyny neřídí. Oznámení by měla být zaslána na formuláři, který lze nalézt v oddíle 5, na e-mailovou adresu compliance@eba.europa.eu s uvedením referenčního čísla „EBA/GL/2014/12“. Oznámení by měly podat osoby oprávněné oznámit jménem svého příslušného orgánu, zda se těmito pokyny řídí, či nikoli.

Oznámení budou v souladu s čl. 16 odst. 3 zveřejněna na internetových stránkách orgánu EBA.

# Hlava I – Oblast působnosti a definice

## Oblast působnosti

1. Tyto obecné pokyny stanoví soubor minimálních požadavků v oblasti bezpečnosti internetových plateb. Obecné pokyny vycházejí z pravidel směrnice 2007/64/ES[1] (dále jen „směrnice o platebních službách“), které se týkají požadavků na informace o platebních službách a povinností poskytovatelů platebních služeb (PPS) v souvislosti s poskytováním platebních služeb. Čl. 10 odst. 4 směrnice dále vyžaduje, aby měly platební instituce zavedeny spolehlivé mechanismy pro správu a řízení a odpovídající vnitřní kontrolní mechanismy.

2. Obecné pokyny se vztahují na poskytování platebních služeb, které PPS definovaní v článku 1 směrnice nabízejí prostřednictvím internetu.

3. Obecné pokyny jsou určeny finančním institucím podle čl. 4 odst. 1 nařízení (EU) č. 1093/2010 a příslušným orgánům podle čl. 4 odst. 2 nařízení (EU) č. 1093/2010. Příslušné orgány ve 28 členských státech Evropské unie by měly zajistit, aby PPS definovaní v článku 1 směrnice o platebních službách používali tyto obecné pokyny pod jejich dohledem.

4. Příslušné orgány mohou dále rozhodnout, že PPS požádají, aby podávali příslušnému orgánu zprávy o tom, že tyto obecné pokyny dodržují.

5. Těmito obecnými pokyny není dotčena platnost „Doporučení pro bezpečnost internetových plateb“ Evropské centrální banky (dále jen „zpráva“)[2]. Zpráva je i nadále především dokumentem, podle něhož by centrální banky v rámci funkce dozoru nad platebními systémy a prostředky měly posuzovat dodržování z hlediska bezpečnosti internetových plateb.

6. Obecné pokyny představují minimální očekávání. Není jimi dotčena povinnost PPS sledovat a posuzovat rizika související s jejich platebními operacemi, vyhotovit své vlastní podrobné bezpečnostní politiky a zavést odpovídající bezpečnostní opatření, opatření pro nepředvídané události, jakož i opatření v oblasti zvládání incidentů a zajištění kontinuity obchodní činnosti, která jsou přiměřená rizikům souvisejícím s poskytovanými platebními službami.

7. Účelem těchto obecných pokynů je určit společné minimální požadavky na níže uvedené internetové platební služby, a to bez ohledu na použité přístupové zařízení:

    - [karty] provádění plateb kartou na internetu, včetně plateb pomocí virtuálních karet, jakož i registrace údajů o platebních kartách pro použití řešení typu elektronické peněženky („wallet solutions“);

[1] Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES, Úř. věst. L 319, 5.12.2007.

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

- [bezhotovostní převody] provádění bezhotovostních převodů na internetu;

- [elektronické oprávnění („e-mandate“)] vydávání a změny elektronických oprávnění k inkasu;

- [elektronické peníze („e-money“)] převody elektronických peněz mezi dvěma elektronickými účty prostřednictvím internetu.

8. Pokud obecné pokyny uvádějí cílový stav, lze tohoto cílového stavu dosáhnout různými způsoby. Kromě dále stanovených požadavků obsahují tyto obecné pokyny pro poskytovatele platebních služeb také příklady osvědčených postupů (v příloze č. 1), jejichž dodržování se nevyžaduje, nýbrž pouze doporučuje.

9. Pokud je poskytování platebních služeb a prostředků nabízeno prostřednictvím platebního systému (např. systému karetních transakcí, systému bankovních převodů, inkasního systému apod.), měly by příslušné orgány a příslušná centrální banka s funkcí dozoru nad platebními prostředky spolupracovat na zajištění jednotného používání obecných pokynů aktéry odpovědnými za fungování systému.

10. Platební integrátoři[3] nabízející služby zahájení plateb jsou považováni buď za zúčtovatele internetových platebních služeb (a tudíž za PPS), nebo za externí poskytovatele technických služeb pro příslušné systémy nebo PPS. Ve druhém jmenovaném případě by měli být platební integrátoři smluvně vázáni řídit se těmito pokyny.

11. Z rozsahu obecných pokynů jsou vyloučeny tyto transakce:

- další internetové služby, které poskytuje PPS prostřednictvím své platební webové stránky (např. elektronické makléřství, on-line smlouvy);

- platby, kde je pokyn podán poštou, na základě telefonické objednávky, hlasovou poštou nebo s využitím technologie SMS;

- mobilní platby kromě plateb z internetových prohlížečů;

- bezhotovostní převody, kde má třetí osoba přístup k platebnímu účtu klienta;

- platební transakce provedené podnikem prostřednictvím vyhrazených sítí;

- platby kartou využívající anonymní fyzické nebo virtuální předplacené karty bez možnosti dobití peněžních prostředků, kdy mezi vydavatelem a držitelem karty není žádný trvalý vztah;

- zúčtování a vypořádání platebních transakcí.

[3] Platební integrátoři poskytují příjemci platby (tj. internetovému obchodníkovi) standardizované rozhraní ke službám pro zahájení plateb poskytovaných PPS.

## Definice

12. Pro účely těchto obecných pokynů a nad rámec definic uvedených ve směrnici o platebních službách se rozumí:

- *autentizací* postup, který PPS umožňuje ověřit totožnost klienta,

- *silnou autentizací klienta* pro účely těchto obecných pokynů postup založený na využití dvou nebo více následujících prvků – klasifikovaných jako znalosti, vlastnictví a jedinečnost: i) něco, co zná pouze uživatel, např. statické heslo, kód, osobní identifikační číslo; ii) něco, co vlastní pouze uživatel, např. bezpečnostní klíč (token), čipová karta, mobilní telefon; iii) něco, čím uživatel je, např. biometrická charakteristika, jako je například otisk prstu. Zvolené prvky musejí být navíc vzájemně nezávislé, tj. porušení jednoho prvku nenaruší ostatní prvky. Nejméně jeden z těchto prvků by neměl být znovu použitelný a replikovatelný (s výjimkou jedinečnosti) a nemělo by být možné jej tajně zcizit přes internet. Celý postup silné autentizace by měl být navržen tak, aby byla chráněna důvěrnost údajů umožňujících autentizaci;

- *autorizací* postup, který kontroluje, zda má klient nebo PPS oprávnění provádět určitou činnost, např. oprávnění k převodu finančních prostředků nebo k přístupu k citlivým údajům;

- *ověřovacími údaji* informace – obecně důvěrné – poskytované klientem nebo PPS za účelem autentizace. Ověřovací údaje mohou také představovat fyzický nástroj obsahující informace (např. generátor jednorázových hesel, čipová karta) nebo něco, co si uživatel zapamatuje nebo co sám představuje (např. biometrické charakteristiky);

- *závažným platebním bezpečnostním incidentem* událost, která má nebo může mít závažný dopad na bezpečnost, integritu nebo kontinuitu souvisejících platebních systémů u PPS anebo na bezpečnost citlivých údajů o platbách nebo finančních prostředcích. Při posouzení závažnosti incidentu by se měl vzít v úvahu počet potenciálně dotčených klientů, rozsah možné škody a dopad na ostatní PPS nebo jiné platební infrastruktury;

- *analýzou transakčního rizika* vyhodnocení rizika spojeného s určitou transakcí při zohlednění kritérií, jako např. platební chování klienta, hodnota příslušné transakce, typ produktu a profil příjemce;

- *virtuálními kartami* platební řešení na bázi karet, kdy je generováno alternativní dočasné číslo karty se zkrácenou dobou platnosti, omezeným rozsahem použití a předem stanoveným limitem výdajů, které může být použito pro internetové nákupy;

- *řešením pro elektronické peněženky* řešení, které umožňuje klientovi registraci údajů souvisejících s jedním či více platebními prostředky tak, aby mohl provádět platby u více internetových obchodníků.

# Hlava II – Obecné pokyny k bezpečnosti internetových plateb

## Celkové kontrolní a bezpečnostní prostředí

### Řízení

1. PPS by měli zavést a pravidelně přezkoumávat formální bezpečnostní politiku pro internetové platební služby.

   1.1 Bezpečnostní politika by měla být řádně zdokumentována a pravidelně přezkoumávána (v souladu s bodem 2.4 obecných pokynů) a schvalována vrcholným vedením společnosti. Měla by určit cíle v oblasti bezpečnosti a ochotu riskovat.

   1.2 Bezpečnostní politika by měla určit role a odpovědnosti, včetně funkce řízení rizika s přímou odpovědností vůči představenstvu, a hierarchické vazby podřízenosti pro poskytované internetové platební služby, včetně řízení citlivých platebních údajů s přihlédnutím k hodnocení, řízení a snižování rizika.

### Hodnocení rizik

2. PPS by měli provést a zdokumentovat důkladná hodnocení rizik týkajících se bezpečnosti internetových plateb a souvisejících služeb, a to jak před zřízením služby (služeb), tak i pravidelně poté.

   2.1 PPS by měli z titulu své funkce řízení rizik provést a zdokumentovat důkladná hodnocení rizik týkajících se internetových plateb a souvisejících služeb. PPS by měli zvážit výsledky soustavného sledování bezpečnostních hrozeb týkajících se internetových platebních služeb, které nabízejí nebo mají v plánu nabízet, přičemž zohlední: i) technologická řešení, která využívají, ii) služby zajišťované u externích poskytovatelů a iii) technické prostředí klientů. PPS by měli posoudit rizika spojená se zvolenými technologickými platformami, architekturou aplikací, programovacími technikami a postupy, a to jak na své straně[4], tak i na straně svých klientů[5], a rovněž výsledky postupu sledování bezpečnostních incidentů (viz obecný pokyn č. 3).

   2.2 Na tomto základě by PPS měli určit, zda a v jakém rozsahu může být nezbytné provést změny stávajících bezpečnostních opatření, používaných technologií a postupů či služeb, které jsou nabízeny. PPS by měli vzít v úvahu dobu potřebnou k provedení těchto změn (včetně jejich zavedení u klientů) a přijmout vhodná předběžná opatření k minimalizaci bezpečnostních incidentů, podvodů i případných rušivých dopadů.

[4] Jedná se např. o odolnost systému vůči neoprávněnému ovládnutí platební relace (payment session hijacking), injektování kódů (SQL injection), XSS (cross-site scripting), přeplnění vyrovnávací paměti (buffer) apod.

[5] Jedná se např. o rizika spojená s používáním multimediálních aplikací, zásuvných modelů prohlížečů, rámečků, externích odkazů apod.

2.3 Hodnocení rizik by mělo řešit potřebu chránit a zabezpečit citlivé platební údaje.

2.4 PPS by měli provést přezkum rizikových scénářů a stávajících bezpečnostních opatření po významných incidentech s dopadem na jejich služby, před významnou změnou své infrastruktury či postupů, a jestliže postupy v oblasti sledování rizik odhalí nové hrozby. Dále by měl být alespoň jednou ročně proveden celkový přezkum hodnocení rizik. Výsledky hodnocení rizik a přezkumů by měly být předloženy ke schválení vrcholnému vedení.

## Sledování a hlášení incidentů

3. PPS by měli zajistit důsledné a integrované sledování, zvládání a následnou kontrolu bezpečnostních incidentů, včetně stížností klientů ohledně bezpečnosti. PPS by měli stanovit postup pro hlášení těchto incidentů vedení společnosti a v případě významných incidentů týkajících se platební bezpečnosti i příslušným orgánům.

3.1 PPS by měli mít zaveden postup pro sledování, zvládání a následnou kontrolu bezpečnostních incidentů, včetně stížností klientů ohledně bezpečnosti a tyto incidenty hlásit vedení společnosti.

3.2 PPS by měli mít zaveden postup pro okamžité informování příslušných orgánů (tj. orgánů v oblasti dohledu, dozoru a ochrany údajů), pokud existují, v případě významných incidentů týkajících se platební bezpečnosti vzhledem k poskytovaným platebním službám.

3.3 PPS by měli mít zaveden postup pro spolupráci v případě významných incidentů týkajících se platební bezpečnosti, včetně porušení ochrany údajů, s příslušnými donucovacími orgány.

3.4 PPS zajišťující zúčtování karetních transakcí by měli smluvně vyžadovat od internetových obchodníků, kteří uchovávají, zpracovávají či přenášejí citlivé platební údaje, aby v případě významných incidentů týkajících se platební bezpečnosti, včetně porušení ochrany údajů, spolupracovali jak s nimi, tak i s příslušnými donucovacími orgány. Pokud se PPS dozví, že internetový obchodník nespolupracuje tak, jak vyžaduje smlouva, měl by podniknout kroky k vymáhání plnění této smluvní povinnosti nebo smlouvu vypovědět.

## Řízení a snižování rizika

4. PPS by měli zavést bezpečnostní opatření v souladu se svými příslušnými bezpečnostními politikami za účelem snížení zjištěných rizik. Tato opatření by měla zahrnovat několik vrstev bezpečnostní ochrany, kdy je případné selhání jedné linie ochrany zachyceno vrstvou následující („hloubková ochrana“).

4.1 Při navrhování, vývoji a údržbě internetových platebních služeb by PPS měli věnovat zvláštní pozornost odpovídajícímu rozdělení povinností v prostředí informačních technologií (např. vývojová, testovací a výrobní prostředí) a řádnému provádění tzv. principu nejnižších privilegií (zásady minimálních práv) jakožto základu pro kvalitní řízení identity a přístupu[6].

4.2 PPS by měli mít zavedena vhodná bezpečnostní řešení na ochranu sítí, webových stránek, serverů a komunikačních spojení proti zneužití nebo útokům. PPS by měli servery zbavit všech nadbytečných funkcí, aby je ochránili (zvýšili jejich odolnost) a aby odstranili či omezili zranitelná místa aplikací vystavených riziku. Přístup různých aplikací k požadovaným údajům a zdrojům by měl být poskytován pouze na nezbytně nutné úrovni v souladu s principem nejnižších privilegií. Za účelem omezení používání „falešných" webových stránek (napodobujících skutečné stránky PPS) by měly být transakční webové stránky nabízející internetové platební služby zajištěny certifikáty s vyšším stupněm ověření vystavených na jméno PPS nebo s využitím obdobných autentizačních metod.

4.3 PPS by měly mít zavedeny vhodné postupy pro sledování, dohledání a omezení přístupu, jestliže se jedná o: i) citlivé platební údaje a ii) logické a fyzické důležité zdroje, jako jsou např. sítě, systémy, databáze, bezpečnostní moduly apod. PPS by měli vytvářet, uchovávat a analyzovat příslušné protokoly a revizní záznamy.

4.4 Při navrhování[7], vývoji a údržbě internetových platebních služeb by měli PPS zajistit, aby zásadní součástí klíčové funkcionality byla minimalizace dat[8]: shromažďování, směrování, zpracování, ukládání anebo archivace a vizualizace citlivých platebních údajů by měly být omezeny pouze na absolutně nezbytné minimum.

4.5 Bezpečnostní opatření pro internetové platební služby by měla být testována pod dohledem útvaru řízení rizik, aby byla zajištěna jejich odolnost a účinnost. Na veškeré změny by se měl vztahovat formální postup změnového řízení, jehož účelem je zajistit, aby byly změny správně naplánovány, otestovány, zdokumentovány a schváleny. Na základě provedených změn a zjištěných bezpečnostních hrozeb by se testy měly pravidelně opakovat a měly by zahrnovat scénáře významných a známých potenciálních útoků.

4.6 Bezpečnostní opatření PPS v oblasti internetových platebních služeb by měla být pravidelně prověřována, aby byla zajištěna jejich odolnost a účinnost. Mělo by být prověřováno i provádění a fungování internetových platebních služeb. Četnost

[6] „Každý program a každý privilegovaný uživatel systému by měl pracovat s použitím nejmenší množiny privilegií potřebných k provedení daného úkolu." Viz Saltzer, J.H. (1974), „Ochrana a řízení sdílení informací v Multicsu", Communications of the ACM, svazek 17, č. 7, str. 388.

[7] Ochrana soukromí již od návrhu (privacy by design).

[8] Minimalizace dat vychází ze zásady shromažďovat co nejmenší množství osobních údajů nutných k výkonu dané funkce.

a zaměření těchto prověrek by měly zohledňovat související bezpečnostní rizika a být jim úměrné. Prověrky by měli provádět důvěryhodní a nezávislí (interní či externí) odborníci. Ti by se neměli žádným způsobem podílet na vývoji, realizaci či provozním řízení poskytovaných internetových platebních služeb.

4.7 Jestliže PPS zajišťují funkce týkající se bezpečnosti internetových platebních služeb u externích dodavatelů, měla by smlouva obsahovat ustanovení vyžadující dodržování zásad a pokynů uvedených v těchto obecných pokynech.

4.8 PPS nabízející služby zúčtování karetních transakcí by měli smluvně vyžadovat od internetových obchodníků, kteří nakládají s citlivými platebními údaji (tj. tyto uchovávají, zpracovávají či přenášejí), aby v rámci své IT infrastruktury přijali bezpečnostní opatření v souladu s body 4.1 až 4.7 obecných pokynů s cílem zabránit krádeži těchto citlivých platebních údajů prostřednictvím svých systémů. Pokud se PPS dozví, že internetový obchodník nemá zavedena požadovaná bezpečnostní opatření, měl by podniknout kroky k vymáhání plnění této smluvní povinnosti nebo smlouvu vypovědět.

### Sledovatelnost

5. PPS by měli mít zavedeny postupy zajišťující, aby veškeré transakce, jakož i postup elektronického oprávnění (e-mandate), byly odpovídajícím způsobem sledovány.

5.1 PPS by měli zajistit, aby jejich služba obsahovala bezpečnostní mechanismy pro podrobné záznamy údajů o transakcích a elektronickém oprávnění, včetně pořadového čísla transakce, časových razítek k údajům o transakcích, změn parametrizace a rovněž včetně přístupu k údajům o transakcích a o elektronickém oprávnění.

5.2 PPS by měli zavést protokolové soubory umožňující dohledání jakýchkoliv případných doplňků, změn či výmazů dat týkajících se transakcí a elektronického oprávnění.

5.3 PPS by měli data týkající se transakcí a elektronického oprávnění podrobit dotazování a analýzám a zajistit, aby měli k dispozici nástroje k vyhodnocení protokolových souborů. Příslušné aplikace by měly být k dispozici pouze oprávněným pracovníkům.

## Konkrétní kontrolní a bezpečnostní opatření pro internetové platby

### Prvotní ověření totožnosti klienta, informace

6. Totožnost klientů by měla být řádně ověřena v souladu s evropskými předpisy proti praní peněz[9] a klienti by měli potvrdit svou ochotu provádět internetové platby s využitím služeb,

[9] Např. směrnice Evropského parlamentu a Rady 2005/60/ES ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu. Úř. věst. L 309, 25. 11. 2005, s. 15–36. Viz také směrnice Komise 2006/70/ES ze dne 1. srpna 2006, kterou se stanoví prováděcí opatření ke směrnici Evropského parlamentu a Rady 2005/60/ES, pokud se jedná o definici „politicky exponovaných osob“ a technická kritéria pro zjednodušenou

dříve než jim bude k těmto službám udělen přístup. PPS by měli klientovi poskytnout odpovídající informace o požadavcích (např. na vybavení a postupy) nezbytných pro realizaci bezpečných platebních transakcí přes internet a o souvisejících rizicích, přičemž tyto informace by měly být podle potřeby poskytovány buď předem, průběžně nebo případně ad hoc.

6.1 PPS by měli zajistit, aby klient podstoupil příslušnou hloubkovou kontrolu (tzv. due diligence) a aby předložil řádné doklady o své totožnosti[10] a související informace před tím, než mu bude udělen přístup k internetovým platebním službám[11].

6.2 PPS by měli zajistit, aby předběžné informace[12] poskytované klientovi obsahovaly konkrétní podrobnosti týkající se internetových platebních služeb. Podle potřeby se jedná o následující informace:

- jasné informace o jakýchkoliv případných požadavcích týkajících se klientova technického vybavení, softwaru či jiných nezbytných nástrojů (např. antivirový software, firewally);
- pokyny pro řádné a bezpečné používání osobních přihlašovacích údajů;
- popis jednotlivých kroků procesu zadávání a schvalování platebních transakcí anebo získávání informací klientem, včetně důsledků každého provedeného úkonu;
- pokyny pro řádné a bezpečné používání veškerého hardwaru a softwaru poskytnutého klientovi;
- postupy, které je potřeba dodržovat v případě ztráty či krádeže osobních přihlašovacích údajů nebo klientova hardwaru či softwaru pro přihlášení do systému či provádění transakcí;
- postupy, které je potřeba dodržovat, pokud je odhaleno nebo existuje podezření na jakékoliv zneužití;
- popis příslušných odpovědností a závazků PPS a klienta, pokud jde o používání internetových platebních služeb.

---

hloubkovou kontrolu klienta a pro výjimku na základě finanční činnosti vykonávané příležitostně nebo ve velmi omezené míře. Úř. věst. L 214, 4. 8. 2006, s. 29-34.

[10] Například cestovní pas, občanský průkaz nebo zaručený elektronický podpis.

[11] Procesem zjišťování totožnosti klienta nejsou dotčeny žádné výjimky stanovené v platných právních předpisech proti praní peněz. PPS nemusí provádět samostatný proces ověření totožnosti klienta pro internetové platební služby za předpokladu, že takové ověření totožnosti klienta již bylo provedeno, např. pro účely jiných existujících služeb souvisejících s platbami nebo při založení účtu.

[12] Tyto informace doplňují článek 42 směrnice o platebních službách, v němž se upřesňují informace, které je PPS povinen poskytnout uživateli platebních služeb před uzavřením smlouvy o poskytování platebních služeb.

6.3 PPS by měli zajistit, aby bylo v rámcové smlouvě s klientem stanoveno, že PPS je oprávněn z bezpečnostních důvodů zablokovat konkrétní transakci nebo platební prostředek[13]. Ve smlouvě by také měl být určen způsob a podmínky informování klienta a také možnosti, jak se může klient spojit s PPS za účelem „odblokování“ internetové platební transakce či služby, a to v souladu se směrnicí o platebních službách.

[13] Viz článek 55 směrnice o platebních službách, který pojednává o limitech pro používání platebního prostředku.

## Silná autentizace klienta

7. Zahájení internetových plateb i přístup k citlivým platebním údajům je nutno chránit silnou autentizací klienta. PPS by měli mít zaveden postup silné autentizace klienta v souladu s definicí uvedenou v těchto obecných pokynech.

7.1 [Bezhotovostní převody / elektronické oprávnění / elektronické peníze] PPS by měli provádět silnou autentizaci klienta při autorizaci internetových platebních transakcí klientem (včetně bezhotovostních převodů s více příjemci) a vystavování či změny elektronických oprávnění k inkasu. PPS by však mohli zvážit přijetí alternativních opatření týkajících se autentizace klienta pro:

- odchozí platby důvěryhodným příjemcům uvedeným na předem stanovených bílých listinách pro takového klienta;
- transakce mezi dvěma účty stejného klienta vedenými u stejného PPS;
- převody v rámci stejného PPS odůvodněné na základě analýzy transakčního rizika;
- platby malých částek ve smyslu směrnice o platebních službách[14].

7.2 Získání přístupu k citlivým platebním údajům a případné změny těchto údajů (včetně vytváření a změn bílých listin) vyžaduje silnou autentizaci klienta. Pokud PPS nabízí výhradně poradenské služby, kdy nedochází k zobrazení citlivých klientských či platebních údajů, jako jsou např. údaje o platební kartě, které lze snadno zneužít pro spáchání podvodu, může PPS provést úpravu svých požadavků na autentizaci na základě svého hodnocení rizika.

7.3 [karty] V případě karetních transakcí by měli všichni PPS vydávající karty podporovat silnou autentizaci držitele karty. Všechny vystavené karty musí být technicky připraveny (aktivovány) pro používání společně se silnou autentizací.

7.4 [karty] PPS nabízející služby zúčtování karetních transakcí by měli podporovat technologie umožňující vydavateli provést silnou autentizaci držitele karty pro karetní platební systémy, jichž se daný zúčtovací subjekt účastní.

7.5 [karty] PPS nabízející služby zúčtování karetních transakcí by měli od svého internetového obchodníka vyžadovat, aby podporoval řešení umožňující vydavateli provést silnou autentizaci držitele karty pro účely karetních transakcí přes internet. Pro předem stanovené kategorie transakcí s nízkým rizikem, např. na základě analýzy transakčního rizika, anebo pro platby malých částek ve smyslu směrnice o platebních službách by bylo možné zvážit používání alternativních autentizačních metod.

[14] Viz definice platebních prostředků pro platby malých částek v čl. 34 odst. 1 a v čl. 53 odst. 1 směrnice o platebních službách.

7.6 [karty] Pro karetní platební systémy akceptované danou službou by poskytovatelé řešení pro elektronické peněženky měli vyžadovat po vydavateli silnou autentizaci v okamžiku, kdy oprávněný držitel karty poprvé registruje údaje o kartě.

7.7 Poskytovatelé řešení pro elektronické peněženky by měli podporovat silnou autentizaci klienta v okamžiku, kdy se klienti přihlašují k platebním službám elektronické peněženky nebo provádějí karetní transakce přes internet. Pro předem stanovené kategorie transakcí s nízkým rizikem, např. na základě analýzy transakčního rizika, anebo pro platby malých částek ve smyslu směrnice o platebních službách, by bylo možné zvážit používání alternativních autentizačních metod.

7.8 [karty] U virtuálních karet by měla počáteční registrace probíhat v bezpečném a důvěryhodném prostředí[15]. Silná autentizace klienta by měla být vyžadována pro účely postupu generování údajů o virtuální kartě, pokud je karta vydávána v prostředí internetu.

7.9 PPS by měli zajistit řádnou vzájemnou autentizaci při komunikaci s internetovými obchodníky za účelem zahájení internetových plateb a přístupu k citlivým platebním údajům.

## Registrace a poskytnutí autentizačních nástrojů anebo softwaru dodávaných klientům

8. PPS by měli zajistit, aby registrace klientů a počáteční poskytnutí autentizačních nástrojů nezbytných pro využívání internetové platební služby anebo dodání s platbami souvisejícího softwaru klientům probíhaly bezpečným způsobem.

8.1 Registrace a poskytnutí autentizačních nástrojů anebo s platbami souvisejícího softwaru dodávaného klientovi by měly splňovat následující požadavky.

- Příslušné postupy by se měly provádět v bezpečném a důvěryhodném prostředí, přičemž by měla být zohledněna potenciální rizika související se zařízeními, která nejsou pod kontrolou daného PPS.

- Měly by být zavedeny účinné a bezpečné postupy pro doručení osobních přihlašovacích údajů, s platbami souvisejícího softwaru a veškerých personalizovaných zařízení souvisejících s internetovými platbami. Software dodávaný po internetu by rovněž měl být daným PPS digitálně podepsán, aby si mohl klient ověřit, že je software pravý a že do něj nebylo nijak zasahováno.

[15] Mezi prostředí, za která nese PPS odpovědnost a kde je zajištěna odpovídající autentizace klienta a PPS nabízejícího danou službu a rovněž ochrana důvěrných či citlivých informací, patří: i) provozovny PPS; ii) internetové bankovnictví či jiná bezpečná webová stránka, např. kde ŘO nabízí srovnatelné bezpečnostní prvky, které jsou mimo jiné uvedeny v pokynu č. 4; nebo iii) služby bankomatů (ATM). (V případě bankomatů je vyžadována silná autentizace klienta. Tuto autentizaci obvykle zajišťuje čip a PIN, nebo čip a biometrické prvky.)

- [karty] U karetních transakcí by měl mít klient možnost aktivovat silnou autentizaci nezávisle na konkrétním internetovém nákupu. Je-li během on-line nakupování nabídnuta aktivace, měla by být provedena přesměrováním klienta do bezpečného a důvěryhodného prostředí.

8.2 [karty] Vydavatelé by měli aktivně podporovat registraci držitelů karet k silné autentizaci a umožnit svým držitelům karet obejít registraci pouze ve výjimečném a omezeném počtu případů, kdy je to odůvodněno rizikem souvisejícím s konkrétní karetní transakcí.

## Pokusy o přihlášení, uplynutí platnosti relace, platnost autentizace

9. PPS by měli omezit počet pokusů o přihlášení nebo o autentizaci, určit pravidla pro uplynutí platnosti relace u internetových platebních služeb a nastavit časové limity pro platnost autentizace.

9.1 Při používání jednorázového hesla pro účely ověření by PPS měli zajistit, aby byla platnost těchto hesel omezena na nezbytně nutnou minimální dobu.

9.2 PPS by měli stanovit maximální počet neúspěšných pokusů o přihlášení nebo o autentizaci, po kterém bude přístup k internetové platební službě zablokován (dočasně či trvale). PPS by měli mít zaveden bezpečný postup pro opětovnou aktivaci zablokovaných internetových platebních služeb.

9.3 PPS by měli stanovit maximální lhůtu, po jejímž uplynutí budou neaktivní relace internetových platebních služeb automaticky ukončeny.

## Sledování transakcí

10. Před konečným schválením ze strany PPS by měly být zprovozněny mechanismy sledování transakcí, jejichž úkolem je předcházet podvodným platebním transakcím, odhalovat je a blokovat, přičemž podezřelé či vysoce rizikové transakce by měly podléhat zvláštnímu postupu prověření a hodnocení. Stejné bezpečnostní sledovací a schvalovací mechanismy by rovněž měly být zavedeny pro vydávání elektronických oprávnění.

10.1 PPS by měli používat systémy pro odhalování a prevenci podvodů, aby zjistili podezřelé transakce ještě dříve, než PPS provede konečné schválení transakcí či elektronických oprávnění. Tyto systémy by měly být založeny například na parametrizovaných pravidlech (jako jsou např. černé listiny napadených či odcizených karetních údajů) a měly by sledovat nestandardní chování klienta nebo jeho přístupového zařízení (jako je např. změna adresy internetového protokolu (IP)[16] nebo rozpětí IP během relace

[16] IP adresa je jedinečný číselný kód označující každý počítač připojený k internetu.

internetových platebních služeb, někdy zjišťované geolokačními kontrolami IP[17], nestandardní kategorie elektronických obchodníků u konkrétního klienta nebo nestandardní transakční údaje apod.). Tyto systémy by rovněž měly být schopny odhalit známky infekce dané relace škodlivými programy, tzv. malware, (např. ověřením, zda se jedná o skript namísto ověření člověkem) a známé scénáře podvodného jednání. Rozsah, složitost a přizpůsobivost sledovacích řešení by měly být, při dodržování platných právních předpisů na ochranu údajů, úměrné výsledku hodnocení rizika.

10.2 PPS zajišťující zúčtování karetních transakcí by měli mít zavedeny systémy na odhalování a prevenci podvodů, které by sledovaly aktivity internetových obchodníků.

10.3 PPS by měli provádět veškeré postupy prověření a hodnocení v přiměřené lhůtě, aby nedocházelo ke zbytečnému prodlení v zahájení anebo provedení dotčené platební služby.

10.4 Pokud se PPS na základě své politiky řízení rizika rozhodne zablokovat určitou platební transakci, která byla označena za potenciálně podvodnou, měla by tato blokace trvat co možná nejkratší dobu, dokud nebudou bezpečnostní otázky vyřešeny.

## Ochrana citlivých platebních údajů

11. Během uchovávání, zpracovávání a přenosu citlivých platebních údajů by měla být zajištěna jejich ochrana.

11.1 Veškeré údaje používané ke zjištění totožnosti a autentizaci klientů (např. při přihlašování do systému, při zahájení internetových plateb a při vydávání, změnách či rušení elektronických oprávnění) včetně klientského rozhraní (webová stránka PPS nebo internetového obchodníka) by měly být řádně zabezpečeny proti krádeži a neoprávněnému přístupu či změnám.

11.2 PPS by měli zajistit, aby při výměně citlivých platebních údajů přes internet používaly komunikující strany během celé příslušné komunikační relace bezpečné mezikoncové šifrování[18], aby byla ochráněna důvěrnost a integrita těchto údajů, a to pomocí účinných a všeobecně uznávaných šifrovacích metod.

11.3 PPS nabízející služby zúčtování karetních transakcí by měli svým internetovým obchodníkům doporučit, aby neuchovávali žádné citlivé platební údaje. V případě, kdy internetoví obchodníci nakládají s citlivými platebními údaji (tj. tyto údaje uchovávají,

[17] Kontrola „Geo-IP“ ověřuje, zda vydávající (vystavující) země odpovídá IP adrese, z níž uživatel zahajuje danou transakci.

[18] Mezikoncové šifrování (end-to-end encryption) představuje šifrování uvnitř nebo na úrovni zdrojového koncového systému, kdy k příslušnému dešifrování dochází pouze uvnitř nebo na úrovni cílového koncového systému. ETSI EN 302 109 V1.1.1. (2003-06).

zpracovávají či přenášejí), měli by tito PPS od internetových obchodníků smluvně vyžadovat, aby měli zavedena nezbytná opatření na ochranu těchto údajů. PPS by měli provádět pravidelné kontroly, a jestliže PPS zjistí, že některý internetový obchodník nakládající s citlivými platebními údaji nemá zavedena požadovaná bezpečnostní opatření, měl by PPS podniknout kroky k vymáhání plnění této smluvní povinnosti nebo smlouvu vypovědět.

## Informovanost a vzdělávání klientů a komunikace

### Vzdělávání klientů a komunikace

12. PPS by měli klientům v případě potřeby poskytovat pomoc a pokyny ohledně bezpečného používání internetových platebních služeb. PPS by měli se svými klienty komunikovat takovým způsobem, aby je ujistili o pravosti obdržených zpráv.

12.1 PPS by měli zajistit alespoň jeden zabezpečený kanál[19] pro nepřetržitou komunikaci s klienty ohledně správného a bezpečného používání internetové platební služby. PPS by měli klienty o tomto kanálu informovat a vysvětlit jim, že jakákoliv zpráva jménem PPS, která je doručena jakýmikoliv jinými prostředky, např. prostřednictvím e-mailu, a která se týká správného a bezpečného používání internetové platební služby, není důvěryhodná. PPS by měl vysvětlit:

- postup, jaký mají klienti použít, pokud chtějí PPS informovat o (domnělých) podvodných platbách, podezřelých incidentech či anomáliích během relace internetových platebních služeb anebo o případných pokusech o sociální inženýrství[20];
- následné kroky, tj. jakým způsobem PPS odpoví klientovi;
- jakým způsobem PPS informuje klienta o (případných) podvodných transakcích nebo jejich nezahájení, nebo jak upozorní klienta na případné útoky (např. phishingové e-maily).

12.2 Prostřednictvím zabezpečeného kanálu by PPS měli klienty informovat o aktualizacích bezpečnostních postupů týkajících se internetových platebních služeb. Veškerá upozornění na významná nově vznikající rizika (např. varování týkající se sociálního inženýrství) by rovněž měla být doručována prostřednictvím zabezpečeného kanálu.

12.3 PPS by měli být připraveni klientům pomoci s veškerými jejich dotazy, stížnostmi, žádostmi o podporu a upozorněními na případné anomálie a incidenty týkající se internetových plateb a souvisejících služeb, přičemž klienti by měli být vhodně informováni o tom, jak tuto pomoc získat.

12.4 PPS by měli zahájit programy vzdělávání a informovanosti klientů, aby zajistili, že klienti přinejmenším chápou potřebu:

- chránit svá hesla, bezpečnostní klíče (tokeny), osobní údaje a další důvěrné informace;

[19] Např. vyhrazenou poštovní schránku na webových stránkách PPS nebo zabezpečenou webovou stránku.

[20] Sociálním inženýrstvím se v této souvislosti rozumí způsob manipulace lidí za účelem získání informací (např. prostřednictvím e-mailu nebo telefonických hovorů), nebo vyhledávání informací ze sociálních sítí za účelem podvodu nebo získání neoprávněného přístupu k určitému počítači nebo do určité sítě.

- řádně zajistit bezpečnost svého osobního zařízení (např. počítače) provedením instalací a aktualizací bezpečnostních prvků (antivirový program, firewally, bezpečnostní opravy, tzv. záplaty);

- zvážit významné hrozby a rizika související se stahováním softwaru z internetu, pokud nemá klient oprávněnou jistotu, že je software pravý a že do něj nebylo zasahováno;

- používat pravé webové stránky PPS pro internetové platby.

12.5 PPS zajišťující zúčtování karetních transakcí by měli od internetových obchodníků požadovat, aby zřetelně oddělili postupy spojené s platbami od on-line obchodu, aby mohli klienti snadněji rozeznat, kdy komunikují s PPS a nikoli s příjemcem platby (např. přesměrováním klienta a otevřením samostatného okna tak, aby se daný platební postup nezobrazoval v prostředí stránky internetového obchodníka).

### Oznámení, stanovení limitů

13. PPS by měli stanovit limity pro internetové platební služby a mohli by svým klientům nabídnout možnosti dalšího omezení rizika v rámci těchto limitů. Mohli by rovněž poskytovat služby zasílání upozornění a správy klientského profilu.

13.1 PPS by měli před poskytnutím internetových platebních služeb klientovi stanovit limity[21] vztahující se na tyto služby (např. maximální částka pro každou jednotlivou platbu nebo kumulativní částka za určité období) a měli by o nich své klienty příslušně informovat. PPS by měli klientům umožnit deaktivovat funkci internetových plateb.

### Přístup klientů k informacím o stavu zahájení a provedení platby

14. PPS by měli svým klientům potvrdit zahájení platby a včas jim poskytnout informace nezbytné k tomu, aby si klienti mohli ověřit, zda byla platební transakce správně zahájena anebo provedena.

14.1 [Bezhotovostní převody / elektronické oprávnění] PPS by měli klientům poskytnout nástroj fungující téměř v reálném čase, který umožňuje kdykoli[22] provést kontrolu stavu provádění transakcí a zůstatků na účtech v bezpečném a důvěryhodném prostředí.

14.2 Veškeré podrobné elektronické výpisy by měly být zpřístupněny v bezpečném a důvěryhodném prostředí. Pokud PPS informuje klienty o dostupnosti elektronických výpisů (např. pravidelně s vydáním pravidelného elektronického výpisu nebo ad hoc po

[21] Tyto limity lze uplatňovat buď všeobecně (tj. na všechny platební prostředky umožňující provádění internetových plateb) nebo individuálně.

[22] S výjimkou výjimečné nedostupnosti daného prostředku z důvodu technické údržby nebo v důsledku závažných incidentů.

provedení konkrétní transakce) prostřednictvím alternativního kanálu, např. formou SMS, e-mailu či dopisu, neměla by taková sdělení obsahovat citlivé platební údaje s tím, že pokud je obsahovat budou, měly by být tyto údaje zamaskovány.

## Hlava III – Závěrečná ustanovení a provádění

15. Tyto obecné pokyny se použijí ode dne 01.08.2015.

# Příloha č. 1 Příklady osvědčených postupů

Kromě výše stanovených požadavků popisují tyto obecné pokyny některé osvědčené postupy určené PPS a příslušným účastníkům trhu, jejichž dodržování se nevyžaduje, nýbrž pouze doporučuje. Pro snadnější orientaci jsou výslovně uvedeny kapitoly, jichž se tyto osvědčené postupy týkají.

## Celkové kontrolní a bezpečnostní prostředí

### Řízení

OP 1: Bezpečnostní politika by mohla být zpracována ve formě samostatného dokumentu.

### Řízení a snižování rizika

OP 2: PPS by mohli zajišťovat bezpečnostní nástroje (např. zařízení anebo upravené prohlížeče, řádně zabezpečené) k ochraně klientského rozhraní před nezákonným zneužitím či útoky (např. útoky typu „man in the browser").

### Sledovatelnost

OP 3: PPS nabízející služby zúčtování karetních transakcí by mohli smluvně vyžadovat od internetových obchodníků, kteří uchovávají platební informace, aby měli zavedeny vhodné postupy k zajištění sledovatelnosti.

## Konkrétní kontrolní a bezpečnostní opatření pro internetové platby

### Prvotní ověření totožnosti klienta, informace

OP 4: Klient by mohl spíše uzavřít samostatnou smlouvu o poskytování služeb zaměřenou na provádění internetových platebních transakcí, než aby byly podmínky těchto transakcí zahrnuty do širší všeobecné smlouvy o poskytování služeb uzavřené s PPS.

OP 5: PPS by rovněž mohli zajistit, aby byly klientům průběžně, nebo případně ad hoc, předávány vhodnými prostředky (např. letáky, webové stránky) jasné a srozumitelné pokyny vysvětlující jejich povinnosti ohledně bezpečného používání příslušné služby.

### Silná autentizace klienta

OP 6: [karty] Internetoví obchodníci by mohli podpořit silnou autentizaci držitele karty prováděné vydavatelem při karetních transakcích přes internet.

OP 7: Pro účely pohodlí klienta by PPS mohli zvážit používání jediného nástroje pro silnou autentizaci klienta u všech internetových platebních služeb. To by mohlo vést k přijetí daného řešení klienty ve větší míře a rovněž k usnadnění správného používání.

OP 8: Silná autentizace klienta by mohla zahrnovat prvky spojující autentizaci s konkrétní částkou a příjemcem platby. To by mohlo u klientů zvýšit jistotu při schvalování plateb.

Technologické řešení umožňující propojení údajů silné autentizace a údajů o transakci by mělo být odolné vůči případným neoprávněným zásahům.

### Ochrana citlivých platebních údajů

OP 9: Je žádoucí, aby internetoví obchodníci nakládající s citlivými platebními údaji řádně vyškolili své pracovníky odpovědné za řízení rizika podvodů a aby obsah tohoto školení pravidelně aktualizovali v souladu s dynamickým rozvojem v oblasti bezpečnostních otázek.

### Vzdělávání klientů a komunikace

OP 10: Je žádoucí, aby PPS nabízející služby zúčtování karetních transakcí zajistili pro své internetové obchodníky vzdělávací programy v oblasti prevence podvodného jednání.

### Oznámení, stanovení limitů

OP 11: V rámci stanovených limitů by PPS mohli poskytnout svým klientům nástroj pro správu limitů internetových platebních služeb v bezpečném a důvěryhodném prostředí.

OP 12: PPS by mohli klientům zasílat upozornění, např. telefonicky nebo prostřednictvím SMS, na podezřelé či vysoce rizikové platební transakce na základě svých politik řízení rizika.

OP 13: PPS by mohli klientům nabídnout možnost stanovit všeobecná, personalizovaná pravidla jako parametry jejich chování ve spojitosti s internetovými platbami a souvisejícími službami, např. že platby zahájí pouze z určitých konkrétních zemí, přičemž platby zahájené z jiné lokality budou blokovány, nebo že mohou konkrétní příjemce plateb uvést na bílou či černou listinu.