NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2018/389

ze dne 27. listopadu 2017,

kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES ([1]), a zejména na čl. 98 odst. 4 druhý pododstavec uvedené směrnice,

vzhledem k těmto důvodům:

(1) Platební služby nabízené elektronicky by měly být prováděny bezpečným způsobem, za použití technologií, které jsou schopny zaručit bezpečné ověření uživatele a v maximální možné míře snížit riziko podvodu. Postup ověření by měl obecně zahrnovat mechanismy sledování transakcí k odhalení pokusů o použití osobních bezpečnostních údajů uživatele platebních služeb, které byly ztraceny, odcizeny nebo zneužity, a měl by rovněž zajistit, aby byl uživatel platebních služeb oprávněným uživatelem, který tudíž udělil souhlas s převodem peněžních prostředků a s přístupem k informacím o jeho účtu prostřednictvím běžného použití osobních bezpečnostních údajů. Mimoto je nutné stanovit požadavky na silné ověření klienta, které by se měly uplatnit pokaždé, když plátce využívá on-line přístupu ke svému platebnímu účtu, iniciuje elektronickou platební transakci nebo prostřednictvím prostředků komunikace na dálku provede jakýkoli úkon, který by mohl vést k riziku platebního podvodu či jiných zneužití, tudíž je nutné vyžadovat vytvoření ověřovacího kódu, který by měl být odolný vůči riziku zfalšování v celém rozsahu nebo v důsledku poskytnutí jakýchkoli prvků, na jejichž základě byl kód vytvořen.

(2) Jelikož se způsoby podvodů neustále vyvíjejí, měly by požadavky na silné ověření klienta umožnit inovace technických řešení, která se zabývají vznikem nových hrozeb pro bezpečnost elektronických plateb. Aby bylo zajištěno, že stanovené požadavky jsou uplatňovány účinně a trvale, je rovněž vhodné požadovat, aby byla bezpečnostní opatření pro uplatnění silného ověření klienta a příslušné výjimky, opatření na ochranu důvěrnosti a integrity osobních bezpečnostních údajů a opatření, která stanoví společné a bezpečné otevřené standardy komunikace, zdokumentována, pravidelně testována, hodnocena a kontrolována auditory, kteří mají odborné znalosti v oblasti bezpečnosti informačních technologií a plateb a jsou funkčně nezávislí. Aby mohly příslušné orgány sledovat kvalitu přezkumu těchto opatření, měly by jim být tyto přezkumy zpřístupněny na žádost.

(3) Jelikož u elektronických platebních transakcí na dálku existuje vyšší riziko podvodu, je nutné zavést u těchto transakcí dodatečné požadavky na silné ověření klienta, které zajišťují, že prvky dynamicky propojují transakci s částkou a příjemcem určeným plátcem při iniciování transakce.

(4) Dynamické propojení je umožněno vytvářením ověřovacích kódů, které podléhá souboru přísných bezpečnostních požadavků. Aby byla zajištěna neutralita z hlediska technologií, neměla by se pro uplatňování ověřovacích kódů vyžadovat konkrétní technologie. Ověřovací kódy by proto měly být založeny na řešeních, jako je vytváření a potvrzování jednorázových hesel, digitální podpisy či jiná kryptograficky podložená potvrzení platnosti pomocí klíčů či kryptografických materiálů uložených v ověřovacích prvcích, jsou-li splněny bezpečnostní požadavky.

([1]) Úř. věst. L 337, 23.12.2015, s. 35.

(5) Je nutné stanovit zvláštní požadavky vztahující se na situaci, kdy v okamžiku iniciování elektronické platební transakce na dálku plátcem není známa konečná částka, aby bylo zajištěno, že se silné ověření klienta týká maximální částky, s ohledem na niž udělil plátce souhlas, jak je uvedeno ve směrnici (EU) 2015/2366.

(6) Aby bylo zajištěno uplatňování silného ověření klienta, je rovněž nutné vyžadovat odpovídající bezpečnostní charakteristiky u prvků silného ověření klienta z kategorie znalost (to, co ví pouze uživatel), jako je délka nebo složitost, u prvků z kategorie držení (to, co drží pouze uživatel), jako jsou specifikace algoritmu, délka klíče a informační entropie, a u zařízení a softwaru, který čte prvky z kategorie inherence (to, čím uživatel je), jako jsou specifikace algoritmu, biometrické čidlo a ochranné prvky vzoru, zejména k zmírnění rizika odhalení těchto prvků, jejich poskytnutí neoprávněným stranám a použití těmito stranami. Je rovněž nutné stanovit požadavky, které zajišťují, aby byly tyto prvky nezávislé, takže nesplněním jednoho z nich není ovlivněna spolehlivost ostatních, zejména v případě, používá-li tyto prvky víceúčelové zařízení, například zařízení jako tablet nebo mobilní telefon, jež lze použít jak pro vydání pokynu k platbě, tak i při ověřování.

(7) Požadavky na silné ověření klienta se vztahují na platby iniciované plátcem bez ohledu na to, zda je plátcem fyzická nebo právnická osoba.

(8) Na platby provedené s použitím anonymních platebních prostředků se vzhledem k jejich povaze povinnost týkající se silného ověření klienta nevztahuje. Je-li anonymita těchto prostředků ze smluvních či legislativních důvodů zrušena, vztahují se na platby bezpečnostní požadavky, které vyplývají ze směrnice (EU) 2015/2366 a této regulační technické normy.

(9) V souladu se směrnicí (EU) 2015/2366 jsou výjimky ze zásady silného ověření klienta stanoveny podle míry rizika, částky, opakování a způsobu platby použitého k provedení platební transakce.

(10) Úkony, které zahrnují přístup k zůstatku a posledním transakcím na platebním účtu bez zveřejnění citlivých údajů o platbách, opakující se platby pro stejné příjemce, které plátce zavedl dříve nebo potvrdil pomocí silného ověření klienta, a platby pro stejnou fyzickou či právnickou osobu nebo od této osoby s účty u téhož poskytovatele platebních služeb představují nízkou míru rizika, a poskytovatelé platebních služeb proto nemusí uplatňovat silné ověření klienta. Vedle toho ovšem platí, že podle článků 65, 66 a 67 směrnice (EU) 2015/2366 by si poskytovatelé služeb iniciování platby, poskytovatelé platebních služeb vydávající karetní platební prostředky a poskytovatelé služeb informování o účtu měli od poskytovatele platebních služeb, který vede účet, vyžádat a získat pouze nezbytné a podstatné informace pro poskytnutí dané platební služby se souhlasem uživatele platebních služeb. Tento souhlas lze udělit jednotlivě pro každou žádost o informace nebo pro každou platbu, která má být iniciována, či v případě poskytovatelů služeb informování o účtu jako pověření pro určené platební účty a související platební transakce stanovené ve smluvní dohodě s uživatelem platebních služeb.

(11) Výjimky pro bezkontaktní platby malých částek v místě prodeje, které zohledňují rovněž maximální počet po sobě následujících transakcí nebo určitou stanovenou maximální hodnotu po sobě následujících transakcí bez použití silného ověření klienta, umožňují rozvoj uživatelsky přívětivých platebních služeb s nízkým rizikem, a proto by měly být povoleny. Je rovněž vhodné stanovit výjimku v případě elektronických platebních transakcí iniciovaných u terminálu bez obsluhy, kdy použití silného ověření klienta nemusí být vždy snadné z provozních důvodů (např. aby se zabránilo frontám a případným nehodám u mýtných bran či jiným bezpečnostním rizikům).

(12) Podobně jako u výjimky pro bezkontaktní platby malých částek v místě prodeje je nutno usilovat o náležitou rovnováhu mezi úsilím o vyšší bezpečnost u plateb na dálku a potřebami týkajícími se uživatelské přívětivosti a dostupnosti plateb v oblasti elektronického obchodu. V souladu s těmito zásadami by měly být prahové hodnoty, pod jejichž úrovní není nutné použít silné ověření klienta, stanoveny obezřetně tak, aby se vztahovaly pouze na on-line nákupy s malými částkami. Prahové hodnoty pro on-line nákupy by měly být stanoveny obezřetněji, jelikož skutečnost, že dotyčná osoba není při provádění nákupu fyzicky přítomna, představuje mírně vyšší bezpečnostní riziko.

(13) Požadavky na silné ověření klienta se vztahují na platby iniciované plátcem bez ohledu na to, zda je plátcem fyzická nebo právnická osoba. Mnoho plateb společností je iniciováno prostřednictvím zvláštních postupů nebo protokolů, které zaručují vysokou úroveň bezpečnosti plateb, o kterou směrnice (EU) 2015/2366 usiluje prostřednictvím silného ověření klienta. Pokud příslušné orgány zjistí, že tyto platební procesy a protokoly, jež jsou zpřístupněny pouze plátcům, kteří nejsou spotřebiteli, dosahují cílů směrnice (EU) 2015/2366, pokud jde o bezpečnost, mohou být poskytovatelé platebních služeb ve vztahu k těmto procesům nebo protokolům osvobozeni od požadavků na silné ověření klienta.

(14) V případě analýzy transakčních rizik v reálném čase, která klasifikuje platební transakci jako transakci s nízkým rizikem, je rovněž vhodné zavést výjimku pro poskytovatele platebních služeb, který hodlá neuplatňovat silné ověření klienta, a to přijetím účinných požadavků založených na rizicích, které zajišťují bezpečnost peněžních prostředků a osobních údajů uživatele platebních služeb. Tyto požadavky založené na rizicích by měly spojovat výsledky analýzy rizik potvrzující, že nebyly zjištěny mimořádné výdaje nebo vzorec chování plátce, přičemž se přihlíží k ostatním rizikovým faktorům, včetně informací o místě plátce a příjemce s peněžními prahovými hodnotami, které vycházejí z míry podvodů vypočítané pro platby na dálku. Nelze-li na základě analýzy transakčních rizik v reálném čase považovat určitou platbu za platbu s nízkou úrovní rizika, měl by se poskytovatel platebních služeb vrátit k silnému ověření klienta. Maximální hodnota této výjimky založené na rizicích by měla být stanovena způsobem, který zajišťuje velmi nízkou odpovídající míru podvodů, a to rovněž porovnáním míry podvodů u všech platebních transakcí daného poskytovatele platebních služeb, včetně transakcí ověřených prostřednictvím silného ověření klienta, klouzavě za určité časové období.

(15) K zajištění účinného prosazování by měli poskytovatelé platebních služeb, kteří chtějí využít výjimky z požadavku na silné ověření klienta, u každého druhu platebních transakcí pravidelně sledovat a na žádost zpřístupňovat příslušným orgánům a Evropskému orgánu pro bankovnictví (EBA) hodnotu podvodných nebo neautorizovaných platebních transakcí a zjištěné míry podvodů u všech svých platebních transakcí bez ohledu na to, zda byly ověřeny prostřednictvím silného ověření klienta, nebo provedeny na základě příslušné výjimky.

(16) Shromažďování těchto nových historických údajů o mírách podvodů u elektronických platebních transakcí přispěje rovněž k účinnému přezkumu prahových hodnot pro výjimku z požadavku na silné ověření klienta na základě analýzy transakčních rizik v reálném čase ze strany orgánu EBA. Orgán EBA by měl tyto regulační technické normy přezkoumávat a v případě potřeby předložit Komisi jejich aktualizace s uvedením nových navrhovaných prahových hodnot a odpovídající míry podvodů k zvýšení bezpečnosti elektronických plateb na dálku v souladu s čl. 98 odst. 5 směrnice (EU) 2015/2366 a s článkem 10 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([1]).

(17) Poskytovatelé platebních služeb, kteří využívají některou ze stanovených výjimek, by měli mít kdykoli možnost rozhodnout se pro uplatňování silného ověření klienta u úkonů a platebních transakcí uvedených ve zmíněných ustanoveních.

(18) Opatření, která chrání důvěrnost a integritu osobních bezpečnostních údajů, a zařízení a software pro ověřování by měly snížit rizika související s podvody prostřednictvím neautorizovaného či podvodného použití platebních prostředků a neoprávněného přístupu k platebním účtům. Za tímto účelem je nutné zavést požadavky na bezpečné vytváření a předávání osobních bezpečnostních údajů a jejich přiřazení k uživateli platebních služeb a stanovit podmínky pro obnovu a deaktivaci těchto údajů.

(19) K zajištění účinné a bezpečné komunikace mezi příslušnými subjekty v rámci služeb informování o účtu, služeb iniciování platby a potvrzení disponibility peněžních prostředků je nutné stanovit požadavky na společné a bezpečné otevřené standardy komunikace, které dodržují všichni příslušní poskytovatelé platebních služeb. Směrnice (EU) 2015/2366 umožňuje poskytovatelům služeb informování o účtu přístup k informacím o platebním účtu a využívání těchto informací. Toto nařízení proto nemění pravidla přístupu k jiným účtům, než jsou platební účty.

([1]) 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 (Úř. věst. L 331, 15.12.2010, s. 12).

(20) Každý poskytovatel platebních služeb, který vede účet, s platebními účty, jež jsou přístupné on-line, by měl nabízet přinejmenším jedno rozhraní pro přístup umožňující bezpečnou komunikaci s poskytovateli služeb informování o účtu, poskytovateli služeb iniciování platby a poskytovateli platebních služeb vydávajícími karetní platební prostředky. Rozhraní by mělo poskytovatelům služeb informování o účtu, poskytovatelům služeb iniciování platby a poskytovatelům platebních služeb vydávajícím karetní platební prostředky umožnit identifikaci u poskytovatele platebních služeb, který vede účet. Rozhraní by mělo poskytovatelům služeb informování o účtu a poskytovatelům služeb iniciování platby umožnit rovněž využívat postupy ověření stanovené poskytovatelem platebních služeb, který vede účet, pro uživatele platebních služeb. K zajištění neutrality obchodních modelů a technologií by poskytovatelé platebních služeb, kteří vedou účet, měli mít možnost rozhodnout, zda nabídnou rozhraní, jež je vyhrazeno pro komunikaci s poskytovateli služeb informování o účtu, poskytovateli služeb iniciování platby a poskytovateli platebních služeb vydávajícími karetní platební prostředky, nebo povolit za účelem této komunikace použití rozhraní pro identifikaci uživatelů platebních služeb poskytovatelů platebních služeb, kteří vedou účet, a komunikaci s nimi.

(21) Aby mohli poskytovatelé služeb informování o účtu, poskytovatelé služeb iniciování platby a poskytovatelé platebních služeb vydávající karetní platební prostředky vyvinout příslušná technická řešení, měla by být náležitě zdokumentována a zveřejněna technická specifikace rozhraní. Poskytovatel platebních služeb, který vede účet, by měl mimoto nabídnout zařízení, které poskytovatelům platebních služeb umožňuje technická řešení otestovat, a to nejméně šest měsíců přede dnem použitelnosti těchto regulačních norem, nebo přede dnem, k němuž bude rozhraní uvedeno na trh, dojde-li k uvedení po dni použitelnosti těchto norem. K zajištění interoperability různých technologických řešení komunikace by rozhraní mělo používat standardy komunikace, které vyvinuly mezinárodní nebo evropské normalizační organizace.

(22) Kvalita služeb poskytovaných poskytovateli služeb informování o účtu a poskytovateli služeb iniciování platby bude záviset na řádném fungování rozhraní, která byla zavedena či upravena poskytovateli platebních služeb, kteří vedou účet. Je proto důležité, aby v případě, že tato rozhraní nevyhovují ustanovením obsaženým v těchto normách, byla přijata opatření, která zaručují kontinuitu činnosti ve prospěch uživatelů těchto služeb. Příslušné vnitrostátní orgány odpovídají za zajištění toho, že poskytovatelům služeb informování o účtu a poskytovatelům služeb iniciování platby není znemožněno poskytování služeb ani jim v něm není bráněno.

(23) Je-li přístup k platebním účtům umožněn prostřednictvím vyhrazeného rozhraní, je nutné k zajištění práva uživatelů platebních služeb využívat poskytovatele služeb iniciování platby a služby umožňující přístup k informacím o účtu, jak je stanoveno ve směrnici (EU) 2015/2366, vyžadovat, aby byla u vyhrazených rozhraní zajištěna stejná úroveň dostupnosti a výkonu jako u rozhraní, které má k dispozici uživatel platebních služeb. Poskytovatelé platebních služeb, kteří vedou účet, by měli stanovit rovněž transparentní klíčové ukazatele výkonnosti a cíle týkající se úrovně služeb s ohledem na dostupnost a výkon vyhrazených rozhraní, jež jsou přinejmenším stejně přísné jako v případě rozhraní používaného u uživatelů platebních služeb. Tato rozhraní by měla být otestována poskytovateli platebních služeb, kteří je budou používat, a podrobena zátěžovým testům a sledována příslušnými orgány.

(24) Aby bylo zajištěno, že poskytovatelé platebních služeb, kteří využívají vyhrazené rozhraní, mohou v případě problémů s dostupností či nepřiměřeného výkonu i nadále poskytovat své služby, je nutno poskytnout s výhradou přísných podmínek záložní mechanismus, který těmto poskytovatelům umožní používat rozhraní, jež poskytovatel platebních služeb, který vede účet, udržuje pro identifikaci svých vlastních uživatelů platebních služeb a pro komunikaci s nimi. Někteří poskytovatelé platebních služeb, kteří vedou účet, budou od povinnosti poskytnout takovýto záložní mechanismus prostřednictvím uživatelských rozhraní osvobozeni, pokud jejich příslušné orgány zjistí, že vyhrazená rozhraní splňují zvláštní podmínky, jež zajišťují nenarušenou hospodářskou soutěž. Pokud vyňatá vyhrazená rozhraní nesplňují požadované podmínky, dotčené příslušné orgány udělené výjimky zruší.

(25) Aby mohly příslušné orgány účinně dohlížet na uplatňování a řízení komunikačních rozhraní a sledovat je, měli by poskytovatelé platebních služeb, kteří vedou účet, zpřístupnit na svých internetových stránkách shrnutí příslušné dokumentace a na žádost poskytnout příslušným orgánům dokumentaci týkající se řešení v případě mimořádných událostí. Poskytovatelé platebních služeb, kteří vedou účet, by měli zveřejnit rovněž statistické údaje o dostupnosti a výkonu tohoto rozhraní.

(26) Aby byla zaručena důvěrnost a integrita údajů, je nutné zajistit bezpečnost komunikačních spojení mezi poskytovateli platebních služeb, kteří vedou účet, poskytovateli služeb informování o účtu, poskytovateli služeb iniciování platby a poskytovateli platebních služeb vydávajícími karetní platební prostředky. Zejména je třeba vyžadovat, aby

se mezi poskytovateli služeb informování o účtu, poskytovateli služeb iniciování platby, poskytovateli platebních služeb vydávajícími karetní platební prostředky a poskytovateli platebních služeb, kteří vedou účet, používalo při výměně údajů bezpečné šifrování.

(27) K zvýšení důvěry uživatelů a zajištění silného ověření klienta by se mělo uvážit použití prostředků pro elektronickou identifikaci a služeb vytvářejících důvěru, jak je stanoveno v nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([1]), zejména co se týká oznámených systémů elektronické identifikace.

(28) Za účelem sladění dat použitelnosti by mělo být toto nařízení použitelné od stejného dne, k němuž musí členské státy zajistit uplatňování bezpečnostních opatření uvedených v článcích 65, 66, 67 a 97 směrnice (EU) 2015/2366.

(29) Toto nařízení vychází z návrhů regulačních technických norem, které Komisi předložil Evropský orgán pro bankovnictví (EBA).

(30) K návrhu regulačních technických norem, z nichž toto nařízení vychází, uskutečnil orgán EBA otevřené a transparentní veřejné konzultace, analyzoval potenciální související náklady a přínosy a požádal o stanovisko skupinu subjektů působících v bankovnictví zřízenou podle článku 37 nařízení (EU) č. 1093/2010,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

Toto nařízení stanoví požadavky, jež musí splňovat poskytovatelé platebních služeb za účelem provádění bezpečnostních opatření, která jim umožňují:

a) uplatňovat postup silného ověření klienta v souladu s článkem 97 směrnice (EU) 2015/2366;

b) použít výjimky z uplatňování bezpečnostních požadavků na silné ověření klienta s výhradou stanovených omezených podmínek založených na míře rizika, částce a opakování platební transakce a způsobu platby použitém k jejímu provedení;

c) chránit důvěrnost a integritu osobních bezpečnostních údajů uživatelů platebních služeb;

d) stanovit společné a bezpečné otevřené standardy komunikace mezi poskytovateli platebních služeb, kteří vedou účet, poskytovateli služeb iniciování platby, poskytovateli služeb informování o účtu, plátci, příjemci a dalšími poskytovateli platebních služeb v souvislosti s poskytováním a používáním platebních služeb podle hlavy IV směrnice (EU) 2015/2366.

Článek 2

Obecné požadavky na ověření

1. Za účelem uplatňování bezpečnostních opatření uvedených v čl. 1 písm. a) a b) zavedou poskytovatelé platebních služeb mechanismy sledování transakcí, které jim umožňují odhalit neautorizované nebo podvodné platební transakce.

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 53).

Tyto mechanismy jsou založeny na analýze platebních transakcí, přičemž se zohlední prvky, jež jsou typické pro uživatele platebních služeb v případě běžného použití osobních bezpečnostních údajů.

2. Poskytovatelé platebních služeb zajistí, aby mechanismy sledování transakcí zohledňovaly minimálně všechny tyto rizikové faktory:

a) seznamy vyzrazených nebo odcizených ověřovacích prvků;

b) částku každé platební transakce;

c) známé scénáře podvodů při poskytování platebních služeb;

d) známky napadení malwarem při spojení v rámci postupu ověření;

e) v případě, že poskytovatel platebních služeb poskytuje zařízení nebo software pro přístup, záznam o použití zařízení nebo softwaru pro přístup poskytnutého uživateli platebních služeb a neobvyklé použití zařízení nebo softwaru pro přístup.

Článek 3

Přezkum bezpečnostních opatření

1. Uplatňování bezpečnostních opatření uvedených v článku 1 je zdokumentováno, pravidelně testováno, vyhodnocováno a kontrolováno v souladu s platným právním rámcem poskytovatele platebních služeb auditory, kteří mají odborné znalosti v oblasti bezpečnosti informačních technologií a plateb a kteří jsou funkčně nezávislí na poskytovateli platebních služeb.

2. Období mezi audity uvedenými v odstavci 1 je stanoveno s přihlédnutím k příslušnému rámci pro účetnictví a povinný audit, který se vztahuje na poskytovatele platebních služeb.

Poskytovatelé platebních služeb, kteří využívají výjimku stanovenou v článku 18, však podléhají auditu metodiky, modelu a oznámené míry podvodů minimálně jednou ročně. Auditor provádějící tento audit má odborné znalosti v oblasti bezpečnosti informačních technologií a plateb a je funkčně nezávislý na poskytovateli platebních služeb. Během prvního roku používání výjimky podle článku 18 a poté nejméně co tři roky či na žádost příslušného orgánu častěji provede tento audit nezávislý a kvalifikovaný externí auditor.

3. V rámci tohoto auditu je předloženo hodnocení a zpráva o souladu bezpečnostních opatření poskytovatele platebních služeb s požadavky stanovenými v tomto nařízení.

Celá zpráva je na žádost zpřístupněna příslušným orgánům.

KAPITOLA II

BEZPEČNOSTNÍ OPATŘENÍ PRO UPLATŇOVÁNÍ SILNÉHO OVĚŘENÍ KLIENTA

Článek 4

Ověřovací kód

1. Pokud poskytovatelé platebních služeb uplatňují silné ověření klienta v souladu s čl. 97 odst. 1 směrnice (EU) 2015/2366, je ověření založeno na dvou či více prvcích z kategorie znalost, držení a inherence a vede k vytvoření ověřovacího kódu.

Ověřovací kód je poskytovatelem platebních služeb akceptován pouze jednou, pokud plátce používá ověřovací kód k on-line přístupu ke svému platebnímu účtu, k iniciování elektronické platební transakce nebo k provedení jakéhokoli úkonu, který by mohl vést k riziku platebního podvodu nebo jiných zneužití, prostřednictvím prostředků komunikace na dálku.

2. Pro účely odstavce 1 přijmou poskytovatelé platebních služeb bezpečnostní opatření, která zajišťují splnění všech těchto požadavků:

a) ze sděleného ověřovacího kódu nelze odvodit informace o žádném z prvků uvedených v odstavci 1;

b) na základě znalosti jiného, dříve vytvořeného ověřovacího kódu nelze vytvořit nový ověřovací kód;

c) ověřovací kód nelze zfalšovat.

3. Poskytovatelé platebních služeb zajistí, aby ověření prostřednictvím vytvoření ověřovacího kódu zahrnovalo všechna tato opatření:

a) pokud ověření za účelem přístupu na dálku, elektronických plateb na dálku a jakýchkoli jiných úkonů, které by mohly vést k riziku platebního podvodu nebo jiných zneužití, provedených prostřednictvím prostředků komunikace na dálku nevytvoří ověřovací kód pro účely odstavce 1, není možné určit, který z prvků uvedených v daném odstavci nebyl správný;

b) počet neúspěšných, po sobě následujících pokusů o ověření, po jehož překročení jsou úkony uvedené v čl. 97 odst. 1 směrnice (EU) 2015/2366 dočasně nebo trvale zablokovány, nepřekročí v daném časovém období pět;

c) komunikační spojení jsou chráněna před získáním ověřovacích údajů předávaných během ověřování a před manipulací neoprávněnými stranami v souladu s požadavky stanovenými v kapitole V;

d) maximální doba nečinnosti plátce po ověření za účelem on-line přístupu k jeho platebnímu účtu nepřesáhne pět minut.

4. Je-li blokování uvedené v odst. 3 písm. b) dočasné, doba trvání tohoto blokování a počet opakovaných pokusů jsou stanoveny podle charakteristik služby poskytované plátci a všech příslušných souvisejících rizik, přičemž se přihlíží minimálně k faktorům uvedeným v čl. 2 odst. 2.

Před trvalým zablokováním je plátce upozorněn.

Je-li blokování trvalé, je stanoven zabezpečený postup, který plátci umožňuje obnovit používání zablokovaných elektronických platebních prostředků.

Článek 5

Dynamické propojení

1. Pokud poskytovatelé platebních služeb uplatňují silné ověření klienta podle čl. 97 odst. 2 směrnice (EU) 2015/2366, přijmou kromě požadavků stanovených v článku 4 tohoto nařízení rovněž bezpečnostní opatření, která splňují všechny tyto požadavky:

a) plátce je informován o částce platební transakce a o příjemci;

b) vytvořený ověřovací kód je specifický pro částku platební transakce a příjemce schváleného plátcem při iniciování transakce;

c) ověřovací kód akceptovaný poskytovatelem platebních služeb odpovídá původní konkrétní částce platební transakce a totožnosti příjemce schváleného plátcem;

d) jakákoli změna částky nebo příjemce vede k zneplatnění vytvořeného ověřovacího kódu.

2. Pro účely odstavce 1 přijmou poskytovatelé platebních služeb bezpečnostní opatření, která zajišťují důvěrnost, pravost a integritu všech těchto údajů:

a) částky transakce a příjemce během všech fází ověřování;

b) informací zobrazených plátci během všech fází ověřování, včetně vytvoření, předání a použití ověřovacího kódu.

3. Pro účely odst. 1 písm. b) se v případě, že poskytovatelé platebních služeb uplatňují silné ověření klienta podle čl. 97 odst. 2 směrnice (EU) 2015/2366, použijí tyto požadavky na ověřovací kód:

a) ve vztahu ke karetní platební transakci, s ohledem na niž plátce udělil souhlas s přesnou výší peněžních prostředků, jež mají být zablokovány, podle čl. 75 odst. 1 uvedené směrnice, je ověřovací kód specifický pro částku, s ohledem na niž udělil plátce souhlas se zablokováním a kterou plátce schválil při iniciování transakce;

b) ve vztahu k platebním transakcím, s ohledem na něž plátce udělil souhlas s provedením dávky elektronických platebních transakcí na dálku pro jednoho či více příjemců, je ověřovací kód specifický pro celkovou částku dávky platebních transakcí a pro uvedené příjemce.

Článek 6

Požadavky na prvky z kategorie znalost

1. Poskytovatelé platebních služeb přijmou opatření k zmírnění rizika toho, že prvky silného ověření klienta z kategorie znalost jsou odhaleny neoprávněnými stranami nebo sděleny těmto stranám.

2. Použití těchto prvků ze strany plátce je podmíněno opatřeními k zmírnění rizika, která mají zabránit jejich sdělení neoprávněným stranám.

Článek 7

Požadavky na prvky z kategorie držení

1. Poskytovatelé platebních služeb přijmou opatření k zmírnění rizika toho, že prvky silného ověření klienta z kategorie držení jsou použity neoprávněnými stranami.

2. Použití těchto prvků ze strany plátce je podmíněno opatřeními, která mají zabránit replikaci prvků.

Článek 8

Požadavky na zařízení a software související s prvky z kategorie inherence

1. Poskytovatelé platebních služeb přijmou opatření k zmírnění rizika toho, že ověřovací prvky z kategorie inherence snímané zařízením a softwarem pro přístup poskytnutým plátci jsou odhaleny neoprávněnými stranami. Poskytovatelé platebních služeb přinejmenším zajistí, aby u tohoto zařízení a softwaru pro přístup existovala velmi nízká pravděpodobnost ověření neoprávněné strany jako plátce.

2. Použití těchto prvků plátcem je podmíněno opatřeními, která zajišťují, aby tato zařízení a software zaručovaly odolnost vůči neautorizovanému použití prvků prostřednictvím přístupu k zařízením a softwaru.

Článek 9

Nezávislost jednotlivých prvků

1. Poskytovatelé platebních služeb zajistí, aby použití prvků silného ověření klienta podle článků 6, 7 a 8 podléhalo opatřením, která z hlediska technologie, algoritmů a parametrů zajišťují, že nesplnění jednoho z těchto prvků neovlivní spolehlivost ostatních prvků.

2. Poskytovatelé platebních služeb přijmou bezpečnostní opatření pro případ, kdy jsou prvky silného ověření klienta nebo samotný ověřovací kód použity víceúčelovým zařízením, k zmírnění rizika vyplývajícího ze zneužití víceúčelového zařízení.

3. Pro účely odstavce 2 zahrnují opatření k zmírnění rizika veškeré tyto součásti:

a) použití odděleného bezpečného prostředí pro provedení prostřednictvím softwaru nainstalovaného ve víceúčelovém zařízení;

b) mechanismy k zajištění toho, aby software nebo zařízení nebyly pozměněny plátcem nebo třetí stranou;

c) došlo-li ke změnám, mechanismy k zmírnění jejich důsledků.

KAPITOLA III

VÝJIMKY Z POŽADAVKU NA UPLATNĚNÍ SILNÉHO OVĚŘENÍ KLIENTA

Článek 10

Informování o platebním účtu

1. Poskytovatelům platebních služeb je umožněno, aby s výhradou dodržení požadavků stanovených v článku 2 a odstavce 2 tohoto článku neuplatňovali silné ověření klienta v případě, je-li on-line přístup uživatele platebních služeb omezen na některou či obě z níže uvedených položek, aniž by byly sděleny citlivé údaje o platbách:

a) zůstatek na jednom či více určených platebních účtech;

b) platební transakce provedené v posledních 90 dnech prostřednictvím jednoho či více určených platebních účtů.

2. Pro účely odstavce 1 nejsou poskytovatelé platebních služeb osvobozeni od požadavku na uplatňování silného ověření klienta, je-li splněna některá z těchto podmínek:

a) uživatel platebních služeb získává on-line přístup k informacím uvedeným v odstavci 1 poprvé;

b) od posledního on-line přístupu uživatele platebních služeb k informacím uvedeným v odst. 1 písm. b), kdy bylo použito silné ověření klienta, uplynulo více než 90 dnů.

Článek 11

Bezkontaktní platby v místě prodeje

Poskytovatelům platebních služeb je umožněno, aby s výhradou splnění požadavků stanovených v článku 2 neuplatňovali silné ověření klienta, pokud plátce iniciuje bezkontaktní elektronickou platební transakci, za předpokladu, že jsou splněny tyto podmínky:

a) jednotlivá částka bezkontaktní elektronické platební transakce nepřesáhne 50 EUR a

b) kumulativní částka předchozích bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku s bezkontaktní funkcí ode dne posledního uplatnění silného ověření klienta nepřesáhne 150 EUR, nebo

c) počet po sobě následujících bezkontaktních elektronických platebních transakcí iniciovaných prostřednictvím platebního prostředku nabízejícího bezkontaktní funkci ode dne posledního uplatnění silného ověření klienta nepřesáhne pět.

Článek 12

Terminály bez obsluhy pro jízdné a poplatky za parkování

Poskytovatelům platebních služeb je umožněno, aby s výhradou splnění požadavků stanovených v článku 2 neuplatňovali silné ověření klienta, pokud plátce iniciuje elektronickou platební transakci u terminálu bez obsluhy za účelem uhrazení jízdného nebo poplatku za parkování.

Článek 13

Důvěryhodní příjemci

1. Poskytovatelé platebních služeb uplatňují silné ověření klienta v případě, že plátce prostřednictvím poskytovatele platebních služeb, který vede účet plátce, vytváří nebo mění seznam důvěryhodných příjemců.

2. Poskytovatelům platebních služeb je umožněno, aby s výhradou splnění obecných požadavků na ověření neuplatňovali silné ověření klienta, pokud plátce iniciuje platební transakci a příjemce je zařazen na seznam důvěryhodných příjemců, který předtím plátce vytvořil.

Článek 14

Opakující se transakce

1. Poskytovatelé platebních služeb uplatňují silné ověření klienta v případě, že plátce vytváří, mění nebo poprvé iniciuje řadu opakujících se transakcí se stejnou částkou a stejným příjemcem.

2. Poskytovatelům platebních služeb je umožněno, aby s výhradou splnění obecných požadavků na ověření neuplatňovali silné ověření klienta v případě iniciování všech následných platebních transakcí zařazených do řady platebních transakcí podle odstavce 1.

Článek 15

Úhrady mezi účty téže fyzické nebo právnické osoby

Poskytovatelům platebních služeb je umožněno, aby s výhradou splnění požadavků stanovených v článku 2 neuplatňovali silné ověření klienta, pokud plátce iniciuje úhradu v situaci, kdy plátcem a příjemcem je stejná fyzická nebo právnická osoba a oba platební účty jsou vedeny týmž poskytovatelem platebních služeb, který vede účet.

Článek 16

Transakce týkající se malých částek

Poskytovatelům platebních služeb je umožněno, aby neuplatňovali silné ověření klienta, pokud plátce iniciuje elektronickou platební transakci na dálku, za předpokladu, že jsou splněny tyto podmínky:

a) částka elektronické platební transakce na dálku nepřesáhne 30 EUR a

b) kumulativní částka předchozích elektronických platebních transakcí na dálku iniciovaných plátcem ode dne posledního uplatnění silného ověření klienta nepřesáhne 100 EUR, nebo

c) počet předchozích elektronických platebních transakcí na dálku iniciovaných plátcem od posledního uplatnění silného ověření klienta nepřesáhne pět po sobě následujících jednotlivých elektronických platebních transakcí na dálku.

Článek 17

Zabezpečené platební procesy a protokoly společností

Poskytovatelům platebních služeb je umožněno, aby neuplatňovali silné ověření klienta s ohledem na právnické osoby, které iniciují elektronické platební transakce použitím zvláštních platebních procesů nebo protokolů, které jsou zpřístupněny pouze plátcům, kteří nejsou spotřebiteli, pokud se příslušné orgány přesvědčí, že tyto procesy nebo protokoly zaručují úrovně bezpečnosti, které jsou přinejmenším rovnocenné úrovním bezpečnosti stanoveným směrnicí (EU) 2015/2366.

Článek 18

Analýza transakčních rizik

1. Poskytovatelům platebních služeb je umožněno, aby neuplatňovali silné ověření klienta, pokud plátce iniciuje elektronickou platební transakci na dálku, kterou poskytovatel platebních služeb identifikoval jako transakci s nízkou mírou rizika na základě mechanismů sledování transakcí uvedených v článku 2 a v odst. 2 písm. c) tohoto článku.

2. Elektronická platební transakce uvedená v odstavci 1 se pokládá za transakci s nízkou mírou rizika, jsou-li splněny všechny tyto podmínky:

a) míra podvodů u tohoto druhu transakcí nahlášená poskytovatelem platebních služeb a vypočítaná podle článku 19 je rovnocenná nebo nižší než referenční míry podvodů stanovené v tabulce v příloze pro „elektronické karetní platby na dálku“, resp. „elektronické úhrady na dálku“;

b) částka transakce nepřesahuje příslušnou prahovou hodnotu pro výjimku stanovenou v tabulce v příloze;

c) poskytovatelé platebních služeb v důsledku provedené analýzy rizik v reálném čase nezjistili:

   i) neobvyklé výdaje nebo vzorec chování plátce;

   ii) neobvyklé informace o zařízení/softwaru plátce pro přístup;

   iii) napadení malwarem při spojení v rámci postupu ověření;

   iv) známé scénáře podvodů při poskytování platebních služeb;

   v) neobvyklé místo plátce;

   vi) vysoce rizikové místo příjemce.

3. Poskytovatelé platebních služeb, kteří hodlají osvobodit elektronické platební transakce na dálku od požadavku na silné ověření klienta z toho důvodu, že představují nízké riziko, vezmou v úvahu minimálně tyto rizikové faktory:

a) předchozí strukturu výdajů jednotlivého uživatele platebních služeb;

b) historii platebních transakcí každého uživatele platebních služeb poskytovatele platebních služeb;

c) místo plátce a příjemce v době provedení platební transakce v případech, kdy poskytovatel platebních služeb zajišťuje zařízení nebo software pro přístup;

d) zjištění neobvyklých struktur plateb uživatele platebních služeb ve vztahu k historii jeho platebních transakcí.

V rámci posouzení provedeného poskytovatelem platebních služeb jsou všechny tyto rizikové faktory zahrnuty do ohodnocení rizika každé jednotlivé transakce za účelem určení, zda by měla být konkrétní platba povolena bez silného ověření klienta.

Článek 19

Výpočet míry podvodů

1. Pro každý druh transakcí uvedený v tabulce v příloze poskytovatel platebních služeb zajistí, aby celkové míry podvodů vztahující se na platební transakce ověřené prostřednictvím silného ověření klienta i na platební transakce provedené na základě výjimek stanovených v článcích 13 až 18 byly rovnocenné nebo nižší než referenční míra podvodů u stejného druhu platebních transakcí podle tabulky v příloze.

Celková míra podvodů u každého druhu transakcí se vypočítá jako celková hodnota neautorizovaných nebo podvodných transakcí na dálku bez ohledu na to, zda byly peněžní prostředky vráceny, či nikoli, vydělená celkovou hodnotou všech transakcí na dálku u stejného druhu transakcí bez ohledu na to, zda byly ověřeny s použitím silného ověření klienta, nebo provedeny na základě některé z výjimek uvedených v článcích 13 až 18, a to klouzavě na čtvrtletním základě (90 dnů).

2. Výpočet míry podvodů a výsledné údaje jsou posouzeny v rámci auditního přezkumu podle čl. 3 odst. 2, který zajistí jejich úplnost a správnost.

3. Metodika a modely používané poskytovatelem platebních služeb k výpočtu míry podvodů i samotné míry podvodů jsou náležitě zdokumentovány a plně zpřístupněny příslušným orgánům a po předchozím vyrozumění dotčených příslušných orgánů též orgánu EBA na jejich žádost.

Článek 20

Ukončení platnosti výjimek na základě analýzy transakčních rizik

1. Poskytovatelé platebních služeb, kteří využívají výjimku stanovenou v článku 18, neprodleně vyrozumí příslušné orgány, pokud jedna ze sledovaných měr podvodů u kteréhokoli druhu platebních transakcí podle tabulky v příloze překročí platnou referenční míru podvodů, a poskytnou příslušným orgánům popis opatření, která hodlají přijmout k obnovení souladu sledované míry podvodů s platnými referenčními mírami podvodů.

2. Poskytovatelé platebních služeb okamžitě přestanou používat výjimku uvedenou v článku 18 u jakéhokoli druhu platebních transakcí podle tabulky v příloze v konkrétním intervalu prahové hodnoty pro výjimku, pokud jejich sledovaná míra podvodů přesáhne během dvou po sobě následujících čtvrtletí referenční míru podvodů vztahující se na daný platební prostředek nebo druh platebních transakcí v daném intervalu prahové hodnoty pro výjimku.

3. Po skončení platnosti výjimky uvedené v článku 18 v souladu s odstavcem 2 tohoto článku nepoužijí poskytovatelé platebních služeb znovu tuto výjimku, dokud se jejich vypočítaná míra podvodů po dobu jednoho čtvrtletí nerovná referenčním mírám podvodů vztahujícím se na daný druh platebních transakcí v daném intervalu prahové hodnoty pro výjimku, nebo není nižší.

4. Pokud poskytovatelé platebních služeb hodlají znovu využívat výjimku uvedenou v článku 18, vyrozumí v přiměřené lhůtě příslušné orgány a před opětovným používáním výjimky předloží důkazy o obnovení shody jejich sledované míry podvodů s platnou referenční mírou podvodů pro daný interval prahové hodnoty pro výjimku v souladu s odstavcem 3 tohoto článku.

Článek 21

Sledování

1. K využití výjimek stanovených v článcích 10 až 18 poskytovatelé platebních služeb alespoň čtvrtletně zaznamenávají a sledují pro každý druh platebních transakcí níže uvedené údaje v rozdělení na platební transakce na dálku a ostatní platební transakce neprováděné na dálku:

a) celkovou hodnotu neautorizovaných nebo podvodných platebních transakcí v souladu s čl. 64 odst. 2 směrnice (EU) 2015/2366, celkovou hodnotu všech platebních transakcí a výslednou míru podvodů, včetně rozdělení na platební transakce iniciované prostřednictvím silného ověření klienta a na základě jednotlivých výjimek;

b) průměrnou hodnotu transakce, včetně rozdělení na platební transakce iniciované prostřednictvím silného ověření klienta a na základě jednotlivých výjimek;

c) počet platebních transakcí, kdy byla použita každá z výjimek, a jejich procentní podíl na celkovém počtu platebních transakcí.

2. Poskytovatelé platebních služeb zpřístupní výsledky sledování podle odstavce 1 příslušným orgánům a po předchozím vyrozumění dotčených příslušných orgánů též orgánu EBA na jejich žádost.

KAPITOLA IV

DŮVĚRNOST A INTEGRITA OSOBNÍCH BEZPEČNOSTNÍCH ÚDAJŮ UŽIVATELŮ PLATEBNÍCH SLUŽEB

Článek 22

Obecné požadavky

1. Poskytovatelé platebních služeb zajistí během všech fází ověřování důvěrnost a integritu osobních bezpečnostních údajů uživatele platebních služeb, včetně ověřovacích kódů.

2. Pro účely odstavce 1 poskytovatelé platebních služeb zajistí, aby byly splněny všechny tyto požadavky:

a) osobní bezpečnostní údaje jsou při zobrazení zamaskovány a při zadávání uživatelem platebních služeb během ověřování nejsou čitelné v celém rozsahu;

b) osobní bezpečnostní údaje v datovém formátu a kryptografické materiály týkající se šifrování osobních bezpečnostních údajů nejsou uchovávány jako nešifrovaný text;

c) tajné kryptografické materiály jsou chráněny před neoprávněným poskytnutím.

3. Poskytovatelé platebních služeb plně dokumentují postup pro správu kryptografických materiálů používaných k šifrování či k zajištění nečitelnosti osobních bezpečnostních údajů jiným způsobem.

4. Poskytovatelé platebních služeb zajistí, aby se zpracování a směrování osobních bezpečnostních údajů a ověřovacích kódů vytvořených podle kapitoly II uskutečňovalo v bezpečném prostředí v souladu s přísnými a obecně uznávanými odvětvovými normami.

Článek 23

Vytváření a předávání údajů

Poskytovatelé platebních služeb zajistí, aby byly osobní bezpečnostní údaje vytvářeny v bezpečném prostředí.

Poskytovatelé platebních služeb sníží rizika neautorizovaného použití osobních bezpečnostních údajů a zařízení a softwaru pro ověřování po jejich ztrátě, odcizení nebo zkopírování před jejich předáním plátci.

Článek 24

Přiřazení k uživateli platebních služeb

1. Poskytovatelé platebních služeb zajistí, aby byl k osobním bezpečnostním údajům a zařízení a softwaru pro ověřování bezpečným způsobem přiřazen pouze jeden uživatel platebních služeb.

2. Pro účely odstavce 1 poskytovatelé platebních služeb zajistí, aby byly splněny všechny tyto požadavky:

a) přiřazení totožnosti uživatele platebních služeb k osobním bezpečnostním údajům a zařízení a softwaru pro ověřování se provádí v bezpečném prostředí v rámci odpovědnosti poskytovatele platebních služeb, jež zahrnuje přinejmenším prostory poskytovatele platebních služeb, internetové prostředí poskytované poskytovatelem platebních služeb nebo jiné podobné bezpečné internetové stránky používané poskytovatelem platebních služeb a jeho služby bankomatu, přičemž se zohlední rizika související se zařízeními a příslušnými prvky používanými v procesu přiřazování, za něž poskytovatel platebních služeb nenese odpovědnost;

b) přiřazení totožnosti uživatele platebních služeb prostřednictvím prostředků komunikace na dálku k osobním bezpečnostním údajům a zařízení nebo softwaru pro ověřování se provádí pomocí silného ověření klienta.

Článek 25

Poskytování údajů a zařízení a softwaru pro ověřování

1. Poskytovatelé platebních služeb zajistí, aby se poskytování osobních bezpečnostních údajů a zařízení a softwaru pro ověřování uživateli platebních služeb uskutečnilo bezpečným způsobem, který odstraňuje rizika související s jejich neautorizovaným použitím v důsledku jejich ztráty, odcizení či zkopírování.

2. Pro účely odstavce 1 uplatňují poskytovatelé platebních služeb přinejmenším všechna tato opatření:

a) účinné a bezpečné mechanismy poskytování, které zajišťují, aby byly osobní bezpečnostní údaje a zařízení a software pro ověřování poskytnuty oprávněnému uživateli platebních služeb;

b) mechanismy, které poskytovateli platebních služeb umožňují ověřit pravost softwaru pro ověřování poskytnutého uživateli platebních služeb prostřednictvím internetu;

c) ujednání, která zajišťují, že pokud k poskytnutí osobních bezpečnostních údajů dochází mimo prostory poskytovatele platebních služeb nebo prostřednictvím prostředků komunikace na dálku:

   i) nemůže neoprávněná strana při poskytování prostřednictvím téhož kanálu získat více než jeden prvek osobních bezpečnostních údajů, zařízení nebo softwaru pro ověřování;

   ii) poskytnuté osobní bezpečnostní údaje a zařízení nebo software pro ověřování vyžadují před použitím aktivaci;

d) ujednání, která zajišťují, že se v případech, kdy je nutno osobní bezpečnostní údaje a zařízení nebo software pro ověřování před prvním použitím aktivovat, tato aktivace uskuteční v bezpečném prostředí v souladu s postupy přiřazování uvedenými v článku 24.

Článek 26

Obnovení osobních bezpečnostních údajů

Poskytovatelé platebních služeb zajistí, aby byly při obnovení nebo opětovné aktivaci osobních bezpečnostních údajů dodrženy postupy pro vytváření, přiřazování a poskytování údajů a zařízení pro ověřování v souladu s články 23, 24 a 25.

Článek 27

Likvidace, deaktivace a zrušení

Poskytovatelé platebních služeb zajistí, aby byly zavedeny účinné procesy pro uplatňování všech těchto bezpečnostních opatření:

a) bezpečná likvidace, deaktivace nebo zrušení osobních bezpečnostních údajů a zařízení nebo softwaru pro ověřování;

b) pokud poskytovatel platebních služeb distribuuje opakovaně použitelná zařízení a software pro ověřování, je stanoveno, zdokumentováno a zajištěno bezpečné opětovné použití zařízení nebo softwaru před jeho poskytnutím jinému uživateli platebních služeb;

c) deaktivace nebo zrušení informací souvisejících s osobními bezpečnostními údaji uchovávanými v systémech a databázích poskytovatele platebních služeb a případně veřejných úložištích.

KAPITOLA V

SPOLEČNÉ A BEZPEČNÉ OTEVŘENÉ STANDARDY KOMUNIKACE

Oddíl 1

Obecné požadavky na komunikaci

Článek 28

Požadavky na identifikaci

1. Poskytovatelé platebních služeb zajistí bezpečnou identifikaci při komunikaci mezi zařízením plátce a zařízeními příjemce pro přijímání elektronických plateb, mimo jiné včetně platebních terminálů.

2. Poskytovatelé platebních služeb zajistí, aby byla v mobilních aplikacích a jiných rozhraních uživatelů platebních služeb, jež nabízejí elektronické platební služby, účinně zmírněna rizika chybného směrování komunikace k neoprávněným stranám.

Článek 29

Sledovatelnost

1. Poskytovatelé platebních služeb zavedou procesy, které zajišťují, že veškeré platební transakce a ostatní interakce s uživatelem platebních služeb, s dalšími poskytovateli platebních služeb a s ostatními subjekty, včetně obchodníků, v rámci poskytování platební služby lze sledovat, a zaručují následnou znalost všech událostí týkajících se elektronické transakce ve všech jednotlivých fázích.

2. Pro účely odstavce 1 poskytovatelé platebních služeb zajistí, aby komunikační spojení navázané s uživatelem platebních služeb, dalšími poskytovateli platebních služeb a ostatními subjekty, včetně obchodníků, využívalo všechny tyto prvky:

a) jedinečný identifikátor spojení;

b) bezpečnostní mechanismy pro podrobné zaznamenání transakce, včetně čísla transakce, časových razítek a všech příslušných údajů o transakci;

c) časová razítka, která se zakládají na systému jednotného času a jsou synchronizována podle oficiálního časového signálu.

Oddíl 2

Zvláštní požadavky na společné a bezpečné otevřené standardy komunikace

Článek 30

Obecné povinnosti vztahující se na rozhraní pro přístup

1. Poskytovatelé platebních služeb, kteří vedou účet a kteří nabízejí plátci platební účet, který je přístupný on-line, zavedou přinejmenším jedno rozhraní, které splňuje všechny tyto požadavky:

a) poskytovatelé služeb informování o účtu, poskytovatelé služeb iniciování platby a poskytovatelé platebních služeb vydávající karetní platební prostředky se mohou identifikovat u poskytovatele platebních služeb, který vede účet;

b) poskytovatelé služeb informování o účtu mohou bezpečně komunikovat za účelem vyžádání a obdržení informací o jednom či více určených platebních účtech a souvisejících platebních transakcích;

c) poskytovatelé služeb iniciování platby mohou bezpečně komunikovat za účelem iniciování platebního příkazu z platebního účtu plátce a obdržení veškerých informací o iniciování platební transakce a veškerých informací o provedení platební transakce, k nimž mají přístup poskytovatelé platebních služeb, kteří vedou účet.

2. Pro účely ověření uživatele platebních služeb umožňuje rozhraní uvedené v odstavci 1 poskytovatelům služeb informování o účtu a poskytovatelům služeb iniciování platby využívat postupy ověření stanovené poskytovatelem platebních služeb, který vede účet, pro uživatele platebních služeb.

Rozhraní splňuje přinejmenším všechny tyto požadavky:

a) poskytovatel služeb iniciování platby nebo poskytovatel služeb informování o účtu může vydat poskytovateli platebních služeb, který vede účet, pokyn k zahájení ověření na základě souhlasu uživatele platebních služeb;

b) po celou dobu ověřování jsou navázána a udržována komunikační spojení mezi poskytovatelem platebních služeb, který vede účet, poskytovatelem služeb informování o účtu, poskytovatelem služeb iniciování platby a dotyčným uživatelem platebních služeb;

c) je zajištěna integrita a důvěrnost osobních bezpečnostních údajů a ověřovacích kódů předaných poskytovatelem služeb iniciování platby nebo poskytovatelem služeb informování o účtu či jejich prostřednictvím.

3. Poskytovatelé platebních služeb, kteří vedou účet, zajistí, aby jejich rozhraní dodržovala standardy komunikace, které vydaly mezinárodní nebo evropské normalizační organizace.

Poskytovatelé platebních služeb, kteří vedou účet, rovněž zajistí, aby byla zdokumentována technická specifikace všech rozhraní, která stanoví soubor postupů, protokolů a nástrojů, jež poskytovatelé služeb iniciování platby, poskytovatelé služeb informování o účtu a poskytovatelé platebních služeb vydávající karetní platební prostředky potřebují k zajištění interoperability jejich softwaru a aplikací se systémy poskytovatelů platebních služeb, kteří vedou účet.

Poskytovatelé platebních služeb, kteří vedou účet, zpřístupní minimálně a nejméně šest měsíců přede dnem použitelnosti uvedeným v čl. 38 odst. 2, nebo před cílovým datem pro uvedení rozhraní pro přístup na trh, dojde-li k jeho uvedení po dni uvedeném v čl. 38 odst. 2, zdarma na žádost oprávněných poskytovatelů služeb iniciování platby, poskytovatelů služeb informování o účtu a poskytovatelů platebních služeb vydávajících karetní platební prostředky nebo poskytovatelů platebních služeb, kteří požádali příslušné orgány o potřebné povolení, příslušnou dokumentaci a zveřejní shrnutí dokumentace na svých internetových stránkách.

4. Kromě odstavce 3 poskytovatelé platebních služeb, kteří vedou účet, zajistí, aby s výjimkou mimořádných situací byly veškeré změny technické specifikace jejich rozhraní předem zpřístupněny oprávněným poskytovatelům služeb iniciování platby, poskytovatelům služeb informování o účtu a poskytovatelům platebních služeb vydávajícím karetní platební prostředky, nebo poskytovatelům platebních služeb, kteří požádali příslušné orgány o potřebné povolení, a to co nejdříve, nejpozději však tři měsíce před provedením změny.

Poskytovatelé platebních služeb zdokumentují mimořádné situace, kdy byly provedeny změny, a zpřístupní dokumentaci na žádost příslušným orgánům.

5. Poskytovatelé platebních služeb, kteří vedou účet, zpřístupní testovací zařízení, včetně podpory, pro spojení a testování funkčnosti, aby mohli oprávnění poskytovatelé služeb iniciování platby, poskytovatelé platebních služeb vydávající karetní platební prostředky a poskytovatelé služeb informování o účtu, nebo poskytovatelé platebních služeb, kteří požádali o potřebné povolení, otestovat svůj software a aplikace používané k nabízení platebních služeb uživatelům. Testovací zařízení by mělo být k dispozici nejpozději šest měsíců přede dnem použitelnosti uvedeným v čl. 38 odst. 2, nebo před cílovým datem pro uvedení rozhraní pro přístup na trh, má-li k uvedení dojít po dni uvedeném v čl. 38 odst. 2.

Prostřednictvím testovacího zařízení však nejsou sdíleny žádné citlivé informace.

6. Příslušné orgány zajistí, aby poskytovatelé platebních služeb, kteří vedou účet, plnili s ohledem na zavedená rozhraní trvale povinnosti obsažené v těchto normách. Pokud poskytovatel platebních služeb, který vede účet, nesplňuje požadavky na rozhraní stanovené v těchto normách, příslušné orgány zajistí, aby poskytování služeb iniciování platby a služeb informování o účtu nebylo znemožněno nebo narušeno, splňují-li příslušní poskytovatelé těchto služeb podmínky stanovené v čl. 33 odst. 5.

Článek 31

Možnosti rozhraní pro přístup

Poskytovatelé platebních služeb, kteří vedou účet, zajistí rozhraní podle článku 30 prostřednictvím vyhrazeného rozhraní nebo tím, že umožní, aby poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 používali rozhraní používaná k ověřování uživatelů platebních služeb poskytovatele platebních služeb, který vede účet, a ke komunikaci s nimi.

Článek 32

Povinnosti týkající se vyhrazeného rozhraní

1. S výhradou dodržení článků 30 a 31 poskytovatelé platebních služeb, kteří vedou účet a kteří zavedli vyhrazené rozhraní, zajistí, aby vyhrazené rozhraní zajišťovalo trvale stejnou úroveň dostupnosti a výkonu, včetně podpory, jako rozhraní zpřístupněná uživateli platebních služeb pro přímý on-line přístup k jeho platebnímu účtu.

2. Poskytovatelé platebních služeb, kteří vedou účet a kteří zavedli vyhrazené rozhraní, stanoví transparentní klíčové ukazatele výkonnosti a cíle týkající se úrovně služeb, jež jsou přinejmenším stejně přísné jako v případě rozhraní, které používají uživatelé jejich platebních služeb, a to jak z hlediska dostupnosti, tak i z hlediska údajů poskytovaných podle článku 36. Tato rozhraní, ukazatele a cíle jsou sledovány příslušnými orgány a jsou podrobeny zátěžovým testům.

3. Poskytovatelé platebních služeb, kteří vedou účet a kteří zavedli vyhrazené rozhraní, zajistí, aby toto rozhraní nevytvářelo překážky pro poskytování služeb iniciování platby a informování o účtu. Tyto překážky mohou zahrnovat mimo jiné zabránění tomu, aby poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 používali údaje vydané poskytovateli platebních služeb, kteří vedou účet, jejich klientům, uložení povinného přesměrování na ověření či jiné funkce poskytovatele platebních služeb, který vede účet, vyžadování dalších povolení a registrací kromě povolení a registrací stanovených v článcích 11, 14 a 15 směrnice (EU) 2015/2366 nebo požadování dodatečných kontrol souhlasu uděleného uživateli platebních služeb poskytovatelům služeb iniciování platby a informování o účtu.

4. Pro účely odstavců 1 a 2 sledují poskytovatelé platebních služeb, kteří vedou účet, dostupnost a výkon vyhrazeného rozhraní. Poskytovatelé platebních služeb, kteří vedou účet, zveřejňují na svých internetových stránkách čtvrtletně statistické údaje o dostupnosti a výkonu vyhrazeného rozhraní a rozhraní, které používají uživatelé jejich platebních služeb.

Článek 33

Nouzová opatření týkající se vyhrazeného rozhraní

1. Poskytovatelé platebních služeb, kteří vedou účet, zahrnou do návrhu vyhrazeného rozhraní strategii a plány týkající se nouzových opatření pro případ, že rozhraní nefunguje v souladu s článkem 32 nebo že dojde k neplánované nedostupnosti rozhraní a k zhroucení systémů. Lze mít za to, že k neplánované nedostupnosti nebo zhroucení systémů dojde tehdy, není-li do 30 sekund vyřízeno pět po sobě následujících žádostí o přístup k informacím pro poskytování služeb iniciování platby nebo služeb informování o účtu.

2. Nouzová opatření zahrnují komunikační plány pro informování poskytovatelů platebních služeb, kteří využívají vyhrazené rozhraní, o opatřeních k obnově systému a popis okamžitě dostupných alternativních možností, které mají poskytovatelé platebních služeb během této doby k dispozici.

3. Poskytovatel platebních služeb, který vede účet, i poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 oznámí neprodleně problémy s vyhrazenými rozhraními, jak je popsáno v odstavci 1, svým příslušným vnitrostátním orgánům.

4. V rámci nouzového mechanismu mohou poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 využít rozhraní zpřístupněná uživatelům platebních služeb za účelem ověření a komunikace s jejich poskytovatelem platebních služeb, který vede účet, dokud není vyhrazené rozhraní obnoveno na úroveň dostupnosti a výkonu stanovenou v článku 32.

5. Za tímto účelem poskytovatelé platebních služeb, kteří vedou účet, zajistí, aby poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 mohli být identifikováni a mohli využívat postupy ověření, které poskytovatel platebních služeb, který vede účet, poskytl uživateli platebních služeb. Pokud poskytovatelé platebních služeb uvedení v čl. 30 odst. 1 využívají rozhraní uvedené v odstavci 4:

a) přijmou nezbytná opatření k zajištění toho, aby nezískali přístup k údajům, neukládali ani nezpracovávali údaje pro jiné účely než poskytování služby podle požadavku uživatele platebních služeb;

b) i nadále dodržují povinnosti vyplývající z čl. 66 odst. 3, resp. čl. 67 odst. 2 směrnice (EU) 2015/2366;

c) zaznamenávají údaje, k nimž je získán přístup prostřednictvím rozhraní provozovaného poskytovatelem platebních služeb, který vede účet, pro uživatele jeho platebních služeb a na žádost neprodleně předají protokolové soubory svému příslušnému vnitrostátnímu orgánu;

d) na žádost svému příslušnému vnitrostátnímu orgánu neprodleně řádně odůvodní použití rozhraní, které bylo zpřístupněno uživatelům platebních služeb pro přímý on-line přístup k jejich platebnímu účtu;

e) náležitě informují poskytovatele platebních služeb, který vede účet.

6. Po konzultaci s orgánem EBA k zajištění jednotného uplatňování níže uvedených podmínek osvobodí příslušné orgány poskytovatele platebních služeb, kteří vedou účet a kteří se rozhodli používat vyhrazené rozhraní, od povinnosti zavést nouzový mechanismus popsaný v odstavci 4, pokud vyhrazené rozhraní splňuje všechny tyto podmínky:

a) dodržuje všechny povinnosti vztahující se na vyhrazená rozhraní, jak je stanoveno v článku 32;

b) bylo navrženo a otestováno v souladu s čl. 30 odst. 5 ke spokojenosti uvedených poskytovatelů platebních služeb;

c) poskytovatelé platebních služeb je rozsáhle používali po dobu alespoň tří měsíců k nabízení služeb informování o účtu, služeb iniciování platby a k potvrzení disponibility peněžních prostředků pro karetní platby;

d) veškeré problémy související s vyhrazeným rozhraním byly neprodleně odstraněny.

7. Příslušné orgány výjimku uvedenou v odstavci 6 zruší, pokud poskytovatelé platebních služeb, kteří vedou účet, nesplňují podmínky uvedené v písmenech a) a d) po dobu delší než dva po sobě následující kalendářní týdny. Příslušné orgány informují orgán EBA o tomto zrušení a zajistí, aby poskytovatel platebních služeb, který vede účet, v nejkratší možné lhůtě, nejpozději však do dvou měsíců, zavedl nouzový mechanismus uvedený v odstavci 4.

Článek 34

Certifikáty

1. Pro účely identifikace podle čl. 30 odst. 1 písm. a) využívají poskytovatelé platebních služeb kvalifikované certifikáty pro elektronické pečetě podle čl. 3 bodu 30 nařízení (EU) č. 910/2014 nebo pro autentizaci internetových stránek podle čl. 3 bodu 39 zmíněného nařízení.

2. Pro účely tohoto nařízení představuje registrační číslo uvedené v úředních záznamech v souladu s přílohou III písm. c) nebo přílohou IV písm. c) nařízení (EU) č. 910/2014 číslo povolení poskytovatele platebních služeb vydávajícího karetní platební prostředky, poskytovatele služeb informování o účtu a poskytovatele služeb iniciování platby, včetně poskytovatelů platebních služeb, kteří vedou účet, poskytujících tyto služby, které je k dispozici ve veřejném rejstříku domovského členského státu podle článku 14 směrnice (EU) 2015/2366 nebo které vyplývá z oznámení každého vydaného povolení uděleného podle článku 8 směrnice Evropského parlamentu a Rady 2013/36/EU ([1]) v souladu s článkem 20 zmíněné směrnice.

3. Pro účely tohoto nařízení zahrnují kvalifikované certifikáty pro elektronické pečetě nebo pro autentizaci internetových stránek uvedené v odstavci 1 v jazyce obvyklém v oblasti mezinárodních financí další zvláštní atributy ve vztahu k:

a) úloze poskytovatele platebních služeb, což může být jedna nebo více těchto služeb:

   i) vedení účtu;

   ii) iniciování platby;

   iii) informování o účtu;

   iv) vydávání karetních platebních prostředků;

b) názvu příslušných orgánů, u nichž je poskytovatel služby zaregistrován.

4. Atributy uvedené v odstavci 3 neovlivňují interoperabilitu a uznávání kvalifikovaných certifikátů pro elektronické pečetě nebo autentizaci internetových stránek.

([1]) Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

Článek 35

Zabezpečení komunikačního spojení

1. Poskytovatelé platebních služeb, kteří vedou účet, poskytovatelé platebních služeb vydávající karetní platební prostředky, poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby zajistí, aby se při výměně údajů prostřednictvím internetu uplatňovalo mezi komunikujícími stranami během celé doby trvání příslušného komunikačního spojení bezpečné šifrování k zajištění důvěrnosti a integrity údajů, a to s použitím důkladných a obecně uznávaných technik šifrování.

2. Poskytovatelé platebních služeb vydávající karetní platební prostředky, poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby zajistí, aby byla přístupová spojení nabízená poskytovateli platebních služeb, kteří vedou účet, co nejkratší, a aktivně toto spojení ukončí, jakmile byl proveden požadovaný úkon.

3. Při udržování souběžných síťových spojení s poskytovatelem platebních služeb, který vede účet, poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby zajistí, že tato spojení jsou bezpečně propojena s příslušnými spojeními navázanými s uživateli platebních služeb, aby se zabránilo možnému chybnému směrování zprávy nebo informací sdělovaných mezi nimi.

4. Poskytovatelé služeb informování o účtu, poskytovatelé služeb iniciování platby a poskytovatelé platebních služeb vydávající karetní platební prostředky s poskytovatelem platebních služeb, který vede účet, uvedou jednoznačné odkazy na všechny tyto položky:

a) na jediného uživatele nebo více uživatelů platebních služeb a odpovídající komunikační spojení k rozlišení jednotlivých žádostí od téhož uživatele či uživatelů platebních služeb;

b) u služeb iniciování platby na jedinečně identifikovanou platební transakci, která byla iniciována;

c) v případě potvrzení disponibility peněžních prostředků na jedinečně identifikovanou žádost týkající se částky potřebné pro provedení karetní platební transakce.

5. Poskytovatelé platebních služeb, kteří vedou účet, poskytovatelé služeb informování o účtu, poskytovatelé služeb iniciování platby a poskytovatelé platebních služeb vydávající karetní platební prostředky zajistí, aby v případě, že sdělují osobní bezpečnostní údaje a ověřovací kódy, nemohly být tyto nikdy přečteny přímo či nepřímo zaměstnanci.

V případě ztráty důvěrnosti osobních bezpečnostních údajů, které spadají do jejich oblasti působnosti, informují tito poskytovatelé neprodleně uživatele platebních služeb, který je k nim přiřazen, a subjekt, který osobní bezpečnostní údaje vydal.

Článek 36

Výměny údajů

1. Poskytovatelé platebních služeb, kteří vedou účet, splňují všechny tyto požadavky:

a) poskytují poskytovatelům služeb informování o účtu stejné informace o určených platebních účtech a souvisejících platebních transakcích, jaké byly zpřístupněny uživateli platebních služeb v případě, že požaduje přímý přístup k informacím o účtu, za předpokladu, že tyto informace neobsahují citlivé údaje o platbách;

b) neprodleně po obdržení platebního příkazu poskytnou poskytovatelům služeb iniciování platby stejné informace o iniciování a provedení platební transakce, jaké byly poskytnuty nebo zpřístupněny uživateli platebních služeb, je-li transakce iniciována přímo uživatelem platebních služeb;

c) na žádost neprodleně poskytnou poskytovatelům platebních služeb potvrzení v jednoduché formě „ano“ nebo „ne“ o tom, zda je na platebním účtu plátce k dispozici částka potřebná pro provedení platební transakce.

2. V případě neočekávané události nebo chyby, která se vyskytne během identifikace, ověřování nebo výměny údajů, zašle poskytovatel platebních služeb, který vede účet, oznamovací zprávu poskytovateli služeb iniciování platby nebo poskytovateli služeb informování o účtu a poskytovateli platebních služeb vydávajícímu karetní platební prostředky, v níž objasní důvod neočekávané události nebo chyby.

Pokud poskytovatel platebních služeb, který vede účet, nabízí vyhrazené rozhraní v souladu s článkem 32, umožňuje toto rozhraní předávání oznamovacích zpráv o neočekávaných událostech nebo chybách ze strany poskytovatele platebních služeb, který událost nebo chybu odhalí, ostatním poskytovatelům platebních služeb, kteří se účastní komunikačního spojení.

3. Poskytovatelé služeb informování o účtu zavedou vhodné a účinné mechanismy, které brání v přístupu k jiným informacím než k informacím o určených platebních účtech a souvisejících platebních transakcích v souladu s výslovným souhlasem uživatele.

4. Poskytovatelé služeb iniciování platby poskytnou poskytovatelům platebních služeb, kteří vedou účet, stejné informace, jaké se vyžadují od uživatele platebních služeb při přímém iniciování platební transakce.

5. Poskytovatelé služeb informování o účtu mohou získat přístup k informacím o určených platebních účtech a souvisejících platebních transakcích, které mají k dispozici poskytovatelé platebních služeb, kteří vedou účet, pro účely poskytování služeb informování o účtu v kterémkoli z těchto případů:

a) požaduje-li aktivně tyto informace uživatel platebních služeb;

b) pokud uživatel platebních služeb tyto informace aktivně nepožaduje, nejvýše čtyřikrát během 24 hodin, ledaže je mezi poskytovatelem služeb informování o účtu a poskytovatelem platebních služeb, který vede účet, se souhlasem uživatele platebních služeb dohodnuta vyšší četnost.

KAPITOLA VI

ZÁVĚREČNÁ USTANOVENÍ

Článek 37

Přezkum

Aniž je dotčeno ustanovení čl. 98 odst. 5 směrnice (EU) 2015/2366 přezkoumá orgán EBA do 14. března 2021 míry podvodů uvedené v příloze tohoto nařízení a výjimky udělené podle čl. 33 odst. 6 ve vztahu k vyhrazeným rozhraním a případně předloží Komisi návrhy na jejich aktualizace v souladu s článkem 10 nařízení (EU) č. 1093/2010.

Článek 38

Vstup v platnost

1. Toto nařízení vstupuje v platnost prvním dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Toto nařízení se použije ode dne 14. září 2019.

3. Ustanovení čl. 30 odst. 3 a 5 se však použijí ode dne 14. března 2019.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 27. listopadu 2017.

Za Komisi

předseda

Jean-Claude JUNCKER

PŘÍLOHA

	Referenční míra podvodů (v %)	
Prahová hodnota pro výjimku	Elektronické karetní platby na dálku	Elektronické úhrady na dálku
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015