DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2018/389

z 27. novembra 2017,

ktorým sa dopĺňa smernica Európskeho parlamentu a Rady (EÚ) 2015/2366, pokiaľ ide o regulačné technické predpisy pre silnú autentifikáciu zákazníka a spoločné a bezpečné otvorené komunikačné normy

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010 a ktorou sa zrušuje smernica 2007/64/ES ([1]), a najmä na jej článok 98 ods. 4 druhý pododsek,

keďže:

(1) Platobné služby ponúkané elektronicky by sa mali poskytovať bezpečne s využitím technológií schopných zaručiť bezpečnú autentifikáciu používateľa a v maximálnej možnej miere znížiť riziko podvodu. Postup autentifikácie by vo všeobecnosti mal zahŕňať mechanizmy monitorovania transakcií s cieľom odhaliť pokusy o používanie personalizovaných bezpečnostných prvkov používateľa platobných služieb, v prípade ktorých došlo k strate, odcudzeniu alebo zneužitiu, a mal by zároveň zaručiť, že používateľ platobných služieb je oprávneným používateľom, a teda udeľuje súhlas na prevod finančných prostriedkov a prístup k informáciám o svojom účte prostredníctvom bežného používania personalizovaných bezpečnostných prvkov. Okrem toho je potrebné špecifikovať požiadavky na silnú autentifikáciu zákazníka, ktoré by sa mali uplatňovať vždy, keď platiteľ pristupuje k svojmu platobnému účtu online, iniciuje elektronickú platobnú transakciu alebo vykoná akékoľvek kroky prostredníctvom diaľkového prístupu, ktoré môžu predstavovať riziko platobného podvodu alebo iného zneužitia, a to vyžadovaním vytvorenia autentifikačného kódu, ktorý by mal byť odolný voči riziku sfalšovania v celom rozsahu, alebo zverejnením ktoréhokoľvek z prvkov, na základe ktorých bol kód vytvorený.

(2) Keďže metódy podvodu sa neustále menia, požiadavky na silnú autentifikáciu zákazníka by mali umožňovať inováciu v oblasti technických riešení reagujúcich na vznik nových hrozieb pre bezpečnosť elektronických platieb. S cieľom zabezpečiť účinné a nepretržité vykonávanie požiadaviek, ktoré sa majú stanoviť, je vhodné vyžadovať aj to, aby bezpečnostné opatrenia na uplatňovanie silnej autentifikácie zákazníka a výnimky z nej, opatrenia na ochranu dôvernosti a integrity personalizovaných bezpečnostných prvkov a opatrenia, ktorými sa stanovujú spoločné a bezpečné otvorené komunikačné normy, boli zdokumentované, pravidelne skúšané, hodnotené a kontrolované audítormi s odbornými znalosťami v oblasti bezpečnosti informačných technológií a platieb, ktorí sú z hľadiska svojho pôsobenia nezávislí. S cieľom umožniť príslušným orgánom monitorovať kvalitu preskúmania týchto opatrení by sa im takéto preskúmania mali na požiadanie sprístupniť.

(3) Keďže elektronické platobné transakcie na diaľku sú vystavené väčšiemu riziku podvodu, je potrebné zaviesť dodatočné požiadavky na silnú autentifikáciu zákazníka takýchto transakcií, čím sa zabezpečí, že prvky dynamicky spájajú transakciu so sumou a s príjemcom platby, ktoré platiteľ určil pri iniciovaní transakcie.

(4) Dynamické spájanie je možné prostredníctvom generovania autentifikačných kódov, ktoré podlieha súboru prísnych bezpečnostných požiadaviek. V záujme zachovania technologickej neutrality by sa na uplatňovanie autentifikačných kódov nemala vyžadovať špecifická technológia. Autentifikačné kódy by preto mali byť založené na riešeniach, ako sú generovanie a validácia jednorazových hesiel, digitálnych podpisov alebo iných kryptograficky podložených validačných vyhlásení s použitím kľúčov alebo kryptografických materiálov uložených v autentifikačných prvkoch, a to za predpokladu, že sú splnené bezpečnostné požiadavky.

([1]) Ú. v. EÚ L 337, 23.12.2015, s. 35.

(5) Je potrebné stanoviť osobitné požiadavky pre situáciu, v ktorej konečná suma nie je známa v okamihu, keď platiteľ iniciuje elektronickú platobnú transakciu na diaľku, aby sa zabezpečilo, že silná autentifikácia zákazníka sa vzťahuje na maximálnu sumu, pre ktorú dal platiteľ svoj súhlas, ako sa uvádza v smernici (EÚ) 2015/2366.

(6) V záujme zabezpečenia uplatňovania silnej autentifikácie zákazníka je potrebné vyžadovať aj primerané bezpečnostné prvky pre prvky silnej autentifikácie zákazníka kategorizované ako poznatok (niečo, čo vie len používateľ), ako napríklad dĺžka alebo zložitosť, pre prvky kategorizované ako vlastníctvo (niečo, čo má len používateľ), ako napríklad špecifikácie algoritmov, dĺžka kľúča a informačná entropia, a pre zariadenia a softvér, ktoré čítajú prvky kategorizované ako inherencia (niečo, čím používateľ je), ako napríklad špecifikácie algoritmov, biometrický senzor a funkcie ochrany formulárov, najmä s cieľom zmierniť riziko, že neautorizované strany tieto prvky odhalia, že im budú sprístupnené a že ich neautorizované strany použijú. Okrem toho je potrebné stanoviť požiadavky na zabezpečenie toho, aby tieto prvky boli nezávislé tak, aby pri porušení jedného nedošlo k ohrozeniu spoľahlivosti ostatných, najmä ak sa niektorý z týchto prvkov používa prostredníctvom viacúčelového zariadenia, a to konkrétne zariadenia ako tablet alebo mobilný telefón, ktoré možno použiť na zadanie pokynu na vykonanie platby aj v procese autentifikácie.

(7) Požiadavky na silnú autentifikáciu zákazníka sa uplatňujú na platby iniciované platiteľom bez ohľadu na to, či platiteľ je fyzická osoba alebo právnická osoba.

(8) Platby uskutočnené prostredníctvom anonymných platobných nástrojov vzhľadom na samotnú svoju povahu nepodliehajú povinnosti silnej autentifikácie zákazníka. Ak sa anonymita takýchto nástrojov zruší zo zmluvných alebo z právnych dôvodov, platby podliehajú bezpečnostným požiadavkám, ktoré vyplývajú zo smernice (EÚ) 2015/2366 a z tohto regulačného technického predpisu.

(9) V súlade so smernicou (EÚ) 2015/2366 sa vymedzili výnimky zo zásady silnej autentifikácie zákazníka na základe úrovne rizika, sumy, častosti výskytu a platobného kanála používaného na vykonanie platobnej transakcie.

(10) Kroky, ktoré zahŕňajú prístup k zostatku a nedávnym transakciám platobného účtu bez zverejnenia citlivých platobných údajov, k opakujúcim sa platbám tým istým príjemcom platieb, ktorých platiteľ predtým určil alebo potvrdil uplatnením silnej autentifikácie zákazníka, ako aj k platbám tej istej fyzickej alebo právnickej osobe a platbám od tej istej fyzickej alebo právnickej osoby s účtami u rovnakého poskytovateľa platobných služieb, predstavujú nízku úroveň rizika, čo umožňuje poskytovateľom platobných služieb neuplatňovať silnú autentifikáciu zákazníka. Napriek tomu by poskytovatelia platobných iniciačných služieb, poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu a poskytovatelia služieb informovania o účte mali v súlade s článkami 65, 66 a 67 smernice (EÚ) 2015/2366 od poskytovateľa platobných služieb spravujúceho účet žiadať a získať potrebné a dôležité informácie na poskytovanie danej platobnej služby len so súhlasom používateľa platobných služieb. Takýto súhlas sa môže udeliť jednotlivo pre každú žiadosť o informácie alebo pre každú platbu, ktorá sa má iniciovať, alebo pre poskytovateľov služieb informovania o účte ako oprávnenie na určené platobné účty a súvisiace platobné transakcie, ako sa stanovuje v zmluvnej dohode s používateľom platobných služieb.

(11) Výnimky pre bezkontaktné platby nízkej hodnoty na predajných miestach, pri ktorých sa zohľadňuje aj maximálny počet po sebe nasledujúcich transakcií alebo určitá stanovená maximálna hodnota po sebe nasledujúcich transakcií bez uplatnenia silnej autentifikácie zákazníka, umožňujú vývoj používateľsky ústretových a nízkorizikových platobných služieb, a preto by sa mali poskytovať. Je vhodné stanoviť aj výnimku pre prípad elektronických platobných transakcií, ktoré sa iniciujú na samoobslužných termináloch, pri ktorých nie je vždy jednoduché použiť silnú autentifikáciu zákazníka z prevádzkových dôvodov (napr. s cieľom vyhnúť sa radám a možným nehodám na mýtnych bránach alebo z iných dôvodov týkajúcich sa rizík v oblasti bezpečnosti a ochrany).

(12) Podobne ako v prípade výnimky pre bezkontaktné platby nízkej hodnoty na predajných miestach je potrebné dosiahnuť primeranú rovnováhu medzi záujmom o posilnenie bezpečnosti pri platbách na diaľku a potrebami používateľskej ústretovosti a prístupnosti platieb v oblasti elektronického obchodu. V súlade s týmito zásadami je potrebné obozretným spôsobom zaviesť limity vzťahujúce sa iba na nákupy online s nízkou hodnotou, pri ktorých neprekročení nie je potrebné uplatňovať silnú autentifikáciu zákazníka. Limity pre nákupy online by sa mali stanoviť obozretnejšie vzhľadom na to, že skutočnosť, že osoba nie je pri nákupe fyzicky prítomná, predstavuje mierne vyššie bezpečnostné riziko.

(13) Požiadavky na silnú autentifikáciu zákazníka sa uplatňujú na platby iniciované platiteľom bez ohľadu na to, či platiteľ je fyzická osoba alebo právnická osoba. Mnoho platieb podnikov sa iniciuje prostredníctvom vyhradených procesov alebo protokolov zaručujúcich vysokú úroveň bezpečnosti platieb, ktorej dosiahnutie prostredníctvom silnej autentifikácie zákazníka je cieľom smernice (EÚ) 2015/2366. Ak príslušné orgány zistia, že tie platobné procesy a protokoly, ktoré sú k dispozícii len platiteľom, ktorí nie sú spotrebiteľmi, dosahujú z hľadiska bezpečnosti ciele smernice (EÚ) 2015/2366, poskytovatelia platobných služieb môžu byť v súvislosti s týmito procesmi alebo protokolmi oslobodení od požiadaviek na silnú autentifikáciu zákazníka.

(14) V prípade analýzy rizík transakcií v reálnom čase, pri ktorej sa platobná transakcia kategorizuje ako nízkoriziková, je vhodné zaviesť aj výnimku pre poskytovateľa platobných služieb, ktorý má v úmysle neuplatňovať silnú autentifikáciu zákazníka, pričom prijme účinné požiadavky zohľadňujúce riziká, ktoré zaručujú bezpečnosť finančných prostriedkov a osobných údajov používateľov platobných služieb. Uvedené požiadavky zohľadňujúce riziká by mali spájať výsledky analýzy rizík a potvrdiť, že nebol zistený žiadny neobvyklý výdavok alebo správanie platiteľa, berúc do úvahy ďalšie rizikové faktory vrátane informácií o mieste platiteľa a príjemcu platby s peňažnými limitmi založenými na mierach podvodu vypočítaných pre platby na diaľku. Ak na základe analýzy rizík transakcií v reálnom čase nie je možné platbu kvalifikovať ako nízkorizikovú, poskytovateľ platobných služieb by sa mal vrátiť k silnej autentifikácii zákazníka. Maximálna hodnota takejto výnimky zohľadňujúcej riziká by sa mala stanoviť tak, aby sa zabezpečila veľmi nízka zodpovedajúca miera podvodu, a to aj v porovnaní s mierami podvodu všetkých platobných transakcií poskytovateľa platobných služieb vrátane tých, ktoré boli autentifikované prostredníctvom silnej autentifikácie zákazníka, a to priebežne počas určitého časového obdobia.

(15) Na účely zabezpečenia účinného presadzovania by poskytovatelia platobných služieb, ktorí chcú využívať výnimky z povinnosti silnej autentifikácie zákazníka, mali pravidelne monitorovať a sprístupňovať príslušným orgánom a Európskemu orgánu pre bankovníctvo (EBA) na ich žiadosť každý typ platobnej transakcie, hodnotu podvodných alebo neautorizovaných platobných transakcií a zaznamenané miery podvodu pre všetky ich platobné transakcie, či už sú autentifikované prostredníctvom silnej autentifikácie zákazníka, alebo vykonané na základe príslušnej výnimky.

(16) Zhromažďovanie týchto nových historických údajov o mierach podvodu pri elektronických platobných transakciách prispeje aj k tomu, aby orgán EBA účinne preskúmal limity pre výnimku z povinnosti silnej autentifikácie zákazníka na základe analýzy rizík transakcií v reálnom čase. Orgán EBA by mal v prípade potreby preskúmať a predložiť Komisii návrh aktualizácií týchto regulačných technických predpisov predložením nových návrhov limitov a príslušných mier podvodu s cieľom posilniť bezpečnosť elektronických platieb na diaľku v súlade s článkom 98 ods. 5 smernice (EÚ) 2015/2366 a s článkom 10 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([1]).

(17) Poskytovatelia platobných služieb, ktorí využívajú ktorúkoľvek z výnimiek, ktoré sa majú stanoviť, by mali mať kedykoľvek možnosť rozhodnúť sa pre uplatnenie silnej autentifikácie zákazníka na kroky a platobné transakcie uvedené v uvedených ustanoveniach.

(18) Opatrenia, ktorými sa chráni dôvernosť a integrita personalizovaných bezpečnostných prvkov, ako aj autentifikačné zariadenia a softvér, by mali obmedziť riziká spojené s podvodmi uskutočňovanými prostredníctvom neautorizovaného alebo podvodného použitia platobných nástrojov a neoprávneného prístupu k platobným účtom. Na tento účel je potrebné zaviesť požiadavky na bezpečné vytvorenie a doručenie personalizovaných bezpečnostných prvkov a ich priradenie k používateľovi platobných služieb, ako aj poskytnúť podmienky na obnovenie a deaktiváciu týchto prvkov.

(19) S cieľom zabezpečiť účinnú a bezpečnú komunikáciu medzi príslušnými aktérmi v súvislosti so službami informovania o účte, s platobnými iniciačnými službami a s potvrdením o dostupnosti finančných prostriedkov je potrebné špecifikovať požiadavky na spoločné a bezpečné otvorené komunikačné normy, ktoré musia spĺňať všetci príslušní poskytovatelia platobných služieb. V smernici (EÚ) 2015/2366 sa stanovuje prístup k informáciám o platobnom účte a ich používanie poskytovateľmi služieb informovania o účte. Týmto nariadením sa preto nemenia pravidlá prístupu k iným účtom, ako sú platobné účty.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

(20) Každý poskytovateľ platobných služieb spravujúci účet s platobnými účtami, ktoré sú prístupné online, by mal ponúkať aspoň jedno prístupové rozhranie umožňujúce bezpečnú komunikáciu s poskytovateľmi služieb informovania o účte, poskytovateľmi platobných iniciačných služieb a poskytovateľmi platobných služieb vydávajúcimi platobné nástroje viazané na kartu. Rozhranie by malo poskytovateľom služieb informovania o účte, poskytovateľom platobných iniciačných služieb a poskytovateľom platobných služieb vydávajúcim platobné nástroje viazané na kartu umožňovať, aby sa identifikovali poskytovateľovi platobných služieb spravujúcemu účet. Malo by okrem toho umožňovať poskytovateľom služieb informovania o účte a poskytovateľom platobných iniciačných služieb, aby sa spoliehali na postupy autentifikácie, ktoré poskytovateľ platobných služieb spravujúci účet poskytuje používateľovi platobných služieb. S cieľom zaistiť neutralitu technológií a podnikateľských modelov by poskytovatelia platobných služieb spravujúci účet mali mať možnosť rozhodnúť sa, či ponúknu rozhranie vyhradené na komunikáciu s poskytovateľmi služieb informovania o účte, poskytovateľmi platobných iniciačných služieb a poskytovateľmi platobných služieb vydávajúcimi platobné nástroje viazané na kartu, alebo či na túto komunikáciu umožnia používať rozhranie na identifikáciu a komunikáciu s používateľmi platobných služieb poskytovateľa platobných služieb spravujúceho účet.

(21) S cieľom umožniť poskytovateľom služieb informovania o účte, poskytovateľom platobných iniciačných služieb a poskytovateľom platobných služieb vydávajúcim platobné nástroje viazané na kartu, aby rozvíjali svoje technické riešenia, by sa technická špecifikácia rozhrania mala primerane zdokumentovať a sprístupniť verejnosti. Poskytovateľ platobných služieb spravujúci účet by navyše mal ponúkať zariadenie umožňujúce poskytovateľom platobných služieb skúšať technické riešenia najmenej šesť mesiacov pred začiatkom uplatňovania týchto regulačných predpisov, alebo, ak sa spustenie uskutoční po dátume začiatku uplatňovania týchto regulačných predpisov, pred dňom uvedenia rozhrania na trh. Na zabezpečenie interoperability rôznych technologických komunikačných riešení by rozhranie malo používať komunikačné normy vytvorené medzinárodnými alebo európskymi normalizačnými organizáciami.

(22) Kvalita služieb poskytovaných poskytovateľmi služieb informovania o účte a poskytovateľmi platobných iniciačných služieb bude závisieť od správneho fungovania rozhraní, ktoré zaviedli alebo upravili poskytovatelia platobných služieb spravujúci účet. Preto je dôležité, aby sa v prípade, že tieto rozhrania nie sú v súlade s ustanoveniami uvedenými v týchto predpisoch, prijali opatrenia na zabezpečenie kontinuity činnosti v prospech používateľov týchto služieb. Príslušné vnútroštátne orgány sú zodpovedné za zabezpečenie toho, aby poskytovateľom služieb informovania o účte a poskytovateľom platobných iniciačných služieb nič nebránilo v poskytovaní služieb a aby neboli pri poskytovaní svojich služieb obmedzovaní.

(23) Ak je prístup k platobným účtom ponúkaný prostredníctvom vyhradeného rozhrania, s cieľom zaručiť právo používateľov platobných služieb využívať poskytovateľov platobných iniciačných služieb a služby umožňujúce prístup k informáciám o účte, ako sa stanovuje v smernici (EÚ) 2015/2366, je potrebné vyžadovať, aby vyhradené rozhrania mali rovnakú úroveň dostupnosti a výkonnosti ako rozhranie dostupné používateľovi platobných služieb. Poskytovatelia platobných služieb spravujúci účet by mali vymedziť aj transparentné kľúčové ukazovatele výkonnosti a cieľové úrovne služieb pre dostupnosť a výkonnosť vyhradených rozhraní, ktoré sú prinajmenšom také prísne ako tie, ktoré sú stanovené pre rozhranie používané používateľmi ich platobných služieb. Skúšky týchto rozhraní by mali vykonávať poskytovatelia platobných služieb, ktorí ich budú používať, a tieto rozhrania by mali byť podrobené záťažovej skúške a monitorované príslušnými orgánmi.

(24) Aby sa zabezpečilo, že poskytovatelia platobných služieb, ktorí sa spoliehajú na vyhradené rozhranie, môžu naďalej poskytovať svoje služby v prípade problémov s dostupnosťou alebo nedostatočnou výkonnosťou, je potrebné poskytnúť záložný mechanizmus za prísnych podmienok, ktorý umožní takýmto poskytovateľom používať rozhranie, ktoré poskytovateľ platobných služieb spravujúci účet spravuje na účely identifikácie svojich vlastných používateľov platobných služieb a na komunikáciu s nimi. Určití poskytovatelia platobných služieb spravujúci účet budú oslobodení od povinnosti poskytovať takýto záložný mechanizmus prostredníctvom svojich používateľských rozhraní, ak ich príslušné orgány zistia, že vyhradené rozhrania spĺňajú špecifické podmienky, ktoré zabezpečujú nerušenú hospodársku súťaž. V prípade, že vyhradené rozhrania, ktorým sa udelili výnimky, nebudú spĺňať požadované podmienky, dotknuté príslušné orgány zrušia udelené výnimky.

(25) S cieľom umožniť príslušným orgánom účinne vykonávať dohľad nad vykonávaním a riadením komunikačných rozhraní a monitorovať vykonávanie a riadenie komunikačných rozhraní by poskytovatelia platobných služieb spravujúci účet mali vypracovať zhrnutie príslušnej dokumentácie dostupnej na ich webovom sídle a na požiadanie poskytnúť príslušným orgánom dokumentáciu riešení v prípade núdzových udalostí. Poskytovatelia platobných služieb spravujúci účet by okrem toho mali zverejňovať štatistiky o dostupnosti a výkonnosti tohto rozhrania.

(26) S cieľom chrániť dôvernosť a integritu údajov je potrebné zaručiť bezpečnosť komunikačných relácií medzi poskytovateľmi platobných služieb spravujúcimi účet, poskytovateľmi služieb informovania o účte, poskytovateľmi platobných iniciačných služieb a poskytovateľmi platobných služieb vydávajúcimi platobné nástroje viazané na kartu. Je potrebné vyžadovať najmä to, aby sa pri výmene údajov medzi poskytovateľmi

služieb informovania o účte, poskytovateľmi platobných iniciačných služieb, poskytovateľmi platobných služieb vydávajúcimi platobné nástroje viazané na kartu a poskytovateľmi platobných služieb spravujúcimi účet uplatňovalo bezpečné šifrovanie.

(27) S cieľom zlepšiť dôveru používateľov a zabezpečiť silnú autentifikáciu zákazníka by sa malo zohľadniť použitie prostriedkov elektronickej identifikácie a dôveryhodných služieb, ako sa uvádza v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([1]), najmä pokiaľ ide o oznámené schémy elektronickej identifikácie.

(28) S cieľom zabezpečiť zosúladené dátumy začiatku uplatňovania by sa toto nariadenie malo uplatňovať od toho istého dátumu, od ktorého majú členské štáty zabezpečiť uplatňovanie bezpečnostných opatrení uvedených v článkoch 65, 66, 67 a 97 smernice (EÚ) 2015/2366.

(29) Toto nariadenie vychádza z návrhu regulačných technických predpisov, ktoré Komisii predložil Európsky orgán pre bankovníctvo (EBA).

(30) Orgán EBA vykonal otvorené a transparentné verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzoval možné súvisiace náklady a prínosy a požiadal o stanovisko Skupinu zainteresovaných strán v bankovníctve vytvorenú v súlade s článkom 37 nariadenia (EÚ) č. 1093/2010,

PRIJALA TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

Týmto nariadením sa stanovujú požiadavky, ktoré musia poskytovatelia platobných služieb dodržiavať na účely vykonávania bezpečnostných opatrení, ktoré im umožňujú:

a) uplatňovať postup silnej autentifikácie zákazníka v súlade s článkom 97 smernice (EÚ) 2015/2366;

b) poskytnúť výnimku z uplatňovania bezpečnostných požiadaviek týkajúcich sa silnej autentifikácie zákazníka za vymedzených a obmedzených podmienok na základe úrovne rizika, sumy a častosti výskytu platobnej transakcie a platobného kanála použitého na vykonanie platobnej transakcie;

c) chrániť dôvernosť a integritu personalizovaných bezpečnostných prvkov používateľov platobných služieb;

d) zaviesť spoločné a bezpečné otvorené komunikačné normy na komunikáciu medzi poskytovateľmi platobných služieb spravujúcimi účet, poskytovateľmi platobných iniciačných služieb, poskytovateľmi služieb informovania o účte, platiteľmi, príjemcami platby a inými poskytovateľmi platobných služieb v súvislosti s poskytovaním a používaním platobných služieb v rámci uplatňovania hlavy IV smernice (EÚ) 2015/2366.

Článok 2

Všeobecné požiadavky na autentifikáciu

1. Poskytovatelia platobných služieb majú zavedené mechanizmy monitorovania transakcií, ktoré im umožnia zistiť neautorizované alebo podvodné platobné transakcie na účely vykonávania bezpečnostných opatrení uvedených v článku 1 písm. a) a b).

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 53).

Uvedené mechanizmy sa zakladajú na analýze platobných transakcií pri zohľadnení prvkov, ktoré sú typické pre používateľov platobných služieb za okolností bežného používania personalizovaných bezpečnostných prvkov.

2. Poskytovatelia platobných služieb zabezpečia, aby mechanizmy monitorovania transakcií zohľadňovali prinajmenšom každý z týchto faktorov zohľadňujúcich riziká:

a) zoznamy zneužitých alebo odcudzených autentifikačných prvkov;

b) sumu každej platobnej transakcie;

c) známe scenáre podvodov pri poskytovaní platobných služieb;

d) príznaky napadnutia škodlivým softvérom v jednotlivých krokoch postupu autentifikácie;

e) v prípade, že poskytovateľ platobných služieb poskytuje prístupové zariadenie alebo softvér, záznam o používaní prístupového zariadenia alebo softvéru poskytnutého používateľovi platobných služieb a o neobvyklom používaní prístupového zariadenia alebo softvéru.

Článok 3

Preskúmanie bezpečnostných opatrení

1. Vykonávanie bezpečnostných opatrení uvedených v článku 1 sa musí zdokumentovať, pravidelne skúšať, hodnotiť a podrobovať auditu v súlade s platným právnym rámcom poskytovateľa platobných služieb audítormi s odbornými znalosťami v oblasti bezpečnosti informačných technológií a platieb, ktorí sú z hľadiska svojho pôsobenia nezávislí od poskytovateľa platobných služieb alebo v rámci neho.

2. Obdobie medzi auditmi podľa odseku 1 sa stanoví s prihliadnutím na príslušný rámec auditu účtov a štatutárneho auditu uplatniteľný na poskytovateľa platobných služieb.

Poskytovatelia platobných služieb, ktorí využívajú výnimku uvedenú v článku 18, však podliehajú auditu metodiky, modelu a oznámených mier podvodu najmenej raz ročne. Audítor vykonávajúci tento audit má odborné znalosti v oblasti bezpečnosti informačných technológií a platieb a je z hľadiska svojho pôsobenia nezávislý od poskytovateľa platobných služieb alebo v rámci neho. V prvom roku uplatňovania výnimky podľa článku 18 a následne najmenej každé tri roky, prípadne častejšie na žiadosť príslušného orgánu vykoná tento audit nezávislý a kvalifikovaný externý audítor.

3. V rámci tohto auditu sa predloží hodnotenie a správa o súlade bezpečnostných opatrení poskytovateľa platobných služieb s požiadavkami stanovenými v tomto nariadení.

Celá správa musí byť na požiadanie poskytnutá príslušným orgánom.

KAPITOLA II

BEZPEČNOSTNÉ OPATRENIA NA UPLATŇOVANIE SILNEJ AUTENTIFIKÁCIE ZÁKAZNÍKA

Článok 4

Autentifikačný kód

1. Ak poskytovatelia platobných služieb uplatňujú silnú autentifikáciu zákazníka v súlade s článkom 97 ods. 1 smernice (EÚ) 2015/2366, autentifikácia sa zakladá na dvoch alebo viacerých prvkoch, ktoré sú kategorizované ako poznatok, vlastníctvo a inherencia, pričom výsledkom je vygenerovanie autentifikačného kódu.

Autentifikačný kód je prijatý poskytovateľom platobných služieb iba jedenkrát, keď platiteľ použije autentifikačný kód na prístup k svojmu platobnému účtu online, na iniciovanie elektronickej platobnej transakcie alebo na vykonanie akýchkoľvek krokov prostredníctvom diaľkového prístupu, ktoré môžu predstavovať riziko platobného podvodu alebo iného zneužitia.

2. Na účely odseku 1 poskytovatelia platobných služieb prijmú bezpečnostné opatrenia, ktorými sa zabezpečí splnenie každej z týchto požiadaviek:

a) zo zverejnenia autentifikačného kódu nemožno vyvodiť žiadne informácie o žiadnom z prvkov uvedených v odseku 1;

b) nie je možné vygenerovať nový autentifikačný kód na základe znalosti akéhokoľvek iného predtým vygenerovaného autentifikačného kódu;

c) autentifikačný kód nemožno sfalšovať.

3. Poskytovatelia platobných služieb zabezpečia, aby autentifikácia prostredníctvom vygenerovania autentifikačného kódu zahŕňala každé z týchto opatrení:

a) ak sa autentifikáciou na účely diaľkového prístupu, elektronických platieb na diaľku a akékoľvek iných krokov prostredníctvom diaľkového prístupu, ktoré môžu predstavovať riziko platobného podvodu alebo iného zneužitia, nevygeneroval autentifikačný kód na účely odseku 1, nesmie byť možné určiť, ktoré z prvkov uvedených v uvedenom odseku boli nesprávne;

b) počet neúspešných pokusov o autentifikáciu, ktoré sa môžu uskutočniť po sebe, po ktorom budú kroky uvedené v článku 97 ods. 1 smernice (EÚ) 2015/2366 dočasne alebo trvalo zablokované, nesmie byť v danom časovom období väčší ako päť;

c) komunikačné relácie sú chránené pred zachytávaním autentifikačných údajov prenášaných počas autentifikácie, ako aj pred manipuláciou neautorizovanými stranami v súlade s požiadavkami uvedenými v kapitole V;

d) maximálny čas bez činnosti platiteľa po autentifikácii na účely prístupu k platobnému účtu online nesmie presiahnuť päť minút.

4. Ak je zablokovanie uvedené v odseku 3 písm. b) dočasné, trvanie tohto zablokovania a počet opakovaných pokusov sa stanoví na základe charakteristík služby poskytovanej platiteľovi a všetkých príslušných súvisiacich rizík, so zreteľom prinajmenšom na faktory uvedené v článku 2 ods. 2

Platiteľ musí byť upozornený pred tým, ako sa zablokovanie stane trvalým.

V prípade trvalého zablokovania sa stanoví bezpečný postup umožňujúci platiteľovi opätovné používanie zablokovaných elektronických platobných nástrojov.

Článok 5

Dynamické spájanie

1. Ak poskytovatelia platobných služieb uplatňujú silnú autentifikáciu zákazníka v súlade s článkom 97 ods. 2 smernice (EÚ) 2015/2366 popri požiadavkách článku 4 tohto nariadenia, prijmú aj bezpečnostné opatrenia, ktoré spĺňajú všetky tieto požiadavky:

a) platiteľ je informovaný o sume platobnej transakcie a o príjemcovi platby;

b) vygenerovaný autentifikačný kód je špecifický pre sumu platobnej transakcie a príjemcu platby, ktorých platiteľ odsúhlasil pri iniciovaní transakcie;

c) autentifikačný kód prijatý poskytovateľom platobných služieb zodpovedá pôvodnej špecifickej sume platobnej transakcie a totožnosti príjemcu platby, ktoré platiteľ odsúhlasil;

d) akákoľvek zmena sumy alebo príjemcu platby vedie k zneplatneniu vygenerovaného autentifikačného kódu.

2. Na účely odseku 1 poskytovatelia platobných služieb prijmú bezpečnostné opatrenia, ktorými sa zabezpečí dôvernosť, pravosť a integrita každého z týchto údajov:

a) sumy transakcie a príjemcu platby počas všetkých fáz autentifikácie;

b) informácií zobrazovaných platiteľovi počas všetkých fáz autentifikácie vrátane vygenerovania, prenosu a použitia autentifikačného kódu.

3. Na účely odseku 1 písm. b), a ak poskytovatelia platobných služieb uplatňujú silnú autentifikáciu zákazníka v súlade s článkom 97 ods. 2 smernice (EÚ) 2015/2366, uplatňujú sa tieto požiadavky na autentifikačný kód:

a) v súvislosti s platobnou transakciou viazanou na kartu, v prípade ktorej platiteľ udelil súhlas s presnou sumou finančných prostriedkov, ktoré majú byť zablokované podľa článku 75 ods. 1 uvedenej smernice, autentifikačný kód je špecifický pre sumu, na ktorej zablokovanie platiteľ udelil súhlas a ktorú platiteľ odsúhlasil pri iniciovaní transakcie;

b) v súvislosti s platobnými transakciami, v prípade ktorých platiteľ udelil súhlas s vykonaním skupinových elektronických platobných transakcií na diaľku adresovaných jednému alebo viacerým príjemcom platby, autentifikačný kód je špecifický pre celkovú sumu skupiny platobných transakcií a pre určených príjemcov platby.

Článok 6

Požiadavky na prvky kategorizované ako poznatok

1. Poskytovatelia platobných služieb prijmú opatrenia na zmiernenie rizika, že neautorizované strany odhalia prvky silnej autentifikácie zákazníka kategorizované ako poznatok alebo že im budú tieto prvky sprístupnené.

2. Použitie týchto prvkov platiteľom podlieha opatreniam na zmiernenie rizika s cieľom zabrániť ich sprístupneniu neautorizovaným stranám.

Článok 7

Požiadavky na prvky kategorizované ako vlastníctvo

1. Poskytovatelia platobných služieb prijmú opatrenia na zmiernenie rizika, že prvky silnej autentifikácie zákazníka kategorizované ako vlastníctvo budú použité neautorizovanými stranami.

2. Použitie týchto prvkov platiteľom podlieha opatreniam určeným na zabránenie replikácii prvkov.

Článok 8

Požiadavky na zariadenia a softvér spojené s prvkami kategorizovanými ako inherencia

1. Poskytovatelia platobných služieb prijmú opatrenia na zmiernenie rizika, že prvky autentifikácie kategorizované ako inherencia a prečítané prístupovými zariadeniami a softvérom poskytnutými platiteľovi odhalia neautorizované strany. Poskytovatelia platobných služieb prinajmenšom zaručia, aby pri týchto prístupových zariadeniach a softvéri bola len veľmi malá pravdepodobnosť, že neautorizovaná strana sa autentifikuje ako platiteľ.

2. Použitie týchto prvkov platiteľom podlieha opatreniam, ktorými sa zabezpečí, že tieto zariadenia a softvér zaručujú odolnosť proti neautorizovanému použitiu prvkov prostredníctvom prístupu k zariadeniam a softvéru.

Článok 9

Nezávislosť prvkov

1. Poskytovatelia platobných služieb zaručia, aby použitie prvkov silnej autentifikácie zákazníka, ako sa uvádza v článkoch 6, 7 a 8, podliehalo opatreniam, ktorými sa zabezpečí, že z hľadiska technológie, algoritmov a parametrov porušenie jedného z prvkov neohrozí spoľahlivosť ostatných prvkov.

2. Keď sa prvky silnej autentifikácie zákazníka alebo samotný autentifikačný kód používajú prostredníctvom viacúčelového zariadenia, poskytovatelia platobných služieb prijmú bezpečnostné opatrenia s cieľom zmierniť riziko, ktoré by vyplývalo zo zneužitia tohto viacúčelového zariadenia.

3. Na účely odseku 2 zmierňujúce opatrenia zahŕňajú každý z týchto bodov:

a) používanie oddelených prostredí na bezpečné vykonávanie prostredníctvom softvéru inštalovaného vo viacúčelovom zariadení;

b) mechanizmy na zabezpečenie toho, že platiteľ alebo tretia strana neupravia softvér alebo zariadenie;

c) ak došlo k úpravám, mechanizmy na zmiernenie ich následkov.

KAPITOLA III

VÝNIMKY Z POVINNOSTI SILNEJ AUTENTIFIKÁCIE ZÁKAZNÍKA

Článok 10

Informácie o platobnom účte

1. Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia požiadaviek stanovených v článku 2, so zreteľom na ustanovenia odseku 2 tohto článku a ak je online prístup používateľa platobných služieb obmedzený na jednu z týchto položiek alebo na obe tieto položky bez toho, aby boli zverejnené citlivé údaje o platbe:

a) zostatok na jednom alebo viacerých určených platobných účtoch;

b) platobné transakcie vykonané za uplynulých 90 dní prostredníctvom jedného alebo viacerých určených platobných účtov.

2. Na účely odseku 1 poskytovatelia platobných služieb nie sú oslobodení od uplatňovania silnej autentifikácie zákazníka, ak je splnená niektorá z týchto podmienok:

a) používateľ platobných služieb pristupuje k informáciám uvedeným v odseku 1 online prvýkrát;

b) od posledného prístupu používateľa platobných služieb online k informáciám uvedeným v odseku 1 písm. b) a od uplatnenia silnej autentifikácie zákazníka uplynulo viac ako 90 dní.

Článok 11

Bezkontaktné platby na predajných miestach

Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia požiadaviek stanovených v článku 2, ak platiteľ iniciuje bezkontaktnú elektronickú platobnú transakciu, a to za predpokladu, že sú splnené tieto podmienky:

a) jednotlivá suma bezkontaktnej elektronickej platobnej transakcie nepresahuje sumu 50 EUR a

b) kumulatívna suma predchádzajúcich bezkontaktných elektronických platobných transakcií iniciovaných prostredníctvom platobného nástroja s bezkontaktnou funkciou od dátumu posledného uplatnenia silnej autentifikácie zákazníka nepresahuje 150 EUR, alebo

c) počet po sebe nasledujúcich bezkontaktných elektronických platobných transakcií iniciovaných prostredníctvom platobného nástroja s bezkontaktnou funkciou od posledného uplatnenia silnej autentifikácie zákazníka nie je väčší ako päť.

Článok 12

Samoobslužné terminály na úhradu cestovného a poplatkov za parkovanie

Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia požiadaviek stanovených v článku 2, ak platiteľ iniciuje elektronickú platobnú transakciu na samoobslužnom platobnom termináli na účely úhrady cestovného alebo poplatkov za parkovanie.

Článok 13

Dôveryhodní príjemcovia

1. Poskytovatelia platobných služieb uplatňujú silnú autentifikáciu zákazníka, ak platiteľ vytvorí alebo zmení zoznam dôveryhodných príjemcov prostredníctvom poskytovateľa platobných služieb spravujúceho účet platiteľa.

2. Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia všeobecných požiadaviek na autentifikáciu, ak platiteľ iniciuje platobnú transakciu a príjemca platby je zahrnutý do zoznamu dôveryhodných príjemcov, ktorý platiteľ predtým vytvoril.

Článok 14

Opakujúce sa transakcie

1. Poskytovatelia platobných služieb uplatňujú silnú autentifikáciu zákazníka, ak platiteľ prvýkrát vytvorí, zmení alebo iniciuje sériu opakujúcich sa transakcií s rovnakou sumou a s rovnakým príjemcom platby.

2. Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia všeobecných požiadaviek na autentifikáciu na iniciovanie všetkých následných platobných transakcií zahrnutých do série platobných transakcií uvedených v odseku 1.

Článok 15

Úhrady medzi účtami, ktoré vlastní tá istá fyzická alebo právnická osoba

Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka pod podmienkou splnenia požiadaviek stanovených v článku 2, ak platiteľ iniciuje úhradu, pričom platiteľ a príjemca platby sú tou istou fyzickou alebo právnickou osobou a oba platobné účty vedie ten istý poskytovateľ platobných služieb spravujúci účet.

Článok 16

Transakcie nízkej hodnoty

Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka, ak platiteľ iniciuje elektronickú platobnú transakciu na diaľku, a to za predpokladu, že sú splnené tieto podmienky:

a) suma elektronickej platobnej transakcie na diaľku nepresahuje 30 EUR a

b) kumulatívna suma predchádzajúcich elektronických platobných transakcií na diaľku iniciovaných platiteľom od posledného uplatnenia silnej autentifikácie zákazníka nepresahuje 100 EUR, alebo

c) počet predchádzajúcich elektronických platobných transakcií na diaľku iniciovaných platiteľom od posledného uplatnenia silnej autentifikácie zákazníka nepresahuje päť po sebe nasledujúcich jednotlivých elektronických platobných transakcií na diaľku.

Článok 17

Bezpečné platobné procesy a protokoly pre podniky

Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka, pokiaľ ide o právnické osoby iniciujúce elektronické platobné transakcie prostredníctvom použitia vyhradených platobných procesov alebo protokolov, ktoré sú k dispozícii len platiteľom, ktorí nie sú spotrebiteľmi, ak sú príslušné orgány presvedčené, že uvedené procesy alebo protokoly zaručujú úroveň bezpečnosti prinajmenšom rovnocennú s úrovňou, ktorá sa stanovuje v smernici (EÚ) 2015/2366.

Článok 18

Analýza rizík transakcií

1. Poskytovatelia platobných služieb majú možnosť neuplatňovať silnú autentifikáciu zákazníka, ak platiteľ iniciuje elektronickú platobnú transakciu na diaľku označenú poskytovateľom platobných služieb za nízkorizikovú podľa mechanizmov monitorovania transakcií uvedených v článku 2 a v odseku 2 písm. c) tohto článku.

2. Elektronická platobná transakcia uvedená v odseku 1 sa považuje za nízkorizikovú, ak sú splnené všetky tieto podmienky:

a) miera podvodu pre tento typ transakcie, oznámená poskytovateľom platobných služieb a vypočítaná v súlade s článkom 19, je rovná referenčným mieram podvodu uvedeným v tabuľke uvedenej v prílohe pre „elektronické platby na diaľku viazané na kartu“, resp. „elektronické úhrady na diaľku“ alebo nižšia ako tieto referenčné miery;

b) suma transakcie nepresahuje príslušnú hodnotu limitu na výnimku uvedenú v tabuľke uvedenej v prílohe;

c) poskytovatelia platobných služieb nezistili v dôsledku vykonania analýzy rizík v reálnom čase žiadny z týchto javov:

   i) neobvyklé výdavky alebo správanie platiteľa;

   ii) nezvyčajné informácie o prístupe platiteľa k zariadeniu/softvéru;

   iii) napadnutie škodlivým softvérom v niektorom kroku postupu autentifikácie;

   iv) známy scenár podvodu pri poskytovaní platobných služieb;

   v) neobvyklé miesto platiteľa;

   vi) vysokorizikové miesto príjemcu platby.

3. Poskytovatelia platobných služieb, ktorí majú v úmysle oslobodiť elektronické platobné transakcie od povinnosti silnej autentifikácie zákazníka z dôvodu, že predstavujú nízke riziko, zohľadnia prinajmenšom tieto faktory zohľadňujúce riziká:

a) zvyčajné predchádzajúce výdavky jednotlivých používateľov platobných služieb;

b) históriu platobných transakcií každého z používateľov platobných služieb poskytovateľa platobných služieb;

c) miesto platiteľa a miesto príjemcu platby v čase uskutočnenia transakcie v prípadoch, keď poskytovateľ platobných služieb poskytne prístupové zariadenie alebo softvér;

d) identifikácia neobvyklých platieb používateľa platobných služieb v súvislosti s históriou platobných transakcií používateľa.

V posúdení vykonanom poskytovateľom platobných služieb sa všetky uvedené faktory zohľadňujúce riziká spoja do rizikového skóre pre každú jednotlivú transakciu s cieľom určiť, či by sa konkrétna platba mala povoliť bez silnej autentifikácie zákazníka.

Článok 19

Výpočet mier podvodu

1. Pre každý typ transakcie uvedený v tabuľke uvedenej v prílohe poskytovateľ platobných služieb zabezpečí, aby celkové miery podvodu týkajúce sa platobných transakcií autentifikovaných prostredníctvom silnej autentifikácie zákazníka, ako aj transakcií vykonaných na základe ktorejkoľvek z výnimiek uvedených v článkoch 13 až 18 boli rovné referenčnej miere podvodu pre ten istý typ platobnej transakcie uvedenej v tabuľke v prílohe alebo nižšie.

Celková miera podvodu pre každý typ transakcie sa vypočíta ako celková hodnota neautorizovaných alebo podvodných transakcií na diaľku bez ohľadu na to, či sa finančné prostriedky získali späť alebo nie, vydelená celkovou hodnotou všetkých transakcií na diaľku pre ten istý typ transakcií, či už autentifikovaných uplatnením silnej autentifikácie zákazníka, alebo vykonaných na základe ktorejkoľvek z výnimiek uvedených v článkoch 13 až 18 na priebežnom štvrťročnom základe (90 dní).

2. Výpočet mier podvodu a výsledné hodnoty sa posúdia audítorským preskúmaním uvedeným v článku 3 ods. 2, čo zabezpečí ich úplnosť a presnosť.

3. Metodika a akýkoľvek model, ktorý používa poskytovateľ platobných služieb na výpočet mier podvodu, ako aj samotné miery podvodu sa náležite zdokumentujú a plne sprístupnia príslušným orgánom a orgánu EBA po predchádzajúcom oznámení dotknutému príslušnému orgánu, resp. orgánom, a to na jeho/ich žiadosť.

Článok 20

Ukončenie výnimiek na základe analýzy rizík transakcií

1. Poskytovatelia platobných služieb, ktorí využívajú výnimku uvedenú v článku 18, bezodkladne oznámia príslušným orgánom, ak jedna z ich monitorovaných mier podvodu pre akýkoľvek typ platobných transakcií v tabuľke v prílohe presahuje príslušnú referenčnú mieru podvodu, a poskytnú príslušným orgánom opis opatrení, ktoré plánujú prijať s cieľom obnoviť súlad ich monitorovanej miery podvodu s príslušnými referenčnými mierami podvodu.

2. Poskytovatelia platobných služieb bezodkladne prestanú využívať výnimku uvedenú v článku 18 pre akýkoľvek typ platobnej transakcie uvedený v tabuľke v prílohe v špecifickom rozsahu limitu na výnimku, ak ich monitorovaná miera podvodu počas dvoch po sebe nasledujúcich štvrťrokov presahuje referenčnú mieru podvodu uplatniteľnú pre daný platobný nástroj alebo typ platobnej transakcie v rámci daného rozsahu limitu na výnimku.

3. Po ukončení výnimky uvedenej v článku 18 v súlade s odsekom 2 tohto článku poskytovatelia platobných služieb nemôžu túto výnimku opäť využívať, až kým ich vypočítaná miera podvodu nebude počas jedného štvrťroka rovná referenčným mieram podvodu uplatniteľným pre daný typ platobnej transakcie v rámci daného rozsahu limitu na výnimku alebo nižšia ako referenčné miery podvodu uplatniteľné pre daný typ platobnej transakcie v rámci daného rozsahu limitu na výnimku.

4. Ak poskytovatelia platobných služieb plánujú opäť využívať výnimku uvedenú v článku 18, oznámia to príslušným orgánom v primeranej časovej lehote a pred opätovným využívaním výnimky poskytnú dôkazy o obnovení súladu monitorovanej miery podvodu s uplatniteľnou referenčnou mierou podvodu pre daný rozsahu limitu na výnimku v súlade s odsekom 3 tohto článku.

Článok 21

Monitorovanie

1. S cieľom využívať výnimky stanovené v článkoch 10 až 18 poskytovatelia platobných služieb zaznamenávajú a monitorujú pre každý typ platobných transakcií s rozpisom pre platobné transakcie na diaľku a pre platobné transakcie, ktoré sa nevykonávajú na diaľku, a to najmenej štvrťročne, tieto údaje:

a) celkovú hodnotu neautorizovaných alebo podvodných platobných transakcií v súlade s článkom 64 ods. 2 smernice (EÚ) 2015/2366, celkovú hodnotu všetkých platobných transakcií a výslednú mieru podvodu vrátane rozpisu platobných transakcií iniciovaných prostredníctvom silnej autentifikácie zákazníka a na základe jednotlivých výnimiek;

b) priemernú hodnotu transakcie vrátane rozpisu platobných transakcií iniciovaných prostredníctvom silnej autentifikácie zákazníka a na základe jednotlivých výnimiek;

c) počet platobných transakcií, pri ktorých sa uplatnili jednotlivé výnimky, a ich percentuálny podiel na celkovom počte platobných transakcií.

2. Poskytovatelia platobných služieb v súlade s odsekom 1 sprístupnia výsledky monitorovania príslušným orgánom a orgánu EBA po predchádzajúcom oznámení dotknutému príslušnému orgánu, resp. orgánom, a to na jeho/ich žiadosť.

KAPITOLA IV

DÔVERNOSŤ A INTEGRITA PERSONALIZOVANÝCH BEZPEČNOSTNÝCH PRVKOV POUŽÍVATEĽOV PLATOBNÝCH SLUŽIEB

Článok 22

Všeobecné požiadavky

1. Poskytovatelia platobných služieb zabezpečia dôvernosť a integritu personalizovaných bezpečnostných prvkov používateľov platobných služieb vrátane autentifikačných kódov počas všetkých fáz autentifikácie.

2. Na účely odseku 1 poskytovatelia platobných služieb zabezpečia, aby bola splnená každá z týchto požiadaviek:

a) personalizované bezpečnostné prvky sú pri zobrazení skryté a pri zadávaní používateľom platobných služieb počas autentifikácie nie sú v plnom rozsahu čitateľné;

b) personalizované bezpečnostné prvky v dátovom formáte, ako aj kryptografické materiály súvisiace so šifrovaním personalizovaných bezpečnostných prvkov sa neukladajú v nešifrovanom textovom formáte;

c) tajný kryptografický materiál je chránený pred neoprávneným zverejnením.

3. Poskytovatelia platobných služieb plne zdokumentujú proces týkajúci sa správy kryptografického materiálu používaného na šifrovanie personalizovaných bezpečnostných prvkov alebo na iný spôsob zabezpečenia nečitateľnosti personalizovaných bezpečnostných prvkov.

4. Poskytovatelia platobných služieb zabezpečia, aby sa spracovanie a smerovanie personalizovaných bezpečnostných prvkov a autentifikačných kódov vygenerovaných v súlade s kapitolou II uskutočňovalo v bezpečnom prostredí v súlade so silnými a všeobecne uznávanými odvetvovými normami.

Článok 23

Vytvorenie a prenos bezpečnostných prvkov

Poskytovatelia platobných služieb zabezpečia, aby sa vytvorenie personalizovaných bezpečnostných prvkov vykonávalo v bezpečnom prostredí.

Zmierňujú riziká neautorizovaného použitia personalizovaných bezpečnostných prvkov a autentifikačných zariadení a softvéru po ich strate, odcudzení alebo kopírovaní pred ich doručením platiteľovi.

Článok 24

Priradenie k používateľovi platobných služieb

1. Poskytovatelia platobných služieb zabezpečia, aby bol k personalizovaným bezpečnostným prvkom, autentifikačným zariadeniam a softvérom bezpečným spôsobom priradený iba používateľ platobných služieb.

2. Na účely odseku 1 poskytovatelia platobných služieb zabezpečia, aby bola splnená každá z týchto požiadaviek:

a) priradenie totožnosti používateľa platobných služieb k personalizovaným bezpečnostným prvkom, autentifikačným zariadeniam a softvérom sa vykonáva v bezpečných prostrediach, za ktoré zodpovedá poskytovateľ platobných služieb a ktoré pozostávajú prinajmenšom z priestorov poskytovateľa platobných služieb, internetového prostredia poskytovaného poskytovateľom platobných služieb alebo iných bezpečných webových sídiel, ktoré používa poskytovateľ platobných služieb a jeho služby bankomatov, a to pri zohľadnení rizík spojených so zariadeniami a základnými zložkami používanými v procese priraďovania, za ktoré nezodpovedá poskytovateľ platobných služieb;

b) priradenie totožnosti používateľa platobných služieb k personalizovaným bezpečnostným prvkom a autentifikačným zariadeniam alebo softvérom prostredníctvom diaľkového prístupu sa vykonáva s použitím silnej autentifikácie zákazníka.

Článok 25

Doručovanie bezpečnostných prvkov, autentifikačných zariadení a softvéru

1. Poskytovatelia platobných služieb zabezpečia, aby sa doručenie personalizovaných bezpečnostných prvkov, autentifikačných zariadení a softvéru používateľovi platobných služieb vykonávalo bezpečným spôsobom s cieľom riešiť riziká súvisiace s ich neautorizovaným použitím v dôsledku ich straty, odcudzenia alebo kopírovania.

2. Na účely odseku 1 poskytovatelia platobných služieb uplatňujú prinajmenšom všetky tieto požiadavky:

a) účinné a bezpečné mechanizmy doručenia, ktorými sa zabezpečí doručenie personalizovaných bezpečnostných prvkov, autentifikačných zariadení a softvéru legitímnemu používateľovi platobných služieb;

b) mechanizmy, ktoré umožňujú poskytovateľovi platobných služieb overiť pravosť autentifikačného softvéru doručeného používateľovi platobných služieb prostredníctvom internetu;

c) keď sa doručenie personalizovaných bezpečnostných prvkov vykoná mimo priestorov poskytovateľa platobných služieb alebo prostredníctvom diaľkového prístupu, opatrenia, ktorými sa zabezpečí:

   i) aby žiadna neautorizovaná strana nemohla získať viac ako jeden prvok personalizovaných bezpečnostných prvkov, autentifikačných zariadení alebo softvéru, ak sú doručované cez ten istý kanál;

   ii) aby si doručené personalizované bezpečnostné prvky, autentifikačné zariadenia alebo softvér pred použitím vyžadovali aktiváciu;

d) opatrenia, ktorými sa zabezpečí, že keď personalizované bezpečnostné prvky, autentifikačné zariadenia alebo softvér musia byť pred ich prvým použitím aktivované, aby aktivácia prebehla v bezpečnom prostredí v súlade s postupmi priraďovania uvedenými v článku 24.

Článok 26

Obnovenie personalizovaných bezpečnostných prvkov

Poskytovatelia platobných služieb zabezpečia, aby sa pri obnovovaní alebo opätovnej aktivácii personalizovaných bezpečnostných prvkov dodržiavali postupy na vytváranie, priraďovanie a doručovanie prvkov a autentifikačných zariadení v súlade s článkami 23, 24 a 25.

Článok 27

Zničenie, deaktivácia a zrušenie

Poskytovatelia platobných služieb zabezpečia, aby mali zavedené účinné postupy na uplatňovanie každého z týchto bezpečnostných opatrení:

a) bezpečné zničenie, deaktivácia alebo zrušenie personalizovaných bezpečnostných prvkov, autentifikačných zariadení a softvéru;

b) ak poskytovateľ platobných služieb distribuuje opätovne použiteľné autentifikačné zariadenia a softvér, pred sprístupnením zariadenia alebo softvéru inému používateľovi platobných služieb sa zaručí, zdokumentuje a vykoná ich bezpečné opätovné použitie;

c) deaktivácia alebo zrušenie informácií týkajúcich sa personalizovaných bezpečnostných prvkov uchovávaných v systémoch a databázach poskytovateľa platobných služieb a v prípade potreby aj vo verejných archívoch.

KAPITOLA V

SPOLOČNÉ A BEZPEČNÉ OTVORENÉ KOMUNIKAČNÉ NORMY

Oddiel 1

Všeobecné požiadavky na komunikáciu

Článok 28

Požiadavky na identifikáciu

1. Poskytovatelia platobných služieb zaručia bezpečnú identifikáciu pri komunikácii medzi zariadením platiteľa a akceptačnými zariadeniami príjemcu platby určenými na elektronické platby okrem iného vrátane platobných terminálov.

2. Poskytovatelia platobných služieb zabezpečia, aby sa účinne zmiernili riziká súvisiace s chybným presmerovaním komunikácie na neautorizované strany v mobilných aplikáciách a iných rozhraniach používateľov platobných služieb ponúkajúcich elektronické platobné služby.

Článok 29

Vysledovateľnosť

1. Poskytovatelia platobných služieb musia mať zavedené postupy, ktoré zaručia, že všetky platobné transakcie a iné interakcie s používateľom platobných služieb, s inými poskytovateľmi platobných služieb a s inými subjektmi vrátane obchodníkov v súvislosti s poskytovaním platobných služieb sú vysledovateľné, čím sa zabezpečí vedomosť *ex post* o všetkých udalostiach, ktoré sú relevantné pre elektronickú transakciu vo všetkých jednotlivých fázach.

2. Na účely odseku 1 poskytovatelia platobných služieb zabezpečia, aby sa všetky komunikačné relácie prebiehajúce s používateľom platobných služieb, inými poskytovateľmi platobných služieb a inými subjektmi vrátane obchodníkov spoliehali na všetky tieto prvky:

a) jedinečný identifikátor relácie;

b) bezpečnostné mechanizmy na podrobné zaznamenávanie transakcie vrátane čísla transakcie, časových pečiatok a všetkých relevantných údajov o transakcii;

c) časové pečiatky, ktoré sa zakladajú na jednotnom časovom referenčnom systéme a ktoré sa synchronizujú podľa oficiálneho časového signálu.

Oddiel 2

Osobitné požiadavky na spoločné a bezpečné otvorené komunikačné normy

Článok 30

Všeobecné povinnosti pre prístupové rozhrania

1. Poskytovatelia platobných služieb spravujúci účet, ktorí platiteľovi ponúkajú platobný účet, ktorý je prístupný online, majú zavedené aspoň jedno rozhranie, ktoré spĺňa všetky tieto požiadavky:

a) poskytovatelia služieb informovania o účte, poskytovatelia platobných iniciačných služieb a poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu sú schopní sa identifikovať voči poskytovateľovi platobných služieb spravujúcemu účet;

b) poskytovatelia služieb informovania o účte sú schopní bezpečne komunikovať s cieľom požiadať o informácie o jednom alebo viacerých určených platobných účtoch a súvisiacich platobných transakciách a získať tieto informácie;

c) poskytovatelia platobných iniciačných služieb sú schopní bezpečne komunikovať s cieľom iniciovať platobný príkaz z platobného účtu platiteľa a získať všetky informácie o iniciovaní platobnej transakcie a všetky informácie, ktoré sú prístupné poskytovateľom platobných služieb spravujúcim účet, pokiaľ ide o vykonanie platobnej transakcie.

2. Na účely autentifikácie používateľa platobných služieb rozhranie uvedené v odseku 1 umožní poskytovateľom služieb informovania o účte a poskytovateľom platobných iniciačných služieb, aby sa spoliehali na všetky postupy autentifikácie, ktoré poskytuje poskytovateľ platobných služieb spravujúci účet používateľovi platobných služieb.

Rozhranie spĺňa prinajmenšom všetky tieto požiadavky:

a) poskytovateľ platobných iniciačných služieb alebo poskytovateľ služieb informovania o účte sú schopní dať pokyn poskytovateľovi platobných služieb spravujúcemu účet, aby začal autentifikáciu na základe súhlasu používateľa platobných služieb;

b) komunikačné relácie medzi poskytovateľom platobných služieb spravujúcim účet, poskytovateľom služieb informovania o účte, poskytovateľom platobných iniciačných služieb a akýmkoľvek príslušným používateľom platobných služieb sa vytvoria a udržiavajú počas celej autentifikácie;

c) zabezpečí sa integrita a dôvernosť personalizovaných bezpečnostných prvkov a autentifikačných kódov prenášaných poskytovateľom platobných iniciačných služieb alebo prostredníctvom neho alebo poskytovateľom služieb informovania o účte alebo prostredníctvom neho.

3. Poskytovatelia platobných služieb spravujúci účet zabezpečia, aby ich rozhrania dodržiavali komunikačné normy, ktoré vydávajú medzinárodné alebo európske normalizačné organizácie.

Poskytovatelia platobných služieb spravujúci účet takisto zabezpečia, aby sa zdokumentovala technická špecifikácia všetkých rozhraní, pričom sa uvedie súbor bežných postupov, protokolov a nástrojov, ktoré potrebujú poskytovatelia platobných iniciačných služieb, poskytovatelia služieb informovania o účte a poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu, aby umožnili interoperabilitu svojho softvéru a aplikácií so systémami poskytovateľov platobných služieb spravujúcich účet.

Najmenej šesť mesiacov pred dátumom začiatku uplatňovania uvedeným v článku 38 ods. 2 alebo pred cieľovým dátumom uvedenia prístupového rozhrania na trh, keď sa uvedenie uskutoční po dátume uvedenom v článku 38 ods. 2, poskytovatelia platobných služieb spravujúci účet prinajmenšom sprístupnia dokumentáciu, a to bezodplatne a na žiadosť autorizovaných poskytovateľov platobných iniciačných služieb, poskytovateľov služieb informovania o účte a poskytovateľov platobných služieb vydávajúcich platobné nástroje viazané na kartu alebo poskytovateľov platobných služieb, ktorí požiadali svoje príslušné orgány o príslušné povolenie, a súhrn dokumentácie zverejnia na svojom webovom sídle.

4. Okrem odseku 3 poskytovatelia platobných služieb spravujúci účet zabezpečia, aby akékoľvek zmeny v technickej špecifikácii ich rozhrania, s výnimkou núdzových situácií, boli sprístupnené oprávneným poskytovateľom platobných iniciačných služieb, poskytovateľom služieb informovania o účte a poskytovateľom platobných služieb vydávajúcim platobné nástroje viazané na kartu, alebo poskytovateľom platobných služieb, ktorí požiadali svoje príslušné orgány o príslušné povolenie, a to v čo najskoršom predstihu a najmenej 3 mesiace pred vykonaním zmeny.

Poskytovatelia platobných služieb zdokumentujú núdzové situácie, pri ktorých sa vykonali zmeny, a na požiadanie sprístupnia dokumentáciu príslušným orgánom.

5. Poskytovatelia platobných služieb spravujúci účet sprístupnia skúšobné zariadenie, ako aj podporu, na pripojenie a funkčné skúšanie, aby oprávnení poskytovatelia platobných iniciačných služieb, poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu a poskytovatelia služieb informovania o účte, alebo poskytovatelia platobných služieb, ktorí požiadali svoje príslušné orgány o príslušné povolenie, mohli skúšať ich softvér a aplikácie používané na ponúkanie platobných služieb používateľom. Toto skúšobné zariadenie by sa malo sprístupniť najneskôr šesť mesiacov pred dátumom začiatku uplatňovania uvedeným v článku 38 ods. 2 alebo pred cieľovým dátumom uvedenia prístupového rozhrania na trh, keď sa uvedenie uskutoční po dátume uvedenom v článku 38 ods. 2

Prostredníctvom skúšobného zariadenia sa však nevymieňajú žiadne citlivé informácie.

6. Príslušné orgány zabezpečia, aby poskytovatelia platobných služieb spravujúci účet vždy dodržiavali povinnosti obsiahnuté v týchto predpisoch v súvislosti s rozhraním, resp. rozhraniami, ktoré zaviedli. V prípade, že poskytovateľ platobných služieb spravujúci účet nedodrží požiadavky na rozhrania stanovené v týchto predpisoch, príslušné orgány zabezpečia, aby poskytovanie platobných iniciačných služieb a služieb informovania o účte nebolo prerušené alebo aby sa mu nebránilo, pokiaľ príslušní poskytovatelia takýchto služieb spĺňajú podmienky vymedzené v článku 33 ods. 5

Článok 31

Možnosti prístupového rozhrania

Poskytovatelia platobných služieb spravujúci účet vytvoria rozhranie, resp. rozhrania uvedené v článku 30 prostredníctvom vyhradeného rozhrania alebo tým, že poskytovateľom platobných služieb uvedeným v článku 30 ods. 1 umožnia použitie rozhraní na autentifikáciu a komunikáciu s používateľmi platobných služieb poskytovateľa platobných služieb spravujúceho účet.

Článok 32

Povinnosti pre vyhradené rozhranie

1. S výhradou súladu s článkami 30 a 31 poskytovatelia platobných služieb spravujúci účet, ktorí zaviedli vyhradené rozhranie, zabezpečia, aby vyhradené rozhranie vždy poskytovalo rovnakú úroveň dostupnosti a výkonnosti, ako aj podpory, ako rozhrania sprístupnené používateľovi platobných služieb na priamy prístup k jeho platobnému účtu online.

2. Poskytovatelia platobných služieb spravujúci účet, ktorí zaviedli vyhradené rozhranie, vymedzia transparentné kľúčové ukazovatele výkonnosti a cieľové úrovne služieb, ktoré sú prinajmenšom také prísne ako tie, ktoré sú stanovené pre rozhranie používané ich používateľmi platobných služieb, pokiaľ ide o dostupnosť aj poskytnuté údaje v súlade s článkom 36. Tieto rozhrania, ukazovatele a ciele sú monitorované príslušnými orgánmi a podrobené záťažovej skúške.

3. Poskytovatelia platobných služieb spravujúci účet, ktorí zaviedli vyhradené rozhranie, zabezpečia, aby toto rozhranie nevytváralo prekážky v poskytovaní platobných iniciačných služieb a služieb informovania o účte. Takéto prekážky môžu okrem iného zahŕňať bránenie tomu, aby poskytovatelia platobných služieb uvedení v článku 30 ods. 1 používali bezpečnostné prvky, ktoré vydali poskytovatelia platobných služieb spravujúci účet svojim zákazníkom, uloženie povinného presmerovania na autentifikáciu alebo iné funkcie poskytovateľa platobných služieb spravujúceho účet, vyžadovanie dodatočných povolení a registrácií okrem tých, ktoré sa stanovujú v článkoch 11, 14 a 15 smernice (EÚ) 2015/2366, alebo vyžadovanie dodatočných kontrol súhlasu, ktorý udelili používatelia platobných služieb poskytovateľom platobných iniciačných služieb a služieb informovania o účte.

4. Na účely odsekov 1 a 2 poskytovatelia platobných služieb spravujúci účet monitorujú dostupnosť a výkonnosť vyhradeného rozhrania. Poskytovatelia platobných služieb spravujúci účet zverejňujú na svojom webovom sídle štvrťročné štatistiky o dostupnosti a výkonnosti vyhradeného rozhrania a rozhrania, ktoré používajú ich používatelia platobných služieb.

Článok 33

Opatrenia pre prípad nepredvídaných udalostí pre vyhradené rozhranie

1. Pre prípad, že rozhranie nefunguje v súlade s článkom 32, že sa vyskytne neplánovaná nedostupnosť rozhrania a že nastane porucha systémov, poskytovatelia platobných služieb spravujúci účet zahrnú pri navrhovaní vyhradeného rozhrania stratégiu a plány pre opatrenia pre prípad nepredvídaných udalostí. Možno predpokladať, že k neplánovanej nedostupnosti alebo poruche systémov dôjde, ak päť po sebe nasledujúcich žiadostí o prístup k informáciám na poskytnutie platobných iniciačných služieb a služieb informovania o účte nie je zodpovedaných do 30 sekúnd.

2. Opatrenia pre prípad nepredvídaných udalostí zahŕňajú komunikačné plány na informovanie poskytovateľov platobných služieb využívajúcich vyhradené rozhranie o opatreniach na obnovu systému a opis okamžite dostupných alternatívnych možností, ktoré poskytovatelia platobných služieb môžu mať počas tohto obdobia k dispozícii.

3. Poskytovateľ platobných služieb spravujúci účet, ako aj poskytovatelia platobných služieb uvedení v článku 30 ods. 1 bezodkladne oznámia problémy s vyhradenými rozhraniami tak, ako sa opisuje v odseku 1, svojim príslušným vnútroštátnym orgánom.

4. V rámci mechanizmu pre prípad nepredvídaných udalostí môžu poskytovatelia platobných služieb uvedení v článku 30 ods. 1 využívať rozhrania sprístupnené používateľom platobných služieb na účely autentifikácie a komunikácie so svojím poskytovateľom platobných služieb spravujúcim účet, a to až kým vyhradené rozhranie nie je obnovené na úroveň dostupnosti a výkonnosti, ako sa stanovuje v článku 32.

5. Na tento účel poskytovatelia platobných služieb spravujúci účet zabezpečia, aby sa poskytovatelia platobných služieb uvedení v článku 30 ods. 1 mohli identifikovať a spoliehať sa na postupy autentifikácie, ktoré poskytovateľ platobných služieb spravujúci účet poskytuje používateľovi platobných služieb. Ak poskytovatelia platobných služieb uvedení v článku 30 ods. 1 využívajú rozhranie uvedené v odseku 4:

a) prijmú potrebné opatrenia, aby zabezpečili, že nebudú pristupovať k údajom, ukladať ani spracúvať údaje na iné účely ako poskytovanie služby požadovanej používateľom platobných služieb;

b) naďalej spĺňajú povinnosti vyplývajúce z článku 66 ods. 3, resp. článku 67 ods. 2 smernice (EÚ) 2015/2366;

c) zaznamenávajú údaje, ku ktorým sa pristupuje prostredníctvom rozhrania prevádzkovaného poskytovateľom platobných služieb spravujúcim účet pre jeho používateľov platobných služieb, a na požiadanie a bez zbytočného odkladu poskytnú zaznamenané súbory svojmu príslušnému vnútroštátnemu orgánu;

d) na požiadanie a bez zbytočného odkladu riadne odôvodnia svojmu príslušnému vnútroštátnemu orgánu použitie rozhrania sprístupneného pre používateľov platobných služieb na priamy prístup k ich platobnému účtu online;

e) zodpovedajúcim spôsobom informujú poskytovateľa platobných služieb spravujúceho účet.

6. Príslušné orgány po konzultácii s orgánom EBA na zabezpečenie jednotného uplatňovania nasledujúcich podmienok oslobodia poskytovateľov platobných služieb spravujúcich účet, ktorí sa rozhodli pre vyhradené rozhranie, od povinnosti zaviesť mechanizmus pre prípad nepredvídaných udalostí opísaný v odseku 4, ak vyhradené rozhranie spĺňa všetky tieto podmienky:

a) spĺňa všetky povinnosti týkajúce sa vyhradených rozhraní, ako sa uvádza v článku 32;

b) bolo navrhnuté a skúšané v súlade s článkom 30 ods. 5 k spokojnosti poskytovateľov platobných služieb uvedených v uvedenom článku;

c) bolo najmenej tri mesiace intenzívne používané poskytovateľmi platobných služieb na poskytovanie služieb informovania o účte, platobných iniciačných služieb a na poskytovanie potvrdenia o dostupnosti finančných prostriedkov pre platby viazané na kartu;

d) prípadný problém súvisiaci s vyhradeným rozhraním bol vyriešený bez zbytočného odkladu.

7. Príslušné orgány zrušia výnimku uvedenú v odseku 6, ak poskytovatelia platobných služieb spravujúci účet nespĺňajú podmienky v písmenách a) a d) počas viac ako dvoch po sebe nasledujúcich kalendárnych týždňov. Príslušné orgány o tomto zrušení informujú orgán EBA a zabezpečia, aby poskytovateľ platobných služieb spravujúci účet zaviedol mechanizmus pre prípad nepredvídaných udalostí uvedený v odseku 4, a to v čo najkratšom možnom čase, najneskôr však do dvoch mesiacov.

Článok 34

Certifikáty

1. Na účely identifikácie podľa článku 30 ods. 1 písm. a) sa poskytovatelia platobných služieb spoliehajú na kvalifikované certifikáty pre elektronické pečate, ako sa uvádza v článku 3 bode 30 nariadenia (EÚ) č. 910/2014, alebo pre autentifikáciu webového sídla, ako sa uvádza v článku 3 bode 39 uvedeného nariadenia.

2. Na účely tohto nariadenia je registračným číslom uvedeným v úradných záznamoch v súlade s písmenom c) prílohy III alebo písmenom c) prílohy IV k nariadeniu (EÚ) č. 910/2014 číslo povolenia poskytovateľa platobných služieb vydávajúceho platobné nástroje viazané na kartu, poskytovateľov služieb informovania o účte a poskytovateľov platobných iniciačných služieb vrátane poskytovateľov platobných služieb spravujúcich účet poskytujúcich takéto služby, ktoré je k dispozícii vo verejnom registri domovského členského štátu podľa článku 14 smernice (EÚ) 2015/2366 alebo ktoré vyplýva z oznámení o každom povolení udelenom podľa článku 8 smernice Európskeho parlamentu a Rady 2013/36/EÚ ([1]) v súlade s článkom 20 uvedenej smernice.

3. Na účely tohto nariadenia kvalifikované certifikáty pre elektronické pečate alebo pre autentifikáciu webového sídla uvedené v odseku 1 zahŕňajú v jazyku, ktorý sa obvykle používa v oblasti medzinárodných financií, ďalšie osobitné atribúty v súvislosti s každým z týchto bodov:

a) úloha poskytovateľa platobných služieb, ktorá môže predstavovať jednu alebo viaceré z týchto možností:

   i) spravovanie účtov;

   ii) iniciovanie platby;

   iii) informovanie o účte;

   iv) vydávanie platobných nástrojov viazaných na kartu;

b) názov príslušných orgánov, v ktorých je poskytovateľ platobných služieb registrovaný.

4. Atribúty uvedené v odseku 3 nemajú vplyv na interoperabilitu a uznávanie kvalifikovaných certifikátov pre elektronické pečate alebo pre autentifikáciu webového sídla.

([1]) Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami a investičnými spoločnosťami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

Článok 35

Bezpečnosť komunikačnej relácie

1. Poskytovatelia platobných služieb spravujúci účet, poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu, poskytovatelia služieb informovania o účte a poskytovatelia platobných iniciačných služieb zabezpečia, aby sa pri výmene údajov prostredníctvom internetu uplatňovalo medzi komunikujúcimi stranami počas celého trvania príslušnej komunikačnej relácie bezpečné šifrovanie s cieľom zachovať dôvernosť a integritu údajov za použitia silných a všeobecne uznávaných techník šifrovania.

2. Poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu, poskytovatelia služieb informovania o účte a poskytovatelia platobných iniciačných služieb zachovávajú prístupové relácie poskytované poskytovateľmi platobných služieb spravujúcimi účet čo najkratšie a hneď, ako sa požadovaný krok dokončí, aktívne každú takúto reláciu ukončia.

3. Pri udržiavaní paralelných sieťových relácií u poskytovateľa platobných služieb spravujúceho účet, poskytovatelia služieb informovania o účte a poskytovatelia platobných iniciačných služieb zabezpečia, aby boli tieto relácie bezpečne prepojené s príslušnými reláciami vytvorenými s používateľom, resp. používateľmi platobných služieb s cieľom zabrániť možnosti chybného presmerovania akejkoľvek správy alebo informácie vymieňanej medzi nimi.

4. Poskytovatelia služieb informovania o účte, poskytovatelia platobných iniciačných služieb a poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu s poskytovateľom služieb spravujúcim účet uvádzajú jednoznačné odkazy na všetky tieto položky:

a) používateľ alebo používatelia platobných služieb a príslušná komunikačná relácia s cieľom rozlíšiť viacero žiadostí od toho istého používateľa alebo používateľov platobných služieb;

b) pri platobných iniciačných službách jednoznačne identifikovaná iniciovaná platobná transakcia;

c) pre potvrdenie dostupnosti finančných prostriedkov jednoznačne identifikovaná žiadosť súvisiaca so sumou potrebnou na vykonanie platobnej transakcie viazanej na kartu.

5. Poskytovatelia platobných služieb spravujúci účet, poskytovatelia služieb informovania o účte, poskytovatelia platobných iniciačných služieb a poskytovatelia platobných služieb vydávajúci platobné nástroje viazané na kartu zabezpečia, aby personalizované bezpečnostné prvky a autentifikačné kódy, ktoré poskytujú, nikdy neboli priamo ani nepriamo čitateľné žiadnymi zamestnancami.

Títo poskytovatelia v prípade straty dôvernosti personalizovaných bezpečnostných prvkov v rozsahu ich pôsobnosti bez zbytočného odkladu informujú používateľa platobných služieb, ktorému sú priradené, ako aj vydavateľa personalizovaných bezpečnostných prvkov.

Článok 36

Výmena údajov

1. Poskytovatelia platobných služieb spravujúci účet spĺňajú všetky tieto požiadavky:

a) poskytujú poskytovateľom služieb informovania o účte tie isté informácie z určených platobných účtov a súvisiacich platobných transakcií, aké boli sprístupnené používateľovi platobných služieb, pri priamej žiadosti o prístup k informáciám o účte za predpokladu, že tieto informácie nezahŕňajú citlivé údaje o platbách;

b) bezodkladne po prijatí platobného príkazu poskytnú poskytovateľom platobných iniciačných služieb tie isté informácie o iniciovaní a vykonaní platobnej transakcie, aké boli poskytnuté alebo sprístupnené používateľovi platobných služieb, keď transakciu iniciuje priamo používateľ platobných služieb;

c) na požiadanie okamžite poskytnú poskytovateľom platobných služieb potvrdenie v jednoduchom formáte „áno“ alebo „nie“ o tom, či je na platobnom účte platiteľa k dispozícii suma potrebná na vykonanie platobnej transakcie.

2. V prípade neočakávanej udalosti alebo chyby, ktorá sa vyskytne počas procesu identifikácie, autentifikácie alebo výmeny údajových prvkov poskytovateľ platobných služieb spravujúci účet zašle správu s oznámením poskytovateľovi platobných iniciačných služieb alebo poskytovateľovi služieb informovania o účte a poskytovateľovi platobných služieb vydávajúcemu platobné nástroje viazané na kartu, v ktorej vysvetlí dôvod neočakávanej udalosti alebo chyby.

Ak poskytovateľ platobných služieb spravujúci účet ponúka vyhradené rozhranie v súlade s článkom 32, toto rozhranie musí zabezpečovať, aby správy s oznámením týkajúcim sa neočakávaných udalostí alebo chýb boli oznamované každým poskytovateľom platobných služieb, ktorý udalosť alebo chybu odhalí, ostatným poskytovateľom platobných služieb zúčastneným na komunikačnej relácii.

3. Poskytovatelia služieb informovania o účte v súlade s výslovným súhlasom používateľa zavedú vhodné a účinné mechanizmy, ktoré bránia prístupu k iným informáciám, ako sú informácie z určených platobných účtov a súvisiacich platobných transakcií.

4. Poskytovatelia platobných iniciačných služieb poskytnú poskytovateľom platobných služieb spravujúcim účet tie isté informácie, aké sa požadujú od používateľa platobných služieb pri priamom iniciovaní platobnej transakcie.

5. Poskytovatelia služieb informovania o účte majú umožnený prístup k informáciám z určených platobných účtov a súvisiacich platobných transakcií, ktoré vedú poskytovatelia platobných služieb spravujúci účet, na účely vykonávania služieb informovania o účte za týchto okolností:

a) vždy, keď používateľ platobných služieb aktívne požaduje takéto informácie;

b) ak používateľ platobných služieb aktívne nepožaduje takéto informácie, najviac štyrikrát za 24 hodín, pokiaľ sa poskytovateľ služieb informovania o účte a poskytovateľ platobných služieb spravujúci účet nedohodnú na častejšej frekvencii so súhlasom používateľa platobných služieb.

KAPITOLA VI

ZÁVEREČNÉ USTANOVENIA

Článok 37

Preskúmanie

Bez toho, aby bol dotknutý článok 98 ods. 5 smernice (EÚ) 2015/2366, orgán EBA preskúma do 14. marca 2021 miery podvodu uvedené v prílohe k tomuto nariadeniu, ako aj výnimky udelené podľa článku 33 ods. 6 v súvislosti s vyhradenými rozhraniami, a v prípade potreby predloží Komisii návrh ich aktualizácií v súlade s článkom 10 nariadenia (EÚ) č. 1093/2010.

Článok 38

Nadobudnutie účinnosti

1. Toto nariadenie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Toto nariadenie sa uplatňuje od 14. septembra 2019.

3. Odseky 3 a 5 článku 30 sa však uplatňujú od 14. marca 2019.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 27. novembra 2017

Za Komisiu

predseda

Jean-Claude JUNCKER

PRÍLOHA

	Referenčná miera podvodu (v %) pre:	
Hodnota limitu na výnimku	Elektronické platby na diaľku viazané na kartu	Elektronické úhrady na diaľku
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015