DELEGIRANA UREDBA KOMISIJE (EU) 2018/389

z dne 27. novembra 2017

o dopolnitvi Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za močno avtentikacijo strank ter skupnih in varnih odprtih standardov komunikacije

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive (EU) 2015/2366 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o plačilnih storitvah na notranjem trgu, spremembah direktiv 2002/65/ES, 2009/110/ES ter 2013/36/EU in Uredbe (EU) št. 1093/2010 ter razveljavitvi Direktive 2007/64/ES ([1]) in zlasti drugega pododstavka člena 98(4) Direktive,

ob upoštevanju naslednjega:

(1) Plačilne storitve, ki se zagotavljajo elektronsko, bi se morale opravljati varno z uporabo tehnologij, ki omogočajo varno avtentikacijo uporabnika in v čim večji meri prispevajo k zmanjšanju tveganja goljufije. Postopek avtentikacije bi moral na splošno vključevati mehanizme za spremljanje transakcij, da bi se zaznali poskusi uporabe osebnih varnostnih elementov uporabnika plačilnih storitev, ki so bili izgubljeni, ukradeni ali zlorabljeni, zagotavljati pa bi morali tudi, da je uporabnik plačilnih storitev zakoniti uporabnik in se torej strinja s prenosom sredstev in dostopom do informacij o računu z običajno uporabo osebnih varnostnih elementov. Poleg tega je treba določiti zahteve za močno avtentikacijo stranke, ki bi se morala uporabiti vsakič, ko plačnik dostopa do svojega plačilnega računa prek spleta, odredi elektronsko plačilno transakcijo ali opravi kakršno koli dejavnost prek kanala na daljavo, ki lahko pomeni tveganje plačilne goljufije ali drugih zlorab, in sicer tako, da bi se ustvarila šifra za avtentikacijo, ki bi morala biti odporna na tveganje ponarejanja v celoti ali na razkritje katerega koli od elementov, na podlagi katerih je bila ustvarjena.

(2) Ker se metode goljufije nenehno spreminjajo, bi morale zahteve za močno avtentikacijo stranke omogočati inovacije pri tehničnih rešitvah, s katerimi se odziva na nove grožnje za varnost elektronskih plačil. Za zagotavljanje, da se zahteve, ki jih je treba določiti, vedno učinkovito izvajajo, je prav tako primerno zahtevati, da varnostne ukrepe za uporabo močne avtentikacije stranke in izjem od njene uporabe, ukrepe za zaščito zaupnosti in celovitosti osebnih varnostnih elementov ter ukrepe za vzpostavitev skupnih in varnih odprtih standardov komunikacije evidentirajo, redno testirajo, vrednotijo in pregledujejo revizorji s strokovnim znanjem s področja informacijsko-tehnološke varnosti in plačil, ki so operativno neodvisni. Da bi pristojnim organom omogočili spremljanje kakovosti pregledov teh ukrepov, bi jim morali biti taki pregledi na voljo na zahtevo.

(3) Ker je pri elektronskih plačilnih transakcijah na daljavo tveganje goljufije večje, je treba uvesti dodatne zahteve za močno avtentikacijo strank v takih transakcijah, s katero se zagotovi, da elementi dinamično povezujejo transakcijo z zneskom in prejemnikom plačila, ki ju je določil plačnik, ko je odredil transakcijo.

(4) Dinamična povezava je mogoča z ustvarjanjem šifer za avtentikacijo, za kar veljajo stroge varnostne zahteve. Da bi ostali tehnološko nevtralni, se ne bi smela zahtevati posebna tehnologija za izvajanje šifer za avtentikacijo. Zato bi morale šifre za avtentikacijo temeljiti na rešitvah, kot so ustvarjanje in potrjevanje enkratnih gesel, digitalni podpisi ali druga kriptografsko utemeljena zagotovila o veljavnosti, ki uporabljajo ključe ali kriptografski material, shranjen v elementih za avtentikacijo, dokler izpolnjujejo varnostne zahteve.

([1]) UL L 337, 23.12.2015, str. 35.

(5) Treba je določiti posebne zahteve za primere, v katerih končni znesek ni znan v trenutku, ko plačnik odredi elektronsko plačilno transakcijo na daljavo, za zagotovitev, da je močna avtentikacija stranke določena za najvišji znesek, za katerega je plačnik dal soglasje, kot je navedeno v Direktivi (EU) 2015/2366.

(6) Da bi zagotovili uporabo močne avtentikacije stranke, je prav tako treba zahtevati ustrezne varnostne značilnosti za elemente močne avtentikacije stranke, ki spadajo v kategorijo znanja (nekaj, kar ve samo uporabnik), na primer dolžina ali kompleksnost, za elemente, ki spadajo v kategorijo lastništva (nekaj, kar je v izključni lasti uporabnika), kot so specifikacije algoritmov, dolžina ključa in entropija informacij, ter za naprave in programsko opremo, ki berejo elemente, ki spadajo v kategorijo inherence (nekaj, kar uporabnik je), kot so specifikacije algoritmov, biometrični senzorji in elementi za zaščito predlog, zlasti zato, da bi zmanjšali tveganje, da navedene elemente odkrijejo in uporabljajo nepooblaščene osebe ali da se jim ti razkrijejo. Treba je določiti tudi zahteve za zagotovitev, da so navedeni elementi neodvisni, tako da kršitev enega elementa ne zmanjša zanesljivosti drugih, zlasti kadar se kateri od teh elementov uporablja na večnamenski napravi, kot je tablica ali mobilni telefon, ki se lahko uporablja za dajanje navodil za izvedbo plačila in v postopku avtentikacije.

(7) Zahteve glede močne avtentikacije stranke veljajo za plačila, ki jih odredi plačnik, ne glede na to, ali je plačnik fizična oseba ali pravni subjekt.

(8) Za plačila, opravljena z anonimnimi plačilnimi instrumenti, zaradi njihove narave ne velja obveznost močne avtentikacije strank. Kadar se anonimnost takih instrumentov odpravi na podlagi pogodbe ali zakonodaje, za plačila veljajo varnostne zahteve, ki izhajajo iz Direktive (EU) 2015/2366 in teh regulativnih tehničnih standardov.

(9) Izjeme od načela močne avtentikacije stranke so bile v skladu z Direktivo (EU) 2015/2366 opredeljene na podlagi stopnje tveganja, zneska, ponovitev transakcije in plačilnega kanala, ki se uporablja za izvršitev plačilne transakcije.

(10) Dejanja, ki pomenijo dostop do stanja na računu in nedavnih transakcij plačilnega računa brez razkritja občutljivih podatkov o plačilih, ponavljajoča se plačila istim prejemnikom plačil, ki jih je plačnik predhodno shranil ali potrdil z uporabo močne avtentikacije stranke, ter plačila istim fizičnim ali pravnim osebam z računi pri istem ponudniku plačilnih storitev in nakazila od njih predstavljajo nizko stopnjo tveganja, zato ponudnikom plačilnih storitev ni treba uporabiti močne avtentikacije stranke. Kljub temu lahko v skladu s členi 65, 66 in 67 Direktive (EU) 2015/2366 ponudniki storitev odreditve plačil, ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, in ponudniki storitev zagotavljanja informacij o računih od ponudnika plačilnih storitev, ki vodi račun, zahtevajo in pridobijo samo potrebne in bistvene informacije za opravljanje dane plačilne storitve, in sicer s soglasjem uporabnika plačilnih storitev. Takšno soglasje se lahko da posamično za vsak zahtevek po informacijah ali za vsako plačilo, ki se odredi, ali kot pooblastilo ponudniku storitev zagotavljanja informacij o računih za določene plačilne račune in povezane plačilne transakcije, kot je določeno v pogodbeni ureditvi z uporabnikom plačilnih storitev.

(11) Izjeme za brezstična plačila malih vrednosti na prodajnem mestu, pri katerih se upošteva tudi največje število zaporednih transakcij ali določena fiksna najvišja vrednost zaporednih transakcij brez uporabe močne avtentikacije stranke, omogočajo oblikovanje uporabniku prijaznih plačilnih storitev z nizkim tveganjem, zato bi morale biti dovoljene. Primerno je določiti tudi izjemo za elektronske plačilne transakcije, odrejene na samopostrežnih terminalih, kjer bi lahko bila uvedba uporabe močne avtentikacije stranke včasih težavna zaradi operativnih razlogov (npr. za izogibanje vrstam in morebitnim nesrečam na cestninskih postajah ali drugim tveganjem za varnost ali zaščito).

(12) Podobno kot pri izjemi za brezstična plačila malih vrednosti na prodajnem mestu bi bilo treba doseči ustrezno ravnovesje med interesom za večjo varnost pri plačilih na daljavo in potrebo po uporabniku prijaznih in dostopnih plačilih na področju e-trgovanja. Skladno s temi načeli bi bilo treba preudarno določiti pragove, pod katerimi se močna avtentikacija stranke ne uporablja, da bi zajeli samo spletne nakupe malih vrednosti. Pragove za spletne nakupe bi bilo treba določiti preudarneje, saj dejstvo, da oseba ni fizično prisotna ob nakupu, predstavlja nekoliko višje varnostno tveganje.

(13) Zahteve glede močne avtentikacije stranke veljajo za plačila, ki jih odredi plačnik, ne glede na to, ali je plačnik fizična oseba ali pravni subjekt. Veliko plačil podjetij se odredi preko namenskih postopkov ali protokolov, ki zagotavljajo visoko raven varnosti plačil, ki se v okviru Direktive (EU) 2015/2366 želi doseči z močno avtentikacijo stranke. Kadar pristojni organi ugotovijo, da plačilni postopki in protokoli, ki so na voljo samo plačnikom, ki niso potrošniki, dosegajo cilje Direktive (EU) 2015/2366 v smislu varnosti, se lahko ponudnike plačilnih storitev pri navedenih postopkih ali protokolih izvzame iz zahtev močne avtentikacije stranke.

(14) V primeru analize tveganja transakcije v realnem času, ki plačilno transakcijo razvrsti kot transakcijo z nizkim tveganjem, je prav tako primerno uvesti izjemo za ponudnika plačilnih storitev, ki ne namerava uporabiti močne avtentikacije stranke, in sicer s sprejetjem učinkovitih zahtev na podlagi tveganja, ki zagotavljajo varnost sredstev in osebnih podatkov uporabnika plačilnih storitev. Te zahteve na podlagi tveganja bi morale združevati rezultate analize tveganja, ki potrjujejo, da pri plačniku ni bil ugotovljen neobičajen vzorec porabe ali vedenja, ob upoštevanju drugih dejavnikov tveganja, vključno z informacijami o lokaciji plačnika in prejemnika plačila, z mejnimi denarnimi pragovi na podlagi stopnje goljufije, izračunane za plačila na daljavo. Kadar na podlagi analize tveganja transakcije v realnem času plačila ni mogoče razvrstiti kot plačila z nizko stopnjo tveganja, bi moral ponudnik plačilnih storitev zahtevati močno avtentikacijo stranke. Najvišjo vrednost takšnih izjem na podlagi tveganja bi bilo treba določiti tako, da se zagotovi zelo nizka povezana stopnja goljufije, tudi v primerjavi s stopnjo goljufije vseh plačilnih transakcij ponudnika plačilnih storitev v določenem časovnem obdobju in na drseči podlagi, vključno s tistimi, potrjenimi z močno avtentikacijo stranke.

(15) Za zagotavljanje učinkovitega izvrševanja bi morali ponudniki plačilnih storitev, ki želijo izkoristiti izjeme od uporabe močne avtentikacije stranke, redno spremljati ter pristojnim organom in Evropskemu bančnemu organu (EBA) na njihovo zahtevo za vsako vrsto plačilne transakcije omogočiti dostop do vrednosti goljufivih ali neodobrenih plačilnih transakcij ter ugotovljenih stopenj goljufije za vse svoje plačilne transakcije ne glede na to, ali so bile odobrene z močno avtentikacijo stranke ali izvršene na podlagi zadevne izjeme.

(16) Zbiranje teh novih podatkov o preteklih stopnjah goljufije pri elektronskih plačilnih transakcijah bo prispevalo tudi k učinkovitemu pregledu pragov za izjeme od uporabe močne avtentikacije stranke na podlagi analize tveganja transakcije v realnem času, ki ga bo opravila EBA. EBA bi morala pregledati in Komisiji predložiti osnutke posodobljenih regulativnih tehničnih standardov, kadar je ustrezno, in sicer s predložitvijo novih osnutkov pragov in povezanih stopenj goljufije za izboljšanje varnosti elektronskih plačil na daljavo, v skladu s členom 98(5) Direktive (EU) 2015/2366 in členom 10 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([1]).

(17) Ponudnikom plačilnih storitev, ki izkoristijo katero koli določeno izjemo, bi moralo biti dovoljeno, da se kadar koli odločijo za uporabo močne avtentikacije stranke za dejanja in plačilne transakcije iz navedenih določb.

(18) Ukrepi, ki ščitijo zaupnost in celovitost osebnih varnostnih elementov, ter naprave in programska oprema za avtentikacijo bi morali omejiti tveganja, povezana z goljufijami na podlagi neodobrene ali goljufive uporabe plačilnih instrumentov in nepooblaščenega dostopa do plačilnih računov. Zato je treba uvesti zahteve za varno oblikovanje in dostavo osebnih varnostnih elementov in njihovo povezavo z uporabnikom plačilnih storitev ter določiti pogoje za obnovitev in deaktivacijo teh elementov.

(19) Zaradi zagotavljanja učinkovite in varne komunikacije med zadevnimi udeleženci v okviru storitev zagotavljanja informacij o računih, storitev odredbe plačil in potrjevanja razpoložljivosti sredstev je treba določiti zahteve za skupne in varne odprte standarde komunikacije, ki jih morajo izpolnjevati vsi zadevni ponudniki plačilnih storitev. Direktiva (EU) 2015/2366 ponudnikom storitev zagotavljanja informacij o računih zagotavlja dostop do informacij o plačilnih računih in njihovo uporabo. Ta uredba zato ne spreminja pravil za dostop do računov, ki niso plačilni računi.

([1]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12).

(20) Vsak ponudnik plačilnih storitev, ki vodi račun, s plačilnimi računi, ki so dostopni prek spleta, bi moral ponujati vsaj en vmesnik za dostop, ki omogoča varno komunikacijo s ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente. Vmesnik bi moral ponudnikom storitev zagotavljanja informacij o računih, ponudnikom storitev odreditve plačil in ponudnikom plačilnih storitev, ki izdajajo kartične plačilne instrumente, omogočati identifikacijo pri ponudniku plačilnih storitev, ki vodi račun. Ponudnikom storitev zagotavljanja informacij o računih in ponudnikom storitev odreditve plačil bi moral omogočati tudi, da uporabljajo postopke avtentikacije, ki jih ponudnik plačilnih računov, ki vodi račun, zagotavlja uporabniku plačilnih storitev. Da bi zagotovili nevtralnost tehnologije in poslovnega modela, bi morali imeti ponudniki plačilnih storitev, ki vodijo račune, prosto izbiro pri odločanju, ali bodo ponudili vmesnik, ki je namenjen komunikaciji s ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, ali pa bodo za to komunikacijo dovolili uporabo vmesnika za identifikacijo in komunikacijo z uporabniki plačilnih storitev ponudnikov plačilnih storitev, ki vodijo račune.

(21) Da bi ponudnikom storitev zagotavljanja informacij o računih, ponudnikom storitev odreditve plačil in ponudnikom plačilnih storitev, ki izdajajo kartične plačilne instrumente, omogočili oblikovanje lastnih tehničnih rešitev, bi morale biti tehnične specifikacije ustrezno dokumentirane in javno dostopne. Poleg tega bi moral ponudnik plačilnih storitev, ki vodi račun, ponuditi platformo, ki bi ponudnikom plačilnih storitev omogočala testiranje tehničnih rešitev vsaj šest mesecev pred začetkom uporabe teh regulativnih standardov ali pred datumom, na katerega se bo vmesnik začel uporabljati na trgu, če se to zgodi po datumu začetka uporabe teh standardov. Da bi zagotovili interoperabilnost različnih tehnološko-komunikacijskih rešitev, bi moral vmesnik uporabljati standarde komunikacije, ki so jih oblikovale mednarodne ali evropske organizacije za standardizacijo.

(22) Kakovost storitev, ki jih zagotovijo ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil, bo odvisna od pravilnega delovanja vmesnikov, ki jih bodo vzpostavili ali prilagodili ponudniki plačilnih storitev, ki vodijo račune. Zato je pomembno, da se v primeru neskladnosti takih vmesnikov z določbami iz teh standardov uvedejo ukrepi, da se zajamči neprekinjeno poslovanje v korist uporabnikov navedenih storitev. Nacionalni pristojni organi so pristojni za zagotavljanje, da se ponudnikov storitev zagotavljanja informacij o računih in ponudnikov storitev odreditve plačil ne blokira ali ovira pri opravljanju njihovih storitev.

(23) Kadar je dostop do plačilnih računov zagotovljen prek namenskega vmesnika, je za zagotavljanje pravice uporabnikov plačilnih storitev, da uporabljajo ponudnike storitev odreditev plačil in storitve, ki omogočajo dostop do informacij o računih, kot določa Direktiva (EU) 2015/2366, treba zahtevati, da imajo namenski vmesniki enako raven razpoložljivosti in zmogljivosti kot vmesnik, ki je na voljo uporabniku plačilnih storitev. Ponudniki plačilnih storitev, ki vodijo račune, bi morali tudi opredeliti pregledne ključne kazalnike smotrnosti in cilje na ravni storitve za razpoložljivost in zmogljivost namenskih vmesnikov, ki so vsaj tako strogi kot tisti za vmesnik, ki se uporabljajo za njihove uporabnike plačilnih storitev. Navedene vmesnike bi morali testirati ponudniki plačilnih storitev, ki jih bodo uporabljali, pristojni organi pa bi morali opraviti obremenitvene teste in jih spremljati.

(24) Za zagotavljanje, da ponudniki plačilnih storitev, ki uporabljajo namenski vmesnik, lahko neprekinjeno opravljajo svoje storitve v primeru težav z razpoložljivostjo ali nezadostno zmogljivostjo, je treba ob upoštevanju strogih pogojev zagotoviti nadomestni mehanizem, ki bo takim ponudnikom omogočil uporabo vmesnika, ki ga ponudnik plačilnih storitev, ki vodi račune, uporablja za identifikacijo svojih uporabnikov plačilnih storitev in komunikacijo z njimi. Določeni ponudniki plačilnih storitev, ki vodijo račune, bodo izvzeti iz obveznosti zagotavljanja takšnega nadomestnega mehanizma z vmesniki za svoje stranke, če bodo njihovi pristojni organi ugotovili, da namenski vmesniki izpolnjujejo posebne pogoje, ki zagotavljajo neovirano konkurenco. Kadar izvzeti namenski vmesniki ne izpolnjujejo zahtevanih pogojev, zadevni pristojni organi prekličejo odobrene izjeme.

(25) Da bi pristojnim organom omogočili učinkovit nadzor in spremljanje izvajanja in upravljanja vmesnikov za komunikacijo, bi morali ponudniki plačilnih storitev, ki vodijo račune, na svojem spletnem mestu zagotoviti povzetek relevantne dokumentacije in pristojnim organom na zahtevo predložiti dokumentacijo o rešitvah v primeru izrednih razmer. Ponudniki plačilnih storitev, ki vodijo račune, bi morali prav tako javno objaviti statistiko o razpoložljivosti in zmogljivosti navedenega vmesnika.

(26) Zaradi varovanja zaupnosti in celovitosti podatkov je treba zagotoviti varnost komunikacijskih sej med ponudniki plačilnih storitev, ki vodijo račune, ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente. Zlasti je treba zahtevati

uporabo varnega šifriranja med ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil, ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, in ponudniki plačilnih storitev, ki vodijo račune, kadar si izmenjujejo podatke.

(27) Da bi izboljšali zaupanje uporabnikov in zagotovili močno avtentikacijo strank, bi bilo treba upoštevati uporabo sredstev elektronske identifikacije in storitev zaupanja, kot je določena v Uredbi (EU) št. 910/2014 Evropskega parlamenta in Sveta ([1]), zlasti glede priglašenih shem elektronske identifikacije.

(28) Da bi zagotovili usklajenost datumov uporabe, bi se morala ta uredba uporabljati od istega datuma, od katerega morajo države članice zagotoviti uporabo varnostnih ukrepov iz členov 65, 66, 67 in 97 Direktive (EU) 2015/2366.

(29) Ta uredba temelji na osnutkih regulativnih tehničnih standardov, ki jih je Komisiji predložil Evropski bančni organ (EBA).

(30) EBA je opravila odprta in pregledna javna posvetovanja o osnutkih regulativnih tehničnih standardov, na katerih temelji ta uredba, analizirala morebitne povezane stroške in koristi ter prosila za mnenje interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1093/2010 –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

Ta uredba določa zahteve, ki jih morajo izpolnjevati ponudniki plačilnih storitev, in sicer za izvajanje varnostnih ukrepov, ki jim omogočajo:

(a) uporabo postopka močne avtentikacije stranke v skladu s členom 97 Direktive (EU) 2015/2366;

(b) izjeme od uporabe varnostnih zahtev po močni avtentikaciji stranke, za katere veljajo določeni in omejeni pogoji na podlagi stopnje tveganja, zneska in ponovitev plačilne transakcije ter plačilnega kanala, ki se uporablja za izvršitev plačilne transakcije;

(c) zaščito zaupnosti in celovitosti osebnih varnostnih elementov uporabnika plačilnih storitev;

(d) vzpostavitev skupnih in varnih odprtih standardov za komuniciranje med ponudniki plačilnih storitev, ki vodijo račune, ponudniki storitev odreditve plačil, ponudniki storitev zagotavljanja informacij o računih, plačniki, prejemniki plačil in drugimi ponudniki plačilnih storitev glede opravljanja in uporabe plačilnih storitev v skladu z naslovom IV Direktive (EU) 2015/2366.

Člen 2

Splošne zahteve glede avtentikacije

1. Ponudniki plačilnih storitev imajo vzpostavljene mehanizme za spremljanje transakcij, ki jim omogočajo zaznavanje neodobrenih ali goljufivih transakcij, za namene izvajanja varnostnih ukrepov iz točk (a) in (b) člena 1.

([1]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 53).

Navedeni mehanizmi temeljijo na analizi plačilnih transakcij ob upoštevanju elementov, ki so tipični za uporabnika plačilnih storitev v okoliščinah običajne uporabe osebnih varnostnih elementov.

2. Ponudniki plačilnih storitev zagotovijo, da mehanizmi za spremljanje transakcij upoštevajo vsaj vse naslednje dejavnike na podlagi tveganja:

(a) seznam zlorabljenih ali ukradenih avtentikacijskih elementov;

(b) znesek vsake plačilne transakcije;

(c) znane scenarije goljufij pri opravljanju plačilnih storitev;

(d) znake okužbe z zlonamerno programsko opremo v kateri koli seji postopka avtentikacije;

(e) kadar napravo ali programsko opremo za dostop zagotovi ponudnik plačilnih storitev, dnevnik uporabe naprave ali programske opreme za dostop, zagotovljene uporabniku plačilnih storitev, ter neobičajne uporabe naprave ali programske opreme za dostop.

Člen 3

Pregled varnostnih ukrepov

1. Izvajanje varnostnih ukrepov iz člena 1 v skladu z veljavnim pravnim okvirom evidentirajo, redno testirajo, vrednotijo in revidirajo revizorji s strokovnim znanjem s področja informacijsko-tehnološke varnosti in plačil, ki so operativno neodvisni znotraj ponudnika plačilnih storitev ali od njega.

2. Obdobje med revizijami iz odstavka 1 se določi ob upoštevanju zadevnega računovodskega okvira in okvira obvezne revizije, ki se uporablja za ponudnika plačilnih storitev.

Vendar za ponudnike plačilnih storitev, ki uporabljajo izjemo iz člena 18, velja obveznost pregleda metodologije, modela in sporočenih stopenj goljufije vsaj enkrat letno. Revizor, ki opravi to revizijo, ima strokovno znanje s področja informacijsko-tehnološke varnosti in plačil ter je operativno neodvisen znotraj ponudnika plačilnih storitev ali od njega. To revizijo v prvem letu po uporabi izjeme iz člena 18 in vsaj vsaka tri leta po tem ali pogosteje, če to zahteva pristojni organ, opravi neodvisen in kvalificiran zunanji revizor.

3. Kot rezultat te revizije se pripravita ocena in poročilo o skladnosti varnostnih ukrepov ponudnika plačilnih storitev z zahtevami iz te uredbe.

Celotno poročilo je na zahtevo na voljo pristojnim organom.

POGLAVJE II

VARNOSTNI UKREPI ZA UPORABO MOČNE AVTENTIKACIJE STRANKE

Člen 4

Šifra za avtentikacijo

1. Kadar ponudnik plačilnih storitev uporablja močno avtentikacijo stranke v skladu s členom 97(1) Direktive (EU) 2015/2366, avtentikacija temelji na dveh ali več elementih, ki spadajo v kategorije znanja, lastništva in inherence, katerih rezultat je ustvarjanje šifre za avtentikacijo.

Ponudnik plačilnih storitev šifro za avtentikacijo sprejme samo enkrat, ko jo plačnik uporabi za dostop do svojega plačilnega računa prek spleta, odredi elektronsko plačilno transakcijo ali opravi kakršno koli dejavnost prek kanala na daljavo, ki lahko pomeni tveganje plačilne goljufije ali drugih zlorab.

2. Za namen odstavka 1 ponudnik plačilnih storitev sprejme varnostne ukrepe, pri čemer zagotovi, da so izpolnjene vse naslednje zahteve:

(a) iz razkritja šifre za avtentikacijo ni mogoče izpeljati nobenih informacij o katerem koli elementu iz odstavka 1;

(b) na podlagi poznavanja katere koli druge predhodno ustvarjene šifre za avtentikacijo ni mogoče ustvariti nove šifre za avtentikacijo;

(c) šifre za avtentikacijo ni mogoče ponarediti.

3. Ponudniki plačilnih storitev zagotovijo, da avtentikacija z ustvarjanjem šifre za avtentikacijo vključuje vse naslednje ukrepe:

(a) kadar pri avtentikaciji za dostop na daljavo, elektronska plačila na daljavo in kakršne koli druge dejavnosti prek kanala na daljavo, ki lahko pomenijo tveganje plačilne goljufije ali drugih zlorab, ni bila ustvarjena šifra za avtentikacijo za namene iz odstavka 1, ni mogoče ugotoviti, kateri od elementov iz navedenega odstavka je bil nepravilen;

(b) število neuspešnih poskusov avtentikacije, do katerih lahko pride zaporedoma, po katerem se dejavnosti iz člena 97(1) Direktive (EU) 2015/2366 začasno ali stalno blokirajo, ne presega petih poskusov v danem obdobju;

(c) komunikacijske seje so zaščitene pred zajemom podatkov za avtentikacijo, posredovanih med avtentikacijo, in pred posegi nepooblaščenih oseb v skladu z zahtevami iz poglavja V;

(d) najdaljši čas neaktivnosti plačnika po avtentikaciji za dostop do plačilnega računa prek spleta ni daljši od petih minut.

4. Kadar je blokada iz odstavka 3(b) začasna, se trajanje blokade in število ponovnih poskusov določi na podlagi značilnosti storitve, ki se zagotavlja plačniku, in vseh zadevnih vključenih tveganj ob upoštevanju vsaj dejavnikov iz člena 2(2).

Plačnika se opozori, preden blokada postane stalna.

Kadar blokada postane stalna, se vzpostavi varen postopek, ki plačniku omogoča, da ponovno pridobi možnost uporabe blokiranih elektronskih plačilnih instrumentov.

Člen 5

Dinamično povezovanje

1. Kadar ponudniki plačilnih storitev uporabljajo močno avtentikacijo stranke v skladu s členom 97(2) Direktive (EU) 2015/2366, poleg zahtev iz člena 4 te uredbe sprejmejo tudi varnostne ukrepe, ki izpolnjujejo vse naslednje zahteve:

(a) plačnika se obvesti o znesku plačilne transakcije in o prejemniku plačila;

(b) ustvarjena šifra za avtentikacijo je vezana na znesek plačilne transakcije in prejemnika plačila, ki ju je določil plačnik, ko je odredil transakcijo;

(c) šifra za avtentikacijo, ki jo ponudnik plačilnih storitev sprejme, ustreza izvirnemu določenemu znesku plačilne transakcije in identiteti prejemnika plačila, ki ju je določil plačnik;

(d) vsaka sprememba zneska ali prejemnika plačila pomeni razveljavitev ustvarjene šifre za avtentikacijo.

2. Ponudniki plačilnih storitev za namene odstavka 1 sprejmejo varnostne ukrepe, ki zagotavljajo zaupnost, avtentičnost in celovitost vseh naslednjih elementov:

(a) zneska transakcije in prejemnika plačila v vseh fazah avtentikacije;

(b) informacij, ki so plačniku prikazane v vseh fazah avtentikacije, vključno z ustvarjanjem, prenosom in uporabo šifre za avtentikacijo.

3. Za namene odstavka 1(b) in kadar ponudniki plačilnih storitev uporabljajo močno avtentikacijo stranke v skladu s členom 97(2) Direktive (EU) 2015/2366, za šifro za avtentikacijo veljajo naslednje zahteve:

(a) v zvezi s kartičnimi plačilnimi transakcijami, za katere je plačnik dal soglasje za točen znesek sredstev, ki jih je treba blokirati, v skladu s členom 75(1) navedene direktive, je šifra za avtentikacijo vezana na znesek, za katerega je plačnik dal soglasje, da se blokira, in s katerim se je plačnik strinjal, ko je odredil transakcijo;

(b) v zvezi s plačilnimi transakcijami, za katere je plačnik dal soglasje za izvršitev serije elektronskih plačilnih transakcij na daljavo enemu ali več prejemnikom plačil, je šifra za avtentikacijo vezana na skupni znesek serije plačilnih transakcij in na določene prejemnike plačil.

Člen 6

Zahteve za elemente, ki spadajo v kategorijo znanja

1. Ponudniki plačilnih storitev sprejmejo ukrepe za zmanjševanje tveganja, da nepooblaščene osebe odkrijejo elemente močne avtentikacije stranke, ki spadajo v kategorijo znanja, ali da se jim ti razkrijejo.

2. Za plačnikovo uporabo navedenih elementov veljajo ukrepi za zmanjševanje tveganja, da se prepreči razkritje teh elementov nepooblaščenim osebam.

Člen 7

Zahteve za elemente, ki spadajo v kategorijo lastništva

1. Ponudniki plačilnih storitev sprejmejo ukrepe za zmanjševanje tveganja, da nepooblaščene osebe uporabljajo elemente močne avtentikacije stranke, ki spadajo v kategorijo lastništva.

2. Za plačnikovo uporabo navedenih elementov veljajo ukrepi, da se prepreči njihova poustvaritev.

Člen 8

Zahteve za naprave in programsko opremo, povezano z elementi, ki spadajo v kategorijo inherence

1. Ponudniki plačilnih storitev sprejmejo ukrepe za zmanjševanje tveganja, da nepooblaščene osebe odkrijejo elemente avtentikacije, ki spadajo v kategorijo inherence in ki jih berejo naprave in programska oprema za dostop, ki se zagotovijo plačniku. Ponudniki plačilnih storitev zagotovijo vsaj, da za navedene naprave in programsko opremo za dostop obstaja zelo majhna verjetnost, da bi nepooblaščene osebe opravile avtentikacijo kot plačnik.

2. Za plačnikovo uporabo navedenih elementov veljajo ukrepi, ki zagotavljajo, da navedene naprave in programska oprema v primeru dostopa do naprav in programske opreme ne dopuščajo nedovoljene uporabe elementov.

Člen 9

Neodvisnost elementov

1. Ponudniki plačilnih storitev zagotovijo, da za uporabo elementov močne avtentikacije stranke iz členov 6, 7 in 8 veljajo ukrepi, ki zagotavljajo, da z vidika tehnologije, algoritmov in parametrov kršitev enega od elementov ne zmanjšuje zanesljivosti drugih elementov.

2. Kadar se kateri koli od elementov močne avtentikacije stranke ali sama šifra za avtentikacijo uporablja na večnamenski napravi, ponudniki plačilnih storitev sprejmejo varnostne ukrepe za zmanjševanje tveganja, ki bi nastalo zaradi zlorabe te večnamenske naprave.

3. Ukrepi za zmanjševanje tveganj za namene iz odstavka 2 vključujejo vse naslednje:

(a) uporabo ločenega varnega okolja za izvršitev prek programske opreme, nameščene na večnamenski napravi;

(b) mehanizme za zagotavljanje, da plačnik ali tretja oseba ni spremenil programske opreme ali naprave;

(c) kadar je prišlo do sprememb, mehanizme za zmanjševanje njihovih posledic.

POGLAVJE III

IZJEME OD MOČNE AVTENTIKACIJE STRANKE

Člen 10

Informacije o plačilnih računih

1. Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije stranke, če izpolnjujejo zahteve iz člena 2 in odstavka 2 tega člena ter kadar je uporabnik plačilnih storitev omejen na uporabo enega ali obeh naslednjih podatkov prek spleta brez razkritja občutljivih podatkov o plačilih:

(a) stanja na enem ali več določenih plačilnih računih;

(b) plačilnih transakcij, izvršenih v zadnjih 90 dneh prek enega ali več določenih plačilnih računov.

2. Za namen odstavka 1 ponudniki plačilnih storitev niso izvzeti iz uporabe močne avtentikacije stranke, kadar je izpolnjen en od naslednjih pogojev:

(a) uporabnik plačilnih storitev do informacij iz odstavka 1 prek spleta dostopa prvič;

(b) od zadnjega dostopa uporabnika plačilnih storitev do informacij iz odstavka 1(b) prek spleta in uporabe močne avtentikacije stranke je minilo več kot 90 dni.

Člen 11

Brezstična plačila na prodajnih mestih

Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije stranke, če izpolnjujejo zahteve iz člena 2, kadar plačnik odredi brezstično elektronsko plačilno transakcijo, če so izpolnjeni naslednji pogoji:

(a) posamezen znesek brezstične elektronske plačilne transakcije ne presega 50 EUR in

(b) skupni znesek predhodnih brezstičnih elektronskih plačilnih transakcij, odrejenih s plačilnim instrumentom, ki ima brezstično funkcijo, od datuma zadnje uporabe močne avtentikacije stranke, ne presega 150 EUR ali

(c) število zaporednih brezstičnih elektronskih plačilnih transakcij, odrejenih s plačilnim instrumentom, ki ponuja brezstično funkcijo, od zadnje uporabe močne avtentikacije stranke, ne presega pet.

Člen 12

Samopostrežni terminali za javni prevoz in parkirnine

Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije stranke, če izpolnjujejo zahteve iz člena 2, kadar plačnik odredi elektronsko plačilno transakcijo na samopostrežnem plačilnem terminalu zaradi plačila vozovnice za javni prevoz ali parkirnine.

Člen 13

Preverjeni prejemniki plačil

1. Ponudniki plačilnih storitev uporabljajo močno avtentikacijo stranke, kadar plačnik ustvari ali spremeni seznam preverjenih prejemnikov plačil prek svojega ponudnika plačilnih storitev, ki vodi račun.

2. Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije stranke, če izpolnjujejo splošne zahteve glede avtentikacije, kadar plačnik odredi plačilno transakcijo in je prejemnik plačila vključen na seznam preverjenih prejemnikov plačil, ki ga je predhodno ustvaril plačnik.

Člen 14

Ponavljajoče se transakcije

1. Ponudnik plačilnih storitev uporablja močno avtentikacijo stranke, kadar plačnik ustvari, spremeni ali prvič odredi serijo ponavljajočih se transakcij z enakim zneskom in istemu prejemniku plačila.

2. Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije stranke, če izpolnjujejo splošne zahteve glede avtentikacije, za odreditev vseh nadaljnjih plačilnih transakcij, vključenih v serijo plačilnih transakcij iz odstavka 1.

Člen 15

Kreditna plačila med računi iste fizične ali pravne osebe

Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije strank, če izpolnjujejo zahteve iz člena 2, kadar plačnik odredi kreditni prenos v primeru, ko sta plačnik in prejemnik plačila ista fizična ali pravna oseba in se oba plačilna računa vodita pri istem ponudniku plačilnih storitev, ki vodi račune.

Člen 16

Transakcije majhnih vrednosti

Ponudnikom plačilnih storitev je dovoljeno, da ne uporabljajo močne avtentikacije strank, kadar plačnik odredi elektronsko plačilno transakcijo na daljavo, pod pogojem da so izpolnjeni naslednji pogoji:

(a) znesek elektronske plačilne transakcije na daljavo ne presega 30 EUR in

(b) skupni znesek predhodnih elektronskih plačilnih transakcij na daljavo, ki jih je plačnik odredil od zadnje uporabe močne avtentikacije stranke, ne presega 100 EUR ali

(c) število predhodnih elektronskih plačilnih transakcij na daljavo, ki jih je plačnik odredil od zadnje uporabe močne avtentikacije stranke, ne presega pet zaporednih posameznih elektronskih plačilnih transakcij na daljavo.

Člen 17

Varni plačilni postopki in protokoli za podjetja

Ponudnikom plačilnih storitev se dovoli, da ne uporabljajo močne avtentikacije stranke pri pravnih osebah, ki elektronske plačilne transakcije odrejajo z uporabo namenskih plačilnih postopkov ali protokolov, ki so na voljo samo plačnikom, ki niso potrošniki, kadar se pristojnim organom zadovoljivo dokaže, da navedeni postopki ali protokoli jamčijo vsaj enakovredno raven varnosti kot tisti, določeni v Direktivi (EU) 2015/2366.

Člen 18

Analiza tveganja transakcije

1. Ponudnikom plačilnih storitev se dovoli, da ne uporabljajo močne avtentikacije stranke, kadar plačnik odredi elektronsko plačilno transakcijo na daljavo, za katero ponudnik plačilnih storitev v skladu z mehanizmi za spremljanje transakcij iz člena 2 in odstavka 2(c) tega člena ugotovi, da predstavlja nizko stopnjo tveganja.

2. Za elektronsko plačilno transakcijo iz odstavka 1 se šteje, da predstavlja nizko stopnjo tveganja, kadar so izpolnjeni vsi naslednji pogoji:

(a) stopnja goljufije za to vrsto transakcij, ki jo sporoči ponudnik plačilnih storitev in se izračuna v skladu s členom 19, je enaka ali nižja od referenčne stopnje goljufije iz preglednice v Prilogi za „elektronske kartične transakcije na daljavo“ oziroma „elektronska kreditna plačila na daljavo“;

(b) znesek transakcije ne presega zadevne mejne vrednosti za izjemo, določene v preglednici v Prilogi;

(c) ponudniki plačilnih storitev po opravljeni analizi tveganja v realnem času niso ugotovili ničesar od naslednjega:

   (i) neobičajnega vzorca porabe ali vedenja plačnika;

   (ii) nenavadnih informacij o dostopu do plačnikove naprave/programske opreme;

   (iii) okužbe z zlonamerno programsko opremo v kateri koli seji postopka avtentikacije;

   (iv) znanega scenarija goljufije pri opravljanju plačilnih storitev;

   (v) neobičajne lokacije plačnika;

   (vi) visoko tvegane lokacije prejemnika plačila.

3. Ponudniki plačilnih storitev, ki nameravajo elektronske plačilne transakcije na daljavo izvzeti iz obveznosti močne avtentikacije stranke, ker predstavljajo nizko tveganje, upoštevajo vsaj naslednje dejavnike na podlagi tveganja:

(a) predhodni vzorec porabe posameznega uporabnika plačilnih storitev;

(b) zgodovino plačilnih transakcij vsakega uporabnika plačilnih storitev ponudnika plačilnih storitev;

(c) lokacijo plačnika in prejemnika plačila v trenutku plačilne transakcije, kadar napravo ali programsko opremo za dostop zagotovi ponudnik plačilnih storitev;

(d) identifikacijo neobičajnih plačilnih vzorcev uporabnika plačilnih storitev glede na njegovo zgodovino transakcij.

Ponudnik plačilnih storitev vse navedene dejavnike na podlagi tveganja v svoji oceni združi v oceno tveganja za vsako posamezno transakcijo, da določi, ali se lahko določeno plačilo dovoli brez močne avtentikacije stranke.

Člen 19

Izračun stopenj goljufije

1. Ponudnik plačilnih storitev za vsako vrsto transakcije iz preglednice v Prilogi zagotovi, da so skupne stopnje goljufije, ki zajemajo tako plačilne transakcije, ki se potrdijo z močno avtentikacijo stranke, kot tudi tiste, ki se izvršijo v okviru katere koli od izjem iz členov 13 do 18, enake ali nižje od referenčne stopnje goljufije za isto vrsto plačilne transakcije, navedene v preglednici v Prilogi.

Splošna stopnja goljufije za vsako vrsto transakcije se izračuna kot skupna vrednost neodobrenih ali goljufivih transakcij na daljavo, in sicer ne glede na to, ali so bila sredstva izterjana ali ne, deljena s skupno vrednostjo vseh transakcij na daljavo za enako vrsto transakcij, odobrenih z uporabo močne avtentikacije stranke ali izvršenih na podlagi katere koli od izjem iz členov 13 do 18, na drseči četrtletni osnovi (90 dni).

2. Izračun stopenj goljufije in dobljene številke se ocenijo v revizijskem pregledu iz člena 3(2), s čimer se zagotovi, da so popolne in točne.

3. Metodologija in vsak model, ki ga ponudnik plačilnih storitev uporablja za izračun stopenj goljufije, ter same stopnje goljufije se ustrezno dokumentirajo in dajo na zahtevo v celoti na voljo pristojnim organom in EBA, in sicer s predhodnim obvestilom zadevnim pristojnim organom.

Člen 20

Prenehanje izjem na podlagi analize tveganja transakcije

1. Ponudniki plačilnih storitev, ki uporabljajo izjemo iz člena 18, pristojnim organom takoj sporočijo, če ena od njihovih spremljanih stopenj goljufije za katero koli vrsto plačilnih transakcij, navedenih v preglednici v Prilogi, preseže veljavno referenčno stopnjo goljufije, in jim zagotovijo opis ukrepov, ki jih nameravajo sprejeti za ponovno vzpostavitev skladnosti svoje spremljane stopnje goljufije z veljavnimi referenčnimi stopnjami goljufije.

2. Ponudniki plačilnih storitev takoj prenehajo uporabljati izjemo iz člena 18 za vsako vrsto plačilnih transakcij iz preglednice v Prilogi v določenem razponu mejne vrednosti za izjemo, če njihova spremljana stopnja goljufije dve zaporedni četrtletji preseže referenčno stopnjo goljufije, ki velja za navedeni plačilni instrument ali vrsto plačilne transakcije v navedenem razponu mejne vrednosti za izjemo.

3. Ponudniki plačilnih storitev po prenehanju izjeme iz člena 18 v skladu z odstavkom 2 tega člena te izjeme ne uporabljajo več, dokler njihova izračunana stopnja goljufije eno četrtletje ni enaka ali nižja od referenčnih stopenj goljufije, ki veljajo za zadevno vrsto plačilnih transakcij v zadevnem razponu mejne vrednosti za izjemo.

4. Ko ponudniki plačilnih storitev nameravajo ponovno uporabiti izjemo iz člena 18, v razumnem času obvestijo pristojne organe in pred ponovno uporabo izjeme predložijo dokazila o ponovni vzpostavitvi skladnosti svoje spremljane stopnje goljufije z veljavno referenčno stopnjo goljufije v zadevnem razponu mejne vrednosti za izjemo v skladu z odstavkom 3 tega člena.

Člen 21

Spremljanje

1. Ponudniki plačilnih storitev za uporabo izjem iz členov 10 do 18 evidentirajo in spremljajo naslednje podatke za vsako vrsto plačilnih transakcij, pri čemer jih razčlenijo na plačilne transakcije na daljavo in plačilne transakcije, ki se ne izvajajo na daljavo, vsaj četrtletno:

(a) skupno vrednost neodobrenih ali goljufivih plačilnih transakcij v skladu s členom 64(2) Direktive (EU) 2015/2366, skupno vrednost vseh plačilnih transakcij in posledično stopnjo goljufije, vključno z razčlenitvijo za plačilne transakcije, odrejene z močno avtentikacijo stranke in v okviru vsake izjeme;

(b) povprečno vrednost transakcije, vključno z razčlenitvijo plačilnih transakcij, odrejenih z močno avtentikacijo stranke in v okviru vsake izjeme;

(c) število plačilnih transakcij, pri katerih so se uporabile izjeme, in njihov delež glede na skupno število plačilnih transakcij.

2. Ponudniki plačilnih storitev rezultate spremljanja v skladu z odstavkom 1 na zahtevo dajo na razpolago pristojnim organom in EBA, s predhodnim obvestilom zadevnim pristojnim organom.

POGLAVJE IV

ZAUPNOST IN CELOVITOST OSEBNIH VARNOSTNIH ELEMENTOV UPORABNIKA PLAČILNIH STORITEV

Člen 22

Splošne zahteve

1. Ponudniki plačilnih storitev zagotovijo zaupnost in celovitost osebnih varnostnih elementov uporabnika plačilnih storitev, vključno s šiframi za avtentikacijo, v vseh fazah avtentikacije.

2. Ponudniki plačilnih storitev za namene odstavka 1 zagotovijo, da so izpolnjene vse naslednje zahteve:

(a) osebni varnostni elementi so med prikazom zakriti in niso v celoti berljivi, ko jih uporabnik plačilnih storitev vnese med avtentikacijo;

(b) osebni varnostni elementi v podatkovni obliki ter kriptografski material, povezan s šifriranjem osebnih varnostnih elementov, niso shranjeni v neformatiranem besedilu;

(c) zaupni kriptografski material je zaščiten pred nedovoljenim razkritjem.

3. Ponudniki plačilnih storitev v celoti dokumentirajo postopek v zvezi z upravljanjem kriptografskega materiala, ki se uporablja za šifriranje ali drugačen način zagotavljanja neberljivosti osebnih varnostnih elementov.

4. Ponudniki plačilnih storitev zagotovijo, da obdelava in usmerjanje osebnih varnostnih elementov in šifer za avtentikacijo, ustvarjenih v skladu s poglavjem II, poteka v varnih okoljih v skladu s strogimi in splošno priznanimi standardi na tem področju.

Člen 23

Ustvarjanje in prenos varnostnih elementov

Ponudniki plačilnih storitev zagotovijo, da ustvarjanje osebnih varnostnih elementov poteka v varnem okolju.

Ponudniki plačilnih storitev zmanjšajo tveganje nedovoljene uporabe osebnih varnostnih elementov ter naprav in programske opreme za avtentikacijo po njihovi izgubi, kraji ali kopiranju pred dostavo plačniku.

Člen 24

Povezava z uporabnikom plačilnih storitev

1. Ponudniki plačilnih storitev zagotovijo, da je samo uporabnik plačilnih storitev na varen način povezan z osebnimi varnostnimi elementi ter napravami in programsko opremo za avtentikacijo.

2. Ponudniki plačilnih storitev za namene odstavka 1 zagotovijo, da so izpolnjene vse naslednje zahteve:

(a) povezava identitete uporabnika plačilnih storitev z osebnimi varnostnimi elementi, napravami in programsko opremo za avtentikacijo se opravi v varnih okoljih, za katera je odgovoren ponudnik plačilnih storitev in ki vključujejo vsaj prostore ponudnika plačilnih storitev, spletno okolje, ki ga zagotavlja ponudnik plačilnih storitev, ali druga podobna varna spletna mesta, ki jih uporablja ponudnik plačilnih storitev, ter njegove bankomate, in ob upoštevanju tveganj, povezanih z napravami in temeljnimi komponentami, uporabljenimi med postopkom povezovanja, za katere ni odgovoren ponudnik plačilnih storitev;

(b) povezava identitete uporabnika plačilnih storitev z osebnimi varnostnimi elementi ter napravami ali programsko opremo za avtentikacijo prek kanala na daljavo se opravi z uporabo močne avtentikacije stranke.

Člen 25

Dostava varnostnih elementov ter naprav in programske opreme za avtentikacijo

1. Ponudniki plačilnih storitev zagotovijo, da se dostava osebnih varnostnih elementov ter naprav in programske opreme za avtentikacijo uporabniku plačilnih storitev opravi na varen način, ki je zasnovan tako, da upošteva tveganja, povezana z njihovo nedovoljeno uporabo zaradi izgube, kraje ali kopiranja.

2. Ponudniki plačilnih storitev za namene odstavka 1 uvedejo vsaj vse naslednje ukrepe:

(a) učinkovite in varne mehanizme dostave, ki zagotavljajo, da se osebni varnostni elementi ter naprave in programska oprema za avtentikacijo dostavijo legitimnemu uporabniku plačilnih storitev;

(b) mehanizme, ki ponudniku plačilnih storitev omogočajo, da preveri avtentičnost programske opreme za avtentikacijo, ki se je uporabniku plačilnih storitev dostavila prek spleta;

(c) ureditve, ki zagotavljajo, da v primerih, kadar se dostava osebnih varnostnih elementov izvede zunaj prostorov ponudnika plačilnih storitev ali prek kanala na daljavo:

(i) nepooblaščena oseba ne more pridobiti več kot en element osebnih varnostnih elementov, naprav ali programske opreme za avtentikacijo, kadar se ti dostavijo prek istega kanala;

(ii) dostavljeni osebni varnostni elementi, naprave ali programska oprema za avtentikacijo pred uporabo zahtevajo aktivacijo;

(d) ureditve, ki zagotavljajo, da v primerih, ko je treba osebne varnostne elemente, naprave ali programsko opremo za avtentikacijo pred prvo uporabo aktivirati, aktivacija poteka v varnem okolju v skladu s postopki povezave iz člena 24.

Člen 26

Obnovitev osebnih varnostnih elementov

Ponudniki plačilnih storitev zagotovijo, da se pri obnovitvi ali ponovni aktivaciji osebnih varnostnih elementov upoštevajo postopki za ustvarjenje, povezavo in dostavo osebnih varnostnih elementov ter naprav za avtentikacijo v skladu s členi 23, 24 in 25.

Člen 27

Uničenje, deaktivacija in preklic

Ponudniki plačilnih storitev zagotovijo, da imajo vzpostavljene učinkovite postopke za uporabo vseh naslednjih varnostnih ukrepov:

(a) varno uničenje, deaktivacijo ali preklic osebnih varnostnih elementov, naprav in programske opreme za avtentikacijo;

(b) kadar ponudnik plačilnih storitev razširja naprave in programsko opremo za avtentikacijo, ki jih je mogoče ponovno uporabiti, se zagotovi, dokumentira in izvede varna ponovna uporaba naprave ali programske opreme, preden se da na voljo drugemu uporabniku plačilnih storitev;

(c) deaktivacijo ali preklic informacij, povezanih z osebnimi varnostnimi elementi, ki so shranjene v sistemih in podatkovnih zbirkah ponudnika plačilnih storitev ter, kadar je primerno, javnih registrih.

POGLAVJE V

SKUPNI IN VARNI ODPRTI STANDARDI KOMUNIKACIJE

Oddelek 1

Splošne zahteve za komunikacijo

Člen 28

Zahteve za identifikacijo

1. Ponudniki plačilnih storitev zagotovijo varno identifikacijo pri komunikaciji med plačnikovo napravo in napravo za sprejemanje elektronskih plačil prejemnika plačila, med drugim vključno s plačilnimi terminali.

2. Ponudniki plačilnih storitev zagotovijo, da se tveganja preusmeritve komunikacije k nepooblaščenim osebam v mobilnih aplikacijah in drugih vmesnikih uporabnika plačilnih storitev, ki ponujajo elektronske plačilne storitve, učinkovito zmanjšujejo.

Člen 29

Sledljivost

1. Ponudniki plačilnih storitev imajo vzpostavljene postopke, ki zagotavljajo, da so vse plačilne transakcije in druga interakcija z uporabnikom plačilnih storitev, z drugimi ponudniki plačilnih storitev in drugimi subjekti, vključno s trgovci, v okviru opravljanja plačilnih storitev sledljive, pri čemer zagotavljajo naknadno poznavanje vseh dogodkov, povezanih z elektronsko transakcijo v vseh različnih stopnjah.

2. Ponudniki plačilnih storitev za namen odstavka 1 zagotovijo, da vsaka komunikacijska seja z uporabnikom plačilnih storitev, drugimi ponudniki plačilnih storitev in drugimi subjekti, vključno s trgovci, temelji na vseh naslednjih elementih:

(a) edinstvenem identifikatorju seje;

(b) varnostnih mehanizmih za natančno beleženje transakcije, vključno s številko transakcije, časovnimi žigi in vsemi relevantnimi podatki o transakciji;

(c) časovnih žigih, ki temeljijo na enotnem časovnem referenčnem sistemu in ki so sinhronizirani v skladu z uradnim časovnim signalom.

Oddelek 2

Posebne zahteve za skupne in varne odprte standarde komunikacije

Člen 30

Splošne obveznosti za vmesnike za dostop

1. Ponudniki plačilnih storitev, ki vodijo račune, ki plačniku ponujajo plačilni račun, ki je dostopen prek spleta, imajo vzpostavljen vsaj en vmesnik, ki izpolnjuje vse naslednje zahteve:

(a) ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, se lahko identificirajo pri ponudniku plačilnih storitev, ki vodi račune;

(b) ponudniki storitev zagotavljanja informacij o računih lahko varno komunicirajo, da zahtevajo in prejmejo informacije o enem ali več določenih plačilnih računih in povezanih plačilnih transakcijah;

(c) ponudniki storitev odreditve plačil lahko varno komunicirajo, da odredijo plačilni nalog s plačnikovega plačilnega računa in prejmejo vse informacije o odreditvi plačilne transakcije ter vse informacije o izvršitvi plačilne transakcije, dostopne ponudnikom plačilnih storitev, ki vodijo račune.

2. Za namene avtentikacije uporabnika plačilnih storitev vmesnik iz odstavka 1 ponudnikom storitev zagotavljanja informacij o računih in ponudnikom storitev odreditve plačil omogoča, da uporabljajo vse postopke avtentikacije, ki jih je uporabniku plačilnih storitev zagotovil ponudnik plačilnih storitev, ki vodi račun.

Vmesniki izpolnjujejo vsaj vse naslednje zahteve:

(a) ponudnik storitev odreditve plačil ali ponudnik storitev zagotavljanja informacij o računih lahko ponudniku plačilnih storitev, ki vodi račune, na podlagi soglasja uporabnika plačilnih storitev naroči, naj začne avtentikacijo;

(b) komunikacijska seja med ponudnikom plačilnih storitev, ki vodi račune, ponudnikom storitev zagotavljanja informacij o računih, ponudnikom storitev odreditve plačil in katerim koli zadevnim uporabnikom plačilnih storitev se vzpostavi in ohrani med celotno avtentikacijo;

(c) zagotovi se celovitost in zaupnost osebnih varnostnih elementov in šifer za avtentikacijo, ki jih prenese ponudnik storitev odreditve plačil ali ponudnik storitev zagotavljanja informacij o računih ali ki se prenesejo preko njiju.

3. Ponudniki plačilnih storitev, ki vodijo račune, zagotovijo, da njihovi vmesniki upoštevajo standarde komunikacije, ki so jih izdale mednarodne ali evropske organizacije za standardizacijo.

Ponudniki plačilnih storitev, ki vodijo račune, zagotovijo tudi, da so tehnične specifikacije vseh vmesnikov dokumentirane, pri čemer navedejo sklope rutin, protokolov in orodij, ki jih ponudniki storitev odreditve plačil, ponudniki storitev zagotavljanja informacij o računih in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, potrebujejo, da zagotovijo interoperabilnost svoje programske opreme in aplikacij s sistemi ponudnikov plačilnih storitev, ki vodijo račune.

Ponudniki plačilnih storitev, ki vodijo račune, dajo na zahtevo ponudnikov storitev odreditve plačil, ponudnikov storitev zagotavljanja informacij o računih in ponudnikov plačilnih storitev, ki izdajajo kartične plačilne instrumente, ki imajo dovoljenje, ali ponudnikov plačilnih storitev, ki so pri svojih pristojnih organih zaprosili za ustrezno dovoljenje, brezplačno na voljo dokumentacijo in na svojem spletnem mestu objavijo povzetek dokumentacije vsaj in ne manj kot šest mesecev pred začetkom datuma uporabe iz člena 38(2) ali pred ciljnim datumom za začetek uporabe vmesnika za dostop na trgu, kadar do začetka uporabe pride po datumu iz člena 38(2).

4. Poleg odstavka 3 ponudniki plačilnih storitev, ki vodijo račune, zagotovijo, da je razen v izrednih razmerah vsaka sprememba tehničnih specifikacij njihovih vmesnikov na voljo ponudnikom storitev odreditve plačil, ponudnikom storitev zagotavljanja informacij o računih in ponudnikom plačilnih storitev, ki izdajajo kartične plačilne instrumente, ali ponudnikom plačilnih storitev, ki so pri svojih pristojnih organih zaprosili za ustrezno dovoljenje, in sicer čim prej vnaprej in ne manj kot tri mesece pred izvedbo spremembe.

Ponudniki plačilnih storitev dokumentirajo izredne razmere, v katerih so bile izvedene spremembe, in dokumentacijo na zahtevo dajo na voljo pristojnim organom.

5. Ponudniki plačilnih storitev, ki vodijo račune, dajo na voljo testno platformo, vključno s podporo, za testiranje povezovanja in delovanja, da ponudnikom storitev odreditve plačil, ponudnikom plačilnih storitev, ki izdajajo kartične plačilne instrumente, in ponudnikom storitev zagotavljanja informacij o računih, ki imajo dovoljenje, ali ponudnikom plačilnih storitev, ki so pri svojih pristojnih organih zaprosili za ustrezno dovoljenje, omogočijo testiranje njihove programske opreme in aplikacij, ki se uporabljajo za ponujanje plačilnih storitev uporabnikom. Testna platforma bi morala biti na voljo najkasneje šest mesecev pred datumom začetka uporabe iz člena 38(2) ali pred ciljnim datumom za začetek uporabe vmesnika za dostop na trgu, kadar do začetka uporabe pride po datumu iz člena 38(2).

Prek testne platforme se ne izmenjujejo občutljive informacije.

6. Pristojni organi zagotovijo, da ponudniki plačilnih storitev, ki vodijo račune, vedno izpolnjujejo obveznosti glede vmesnika ali vmesnikov, ki jih vzpostavijo, ki so vključene v te standarde. Kadar ponudnik plačilnih storitev, ki vodi račune, ne izpolnjuje zahtev za vmesnike iz teh standardov, pristojni organi zagotovijo, da se opravljanje storitev odrejanja plačil in zagotavljanja informacij o računih ne prepreči ali prekine, če zadevni ponudniki takih storitev izpolnjujejo pogoje iz člena 33(5).

Člen 31

Možnosti dostopa do vmesnika

Ponudniki plačilnih storitev, ki vodijo račune, vzpostavijo vmesnik ali vmesnike iz člena 30 prek namenskega vmesnika ali tako, da ponudnikom plačilnih storitev iz člena 30(1) dovolijo uporabo vmesnikov, ki se uporabljajo za avtentikacijo in komunikacijo z uporabniki plačilnih storitev ponudnika plačilnih storitev, ki vodi račune.

Člen 32

Zahteve za namenski vmesnik

1. Če so izpolnjene zahteve iz členov 30 in 31, ponudniki plačilnih storitev, ki vodijo račune in ki so vzpostavili namenski vmesnik, zagotovijo, da namenski vmesnik vedno zagotavlja enako raven razpoložljivosti in zmogljivosti, vključno s podporo, kot vmesniki, ki so uporabniku plačilnih storitev na voljo za neposreden dostop do njegovega plačilnega računa prek spleta.

2. Ponudniki plačilnih storitev, ki vodijo račune in ki so vzpostavili namenski vmesnik, opredelijo pregledne ključne kazalnike uspešnosti in cilje glede ravni storitve, ki so vsaj tako strogi kot tisti za vmesnik, ki ga uporabljajo njihovi uporabniki plačilnih storitev, in sicer tako v smislu razpoložljivosti kot tudi podatkov, predloženih v skladu s členom 36. Navedene vmesnike, kazalnike in cilje spremljajo pristojni organi in na njih izvajajo obremenitvene teste.

3. Ponudniki plačilnih storitev, ki vodijo račune in ki so vzpostavili namenski vmesnik, zagotovijo, da ta vmesnik ne predstavlja ovir za opravljanje storitev odreditve plačil in zagotavljanja informacij o računih. Take ovire lahko med drugim vključujejo preprečevanje, da bi ponudniki plačilnih storitev iz člena 30(1) uporabljali varnostne elemente, ki so jih svojim strankam izdali ponudniki plačilnih storitev, ki vodijo račune, vsiljevanje preusmeritve na avtentikacijo ali druge funkcije ponudnika plačilnih storitev, ki vodi račune, zahtevanje dodatnih dovoljenj in registracij poleg tistih iz členov 11, 14 in 15 Direktive (EU) 2015/2366 ali zahtevanje dodatnih preverjanj soglasja, ki ga uporabniki plačilnih storitev dajo ponudnikom storitev odreditve plačil in ponudnikom storitev zagotavljanja informacij o računih.

4. Ponudniki plačilnih storitev, ki vodijo račune, za namene odstavkov 1 in 2 spremljajo razpoložljivost in zmogljivost namenskega vmesnika. Ponudniki plačilnih storitev, ki vodijo račune, na svojem spletnem mestu četrtletno objavijo statistiko o razpoložljivosti in zmogljivosti namenskega vmesnika ter vmesnika, ki ga uporabljajo njihovi uporabniki plačilnih storitev.

Člen 33

Ukrepi za namenski vmesnik ob nepredvidljivih dogodkih

1. Ponudniki plačilnih storitev, ki vodijo račune, v zasnovo namenskega vmesnika vključijo strategijo in načrte za ukrepe ob nepredvidljivih dogodkih v primeru, da vmesnik ne deluje v skladu s členom 32, če pride do nenačrtovane nerazpoložljivosti vmesnika in če pride do okvare sistema. Lahko se domneva, da je prišlo do nenačrtovane nerazpoložljivosti ali okvare sistema, če ni odgovora na pet zaporednih zahtev za dostop do informacij za opravljanje storitev odreditve plačil ali storitev za zagotavljanje informacij o računih v 30 sekundah.

2. Ukrepi ob nepredvidljivih dogodkih vključujejo komunikacijske načrte za obveščanje ponudnikov plačilnih storitev, ki uporabljajo namenski vmesnik, o ukrepih za ponovno vzpostavitev sistema in opis alternativnih možnosti, ki so takoj na voljo ponudnikom plačilnih storitev in jih lahko uporabljajo v tem času.

3. Ponudnik plačilnih storitev, ki vodi račun, in ponudniki plačilnih storitev iz člena 30(1) brez odlašanja sporočijo težave z namenskimi vmesniki iz odstavka 1 svojim nacionalnim pristojnim organom.

4. V okviru nadomestnega mehanizma se ponudnikom plačilnih storitev iz člena 30(1) dovoli uporaba vmesnikov, ki so uporabnikom plačilnih storitev na voljo za avtentikacijo in komunikacijo z njihovim ponudnikom plačilnih storitev, ki vodi račun, dokler ni ponovno vzpostavljena raven razpoložljivosti in zmogljivosti namenskega vmesnika, kot je določeno v členu 32.

5. Ponudniki plačilnih storitev, ki vodijo račune, v ta namen zagotovijo, da je ponudnike plačilnih storitev iz člena 30(1) mogoče identificirati in da lahko uporabljajo postopke avtentikacije, ki jih je uporabniku plačilnih storitev zagotovil ponudnik plačilnih storitev, ki vodi račun. Kadar ponudniki plačilnih storitev iz člena 30(1) uporabljajo vmesnik iz odstavka 4:

(a) sprejmejo potrebne ukrepe za zagotovitev, da ne dostopajo do podatkov, jih shranjujejo in obdelujejo v druge namene kot za opravljanje storitev, za katere je zaprosil uporabnik plačilnih storitev;

(b) še naprej izpolnjujejo obveznosti iz člena 66(3) oziroma člena 67(2) Direktive (EU) 2015/2366;

(c) beležijo podatke, do katerih se dostopa prek vmesnika, ki ga za svoje uporabnike plačilnih storitev upravlja ponudnik plačilnih storitev, ki vodi račune, in na zahtevo ter brez nepotrebnega odlašanja dnevniške datoteke predložijo nacionalnemu pristojnemu organu;

(d) svojemu nacionalnemu pristojnemu organu na zahtevo in brez nepotrebnega odlašanja ustrezno utemeljijo uporabo vmesnika, ki je uporabnikom plačilnih storitev na voljo za neposreden dostop do njihovih plačilnih računov prek spleta;

(e) ustrezno obvestijo ponudnika plačilnih storitev, ki vodi račune.

6. Pristojni organi po posvetovanju z EBA za zagotavljanje dosledne uporabe naslednjih pogojev iz obveznosti vzpostavitve nadomestnega mehanizma iz odstavka 4 izvzamejo ponudnike plačilnih storitev, ki vodijo račune in ki so se odločili za namenski vmesnik, kadar namenski vmesnik izpolnjuje vse naslednje pogoje:

(a) skladen je z vsemi zahtevami za namenske vmesnike iz člena 32;

(b) zasnovan in testiran je bil v skladu s členom 30(5), njegovo ustreznost pa so potrdili ponudniki plačilnih storitev iz navedenega člena;

(c) ponudniki plačilnih storitev so ga vsaj tri mesece redno uporabljali za ponujanje storitev zagotavljanja informacij o računih, storitev odreditve plačil in potrjevanje razpoložljivosti sredstev za kartična plačila;

(d) vse težave, povezane z namenskim vmesnikom, so bile rešene brez nepotrebnega odlašanja.

7. Pristojni organi prekličejo izjemo iz odstavka 6, kadar ponudniki plačilnih storitev, ki vodijo račune, dlje kot dva zaporedna koledarska tedna ne izpolnjujejo pogojev (a) in (d). Pristojni organi o tem preklicu obvestijo EBA in zagotovijo, da ponudnik plačilnih storitev, ki vodi račune, v najkrajšem možnem času in najkasneje v dveh mesecih vzpostavi nadomestni mehanizem iz odstavka 4.

Člen 34

Potrdila

1. Ponudniki plačilnih storitev za namene identifikacije iz člena 30(1)(a) uporabljajo kvalificirana potrdila za elektronske žige iz člena 3(30) Uredbe (EU) št. 910/2014 ali kvalificirana potrdila za avtentikacijo spletišč iz člena 3(39) navedene uredbe.

2. Za namene te uredbe je registrska številka, kot je navedena v uradnih evidencah, iz točke (c) Priloge III ali točke (c) Priloge IV k Uredbi (EU) št. 910/2014 številka dovoljenja ponudnika plačilnih storitev, ki izdaja kartične plačilne instrumente, ponudnikov storitev zagotavljanja informacij o računih in ponudnikov storitev odreditve plačil, vključno s ponudniki plačilnih storitev, ki vodijo račune in ki opravljajo takšne storitve, ki je na voljo v javnem registru matične države članice v skladu s členom 14 Direktive (EU) 2015/2366 ali na podlagi uradnega obvestila o vsakem dovoljenju, izdanem na podlagi člena 8 Direktive 2013/36/EU Evropskega parlamenta in Sveta ([1]), v skladu s členom 20 navedene direktive.

3. Za namene te uredbe kvalificirana potrdila za elektronske žige ali za avtentikacijo spletišč iz odstavka 1 vključujejo, in sicer v jeziku, ki se običajno uporablja na področju mednarodnih financ, dodatne posebne značilnosti glede vsega naslednjega:

(a) vloge ponudnika plačilnih storitev, ki lahko ima eno ali več od naslednjih vlog:

  (i) vodenje računov;

  (ii) odrejanje plačil;

  (iii) zagotavljanje informacij o plačilnih računih;

  (iv) izdajanje kartičnih plačilnih instrumentov;

(b) naziv pristojnih organov, pri katerih je ponudnik plačilnih storitev registriran.

4. Značilnosti iz odstavka 3 ne vplivajo na interoperabilnost in priznavanje kvalificiranih potrdil za elektronske žige ali za avtentikacijo spletišč.

([1]) Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij in investicijskih podjetij, spremembi Direktive 2002/87/ES in razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

Člen 35

Varnost komunikacijske seje

1. Ponudniki plačilnih storitev, ki vodijo račune, ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil zagotovijo, da se pri izmenjavi podatkov prek spleta uporablja varno šifriranje med stranmi, udeleženimi v komunikaciji, v celotni posamezni komunikacijski seji, da se zavarujeta zaupnost in celovitost podatkov, in sicer z uporabo močnih in splošno priznanih tehnik šifriranja.

2. Ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil poskrbijo, da so seje za dostop, ki jih zagotovijo ponudniki plačilnih storitev, ki vodijo račune, čim krajše, in aktivno končajo vsako tako sejo takoj, ko se zahtevana dejavnost zaključi.

3. Ponudniki storitev zagotavljanja informacij o računih in ponudniki storitev odreditve plačil v primeru vzporednih omrežnih sej s ponudnikom plačilnih storitev, ki vodi račun, zagotovijo, da so te seje varno povezane z relevantnimi sejami, vzpostavljenimi z uporabnikom ali uporabniki plačilnih storitev, da se prepreči možnost napačnega usmerjanja sporočil ali informacij, ki si jih izmenjajo med komunikacijo.

4. Ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, s ponudniki plačilnih storitev, ki vodijo račune, vsebujejo nedvoumne sklice na vse naslednje elemente:

(a) uporabnika ali uporabnike plačilnih storitev in ustrezno komunikacijsko sejo, da se razlikuje med več zahtevami istega uporabnika ali uporabnikov plačilnih storitev;

(b) za storitve odreditve plačil enolično identificirano odrejeno plačilno transakcijo;

(c) za potrditev razpoložljivosti sredstev enolično identificirano zahtevo, povezano z zneskom, potrebnim za izvršitev kartične plačilne transakcije.

5. Ponudniki plačilnih storitev, ki vodijo račune, ponudniki storitev zagotavljanja informacij o računih, ponudniki storitev odreditve plačil in ponudniki plačilnih storitev, ki izdajajo kartične plačilne instrumente, zagotovijo, da v primeru sporočanja osebnih varnostnih elementov in šifer za avtentikacijo ti niso nikoli posredno ali neposredno čitljivi za zaposlene.

V primeru izgube zaupnosti osebnih varnostnih elementov v njihovi pristojnosti navedeni ponudniki brez nepotrebnega odlašanja obvestijo uporabnika plačilnih storitev, ki je povezan z njimi, ter izdajatelja osebnih varnostnih elementov.

Člen 36

Izmenjava podatkov

1. Ponudniki plačilnih storitev, ki vodijo račune, izpolnjujejo vse naslednje zahteve:

(a) ponudnikom storitev zagotavljanja informacij o računih zagotovijo iste informacije o določenih plačilnih računih in povezanih plačilnih transakcijah, ki so na voljo uporabniku plačilnih storitev, kadar zahteva neposreden dostop do informacij o računu, pod pogojem, da te informacije ne vključujejo občutljivih podatkov o plačilih;

(b) takoj po prejemu plačilnega naloga ponudniku storitev odreditve plačil zagotovijo iste informacije o odreditvi in izvršitvi plačilne transakcije, ki se zagotovijo ali dajo na voljo uporabniku plačilnih storitev, kadar transakcijo odredi neposredno uporabnik plačilnih transakcij;

(c) na zahtevo ponudnikom plačilnih storitev v obliki preprostega „da“ ali „ne“ takoj sporočijo, ali je znesek, potreben za izvršitev plačilne transakcije, na voljo na plačilnem računu plačnika.

2. Ponudnik plačilnih storitev, ki vodi račun, v primeru nepričakovanega dogodka ali napake med postopkom identifikacije, avtentikacije ali izmenjave elementov podatkov pošlje obvestilo ponudniku storitev odreditve plačil ali ponudniku storitev zagotavljanja informacij o računih in ponudniku plačilnih storitev, ki izdaja kartične plačilne instrumente, v katerem pojasni razlog za nepričakovan dogodek ali napako.

Kadar ponudnik plačilnih storitev, ki vodi račun, zagotavlja namenski vmesnik v skladu s členom 32, ta vmesnik omogoča, da vsak ponudnik plačilnih storitev, ki zazna nepričakovan dogodek ali napako, drugim ponudnikom plačilnih storitev, ki sodelujejo v komunikacijski seji, pošlje obvestilo o nepričakovanem dogodku ali napaki.

3. Ponudniki storitev zagotavljanja informacij o računih imajo vzpostavljene primerne in učinkovite mehanizme, da preprečijo dostop do informacij, ki niso informacije o določenih plačilnih računih in povezanih plačilnih transakcijah, za katere je uporabnik dal izrecno soglasje.

4. Ponudniki storitev odreditve plačil ponudnikom plačilnih storitev, ki vodijo račune, zagotovijo enake informacije, kot se zahtevajo od uporabnika plačilne storitve, kadar ta neposredno odredi plačilno transakcijo.

5. Ponudniki storitev zagotavljanja informacij o računih imajo dostop do informacij o določenih plačilnih računih in povezanih plačilnih transakcijah, ki jih vodijo ponudniki plačilnih storitev, ki vodijo račune, za opravljanje storitve zagotavljanja informacij o računih v naslednjih okoliščinah:

(a) kadar uporabnik plačilnih storitev aktivno zahteva take informacije;

(b) kadar uporabnik plačilnih storitev ne zahteva takih informacij aktivno, ne več kot štirikrat v 24-urnem obdobju, razen če se ponudnik storitev zagotavljanja informacij o računih in ponudnik plačilnih storitev, ki vodi račun, ne dogovorita drugače, in sicer s soglasjem uporabnika plačilnih storitev.

POGLAVJE VI

KONČNE DOLOČBE

Člen 37

Pregled

Brez poseganja v člen 98(5) Direktive (EU) 2015/2366 EBA do 14. marca 2021 pregleda stopnje goljufije iz Priloge k tej uredbi ter izjeme, odobrene na podlagi člena 33(6), v zvezi z namenskimi vmesniki in, kadar je primerno, Komisiji predloži osnutke njihovih posodobitev v skladu s členom 10 Uredbe (EU) št. 1093/2010.

Člen 38

Začetek veljavnosti

1. Ta uredba začne veljati dan po objavi v *Uradnem listu Evropske unije*.

2. Ta uredba se uporablja od 14. septembra 2019.

3. Vendar se odstavka 3 in 5 člena 30 uporabljata od 14. marca 2019.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 27. novembra 2017

Za Komisijo

Predsednik

Jean-Claude JUNCKER

PRILOGA

	Referenčna stopnja goljufije (v %) za:	
Mejna vrednost za izjemo	Elektronske kartične transakcije na daljavo	Elektronska kreditna plačila na daljavo
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015