Na temelju članka 2. stavka 2. Odluke o dodatnim i izmijenjenim usklađenim uvjetima za otvaranje i funkcioniranje PM računa u sustavu TARGET2 upotrebnom internetskog pristupa ("Narodne novine", br. 136/2015.) i članka 43. stavka 2. točke 10. Zakona o Hrvatskoj narodnoj banci ("Narodne novine", br. 75/2008. i 54/2013.)
guverner Hrvatske narodne banke donosi

DODATAK I.A
ODLUCI O DODATNIM I IZMIJENJENIM UVJETIMA ZA OTVARANJE I FUNKCIONIRANJE PM RAČUNA U SUSTAVU TARGET2-HR UPOTREBOM INTERNETSKOG PRISTUPA

TEHNIČKE SPECIFIKACIJE ZA OBRADU NALOGA ZA PLAĆANJE ZA INTERNETSKI PRISTUP

1. Opća odredba

Ovim se Dodatkom utvrđuju dodatna pravila za obradu naloga za plaćanje kod internetskog pristupa osim onih utvrđenih Odlukom o dodatnim i izmijenjenim uvjetima za otvaranje i funkcioniranje PM računa u sustavu TARGET2-HR upotrebom internetskog pristupa.

2. Tehnički zahtjevi za sudjelovanje u sustavu TARGET2-HR u vezi s infrastrukturom, mrežom i formatom

(1) Svaki sudionik koji se koristi internetskim pristupom mora se povezati s ICM-om sustava TARGET2 upotrebom lokalnoga klijenta, operativnog sustava i internetskog preglednika kako je određeno u Prilogu Detaljnim funkcionalnim specifikacijama za korisnike (UDFS) pod nazivom „Internetsko sudjelovanje – sistemski zahtjevi za internetski pristup", s određenim postavkama. Svaki PM račun sudionika identificira se osmeroznamenkastim ili jedanaesteroznamenkastim BIC-em. Nadalje, prije sudjelovanja u sustavu TARGET2-HR svaki sudionik prolazi niz testova da bi dokazao svoje tehničke i operativne sposobnosti.

(2) Za podnošenje naloga za plaćanje i razmjenu platnih poruka u PM-u upotrebljava se BIC platforme sustava TARGET2, TRGTXEPMLVP kao pošiljatelj/primatelj poruka. Nalozi za plaćanje poslani sudioniku koji se koristi internetskim pristupom moraju identificirati tog

sudionika primatelja u polju institucije korisnika. Nalozi za plaćanje koje zada sudionik koji se koristi internetskim pristupom identificiraju tog sudionika kao instituciju nalogodavca.

(3) Sudionici koji se koriste internetskim pristupom upotrebljavaju usluge infrastrukture javnog ključa kako je navedeno u „Priručniku za korištenje usluga certificiranja javnog ključa kod internetskog pristupa".

3. Vrste platnih poruka

(1) Internetski sudionici mogu izvršiti sljedeće vrste plaćanja:

(a) plaćanja klijenata, tj. kreditni transfer kod kojih klijent nalogodavac i/ili klijent korisnik nisu financijske institucije,

(b) plaćanja klijenta (potpuna automatska obrada), tj kreditni transfer kod kojih klijent nalogodavac i/ili klijent korisnik nisu financijske institucije, izvršena u načinu potpuno automatske obrade,

(c) transferi banke banci kojima se zahtijeva prijenos sredstava između financijskih institucija,

(d) plaćanja pokrića kojima se zahtijeva prijenos sredstava između financijskih institucija u vezi s klijentovim temeljnim kreditnim transferom.

Osim toga, sudionici koji se koriste internetskim pristupom za pristup PM računu mogu primiti naloge za izravno terećenje na teret PM računa.

(2) Sudionici moraju postupati u skladu sa specifikacijama polja kako je određeno u poglavlju 9.1.2.2. UDFS-a, Knjiga 1.

(3) Sadržaj polja provjerava se na razini TARGET2-HR u skladu sa zahtjevima UDFS-a. Sudionici se mogu međusobno sporazumjeti o posebnim pravilima o sadržaju polja. Međutim, u sustavu TARGET2-HR ne postoje posebne provjere postupaju li sudionici u skladu s takvim pravilima.

(4) Sudionici koji se koriste internetskim pristupom mogu izvršiti plaćanja pokrića preko sustava TARGET2, tj. plaćanja korespondentnih banaka radi namire (pokrića) poruka o kreditnom transferu, koje se dostavljaju klijentovoj banci drugim, izravnijim sredstvima. Pojedinosti o klijentu sadržane u tim plaćanjima pokrića ne prikazuju se u ICM-u.

4. Provjera dvostrukog unosa

(1) Svi nalozi za plaćanje prolaze provjeru dvostrukog unosa, čiji je cilj odbiti naloge za plaćanje koji su pogreškom dostavljeni više od jednog puta.

(2) Provjeravaju se sljedeća polja vrsta poruka:

Pojedinosti	**Dio poruke**	**Polje**
Pošiljatelj	Osnovno zaglavlje	BIC adresa
Vrsta poruke	Zaglavlje aplikacije	Vrsta poruke
Primatelj	Zaglavlje aplikacije	Adresa odredišta
Referentni broj transakcije (TRN)	Tekstualni blok	:20
Povezana referencija	Tekstualni blok	:21
Datum valute	Tekstualni blok	:32
Iznos	Tekstualni blok	:32

(3) Ako su sva polja opisana u podtočki 2. ove točke u novodostavljenom nalogu za plaćanje identična onima u nalogu za plaćanje koji je već primljen, novodostavljeni se nalog za plaćanje vraća.

5. Kodovi pogrešaka

Ako je nalog za plaćanje odbijen, obavijest o prekidu dostavlja se preko ICM-a s naznakom razloga za odbijanje koji se navodi upotrebom kodova pogrešaka. Kodovi pogrešaka određeni su u poglavlju 9.4.2. UDFS-a.

6. Unaprijed utvrđeno vrijeme namire

(1) Za naloge za plaćanje koji upotrebljavaju indikator najranijeg vremena terećenja upotrebljava se kod „/FROTIME/”.

(2) Za naloge za plaćanje koji upotrebljavaju indikator najkasnijeg vremena terećenja postoje dvije mogućnosti.

(a) Kod „/REJTIME/”: ako nalog za plaćanje ne može biti namiren do naznačenog vremena terećenja, nalog za plaćanje se vraća.

(b) Kod „/TILTIME/”: ako nalog za plaćanje ne može biti namiren do naznačenog vremena terećenja, nalog za plaćanje se ne vraća, nego se zadržava u odgovarajućem redu.

Kod obiju opcija automatski se šalje obavijest preko ICM-a ako nalog za plaćanje s indikatorom najkasnijeg vremena terećenja nije namiren 15 minuta prije naznačenog vremena.

(3) Ako se upotrijebi kod „/CLSTIME/”, s plaćanjem se postupa kao i s nalozima za plaćanje iz podtočke 2. pod (b) ove točke.

7. Namira naloga za plaćanje pri ulaznoj dispoziciji

(1) U sklopu ulazne dispozicije nalozi za plaćanje podvrgavaju se provjeri mogućnosti prebijanja i prema potrebi dodatnoj provjeri mogućnosti prebijanja (oba su izraza određena u podtočkama 2. i 3. ove točke) radi osiguravanja brze namire naloga za plaćanje na bruto načelu koja čuva likvidnost.

(2) Pri provjeri mogućnosti prebijanja utvrđuje se jesu li nalozi za plaćanje primatelja plaćanja koji su na početku vrlo hitnog ili, ako je to neprimjenjivo, hitnog reda, dostupni radi prebijanja s nalozima za plaćanje platitelja (u nastavku teksta: „prebijanje naloga za plaćanje”). Ako prebijanje naloga za plaćanje ne osigurava dovoljno sredstava za odnosni nalog za plaćanje platitelja u ulaznoj dispoziciji, utvrđuje se postoji li dovoljna dostupna likvidnost na platiteljevu PM računu.

(3) Ako provjera mogućnosti prebijanja ne uspije, Hrvatska narodna banka može primijeniti dodatnu provjeru mogućnosti prebijanja. Dodatnom provjerom mogućnosti prebijanja utvrđuje se dostupnost naloga za plaćanje za prebijanje u bilo kojem redu primatelja plaćanja bez obzira na to kada su uvršteni u red. Međutim, ako u redu primatelja plaćanja postoje nalozi za plaćanje s višim prioritetom, naslovljeni na druge sudionike u sustavu TARGET2, načelo FIFO može se prekršiti samo ako bi namira naloga za plaćanje prebijanjem imala za posljedicu povećanje likvidnosti kod primatelja plaćanja.

8. Namira naloga za plaćanje u redu

(1) Postupanje s nalozima za plaćanje u redovima ovisi o prioritetnom razredu za koji ih je odredio sudionik nalogodavac.

(2) Nalozi za plaćanje u vrlo hitnim i hitnim redovima namiruju se upotrebom provjere mogućnosti prebijanja opisane u točki 7. ovog Dodatka, počevši s nalogom za plaćanje na početku reda u slučajevima povećanja likvidnosti ili intervencije na razini reda (promjena mjesta u redu, vremena namire ili prioriteta, ili opoziv naloga za plaćanje).

(3) Nalozi za plaćanje u redovitom redu namiruju se na trajnoj osnovi uključujući sve vrlo hitne i hitne naloge za plaćanje koji još nisu namireni. Upotrebljavaju se različiti optimizacijski mehanizmi (algoritmi). Ako je algoritam uspješan, namiruje se uključeni nalog za plaćanje; ako algoritam nije uspješan, uključeni nalog za plaćanje ostaje u redu. Za prebijanje platnih tokova upotrebljavaju se tri algoritma (od 1 do 3). Putem algoritma 4 postupak namire 5 (određen u poglavlju 2.8.1. UDFS-a) dostupan je za namiru instrukcija za plaćanje sporednog sustava. Radi optimizacije namire vrlo hitnih transakcija sporednog sustava na podračunima sudionika upotrebljava se poseban algoritam (algoritam 5).

(a) Kod algoritma 1 („sve ili ništa”) Hrvatska narodna banka mora za svaki odnos u vezi s kojim je određeno dvostrano ograničenje, i za ukupni iznos odnosa, za koji je određeno višestrano ograničenje:

i. izračunati cjelokupnu likvidnosnu poziciju svakog PM računa sudionika u sustavu TARGET2 utvrđujući je li zbir svih izlaznih i ulaznih naloga za plaćanje koji čekaju u redu negativan ili pozitivan i, ako je negativan, provjeriti premašuje li sudionikovu dostupnu likvidnost (cjelokupna likvidnosna pozicija čini „ukupnu likvidnosnu poziciju”),

ii. provjeriti uvažavaju li se ograničenja i rezervacije koje je svaki sudionik u sustavu TARGET2 odredio u odnosu na svaki relevantni PM račun.

Ako je ishod ovih izračuna i provjera pozitivan za svaki relevantni PM račun, Hrvatska narodna banka i druge uključene središnje banke namiruju istodobno sva plaćanja na PM računima sudionika u sustavu TARGET2.

(b) Kod algoritma 2 („djelomično”) Hrvatska narodna banka mora:

i. izračunati i provjeriti likvidnosne pozicije, ograničenja i rezervacije svakog relevantnog PM računa kao i kod algoritma 1,

ii. ako je ukupna likvidnosna pozicija jednog ili više relevantnih PM računa negativna, isključiti pojedinačne naloge za plaćanje dok ukupna likvidnosna pozicija svakog relevantnog PM računa ne bude pozitivna.

Nakon toga Hrvatska narodna banka i druge uključene središnje banke, pod uvjetom da postoji dovoljno sredstava, namiruju sva preostala plaćanja (osim isključenih naloga za plaćanje) istodobno na PM računima relevantnih sudionika u sustavu TARGET2.

Pri isključivanju naloga za plaćanje Hrvatska narodna banka počinje od PM računa sudionika u sustavu TARGET2 s najvišom negativnom ukupnom likvidnosnom pozicijom i od naloga za plaćanje na kraju reda s najnižim prioritetom. Postupak odabira traje kratko vrijeme, što određuje Hrvatska narodna banka po vlastitoj procjeni.

(c) Kod algoritma 3 („višekratna") Hrvatska narodna banka mora:

i. usporediti parove PM računa sudionika u sustavu TARGET2 kako bi se utvrdilo mogu li nalozi za plaćanje koji čekaju u redu biti namireni u sklopu dostupne likvidnosti na PM računima tih dvaju sudionika u sustavu TARGET2 i unutar ograničenja koje su odredili (počevši od para PM računa s najmanjom razlikom između naloga za plaćanje naslovljenih jedan na drugog) te će uključene središnje banke uknjižiti ta plaćanja istodobno na PM račune tih dvaju sudionika u sustavu TARGET2,

ii. ako je, u odnosu na par PM računa opisanih pod (c) i. ove podtočke, likvidnost nedovoljna radi financiranja dvostrane pozicije, isključiti pojedinačne naloge za plaćanje dok likvidnost ne bude dovoljna. U tom slučaju uključene središnje banke namiruju preostala plaćanja osim isključenih, istodobno na PM računima tih dvaju sudionika u sustavu TARGET2.

Nakon izvršene provjere određene pod (c) i. i ii. ove podtočke Hrvatska narodna banka provjerava višestrane pozicije za namiru (između sudionikova PM računa i PM računa drugih sudionika u sustavu TARGET2 u vezi s kojima su određena višestrana ograničenja). U tu svrhu postupak opisan pod (c) i. i ii. ove podtočke primjenjuje se na odgovarajući način.

(d) Kod algoritma 4 („djelomična namira zajedno s namirom sporednog sustava") Hrvatska narodna banka slijedi isti postupak kao i za algoritam 2, ali bez isključivanja naloga za plaćanje u vezi s namirom sporednog sustava (koji namiruje na istodobnoj višestranoj osnovi).

(e) Kod algoritma 5 („namira sporednog sustava preko podračuna”) Hrvatska narodna banka slijedi isti postupak kao i za algoritam 1, uz izmjenu prema kojoj Hrvatska narodna banka započinje algoritam 5 preko sučelja sporednog sustava i provjerava samo postoji li dovoljno sredstava na podračunima sudionika. Osim toga, ne uzimaju se u obzir ograničenja i rezervacije. Algoritam 5 također se izvodi za vrijeme noćne namire.

(4) Nalozi za plaćanje uneseni u ulaznu dispoziciju nakon početka bilo kojeg algoritma od 1 do 4 mogu se ipak namiriti odmah u ulaznoj dispoziciji, ako su pozicije i ograničenja uključenih PM računa sudionika u sustavu TARGET2 kompatibilni s namirom tih naloga za plaćanje i namirom naloga za plaćanje u trenutačnom optimizacijskom postupku. Međutim, dva algoritma ne smiju se izvoditi istodobno.

(5) Za vrijeme dnevne obrade algoritmi se izvode uzastopno. Sve dok u tijeku nisu istodobne višestrane namire sporednog sustava, redoslijed je sljedeći:

(a) algoritam 1,

(b) ako algoritam 1 ne uspije, slijedi algoritam 2,

(c) ako algoritam 2 ne uspije, slijedi algoritam 3 ili, ako algoritam 2 uspije, ponavlja se algoritam 1.

Dok je u tijeku istodobna višestrana namira („postupak 5”) u vezi sa sporednim sustavom, izvodi se algoritam 4.

(6) Algoritmi se izvode fleksibilno postavljajući unaprijed utvrđeno vremensko kašnjenje između aplikacija različitih algoritama kako bi se osigurao najmanji interval između izvođenja dvaju algoritama. Vremenski slijed automatski se nadzire. Ručna intervencija je moguća.

(7) Kad je uključen u algoritam koji se izvodi, nalog za plaćanje ne smije biti ponovo raspoređen (promjena mjesta u redu) ili opozvan. Zahtjevi za ponovni raspored ili opoziv naloga za plaćanje čekaju u redu dok se algoritam ne dovrši. Ako se odnosni nalog za plaćanje namiri dok se algoritam izvodi, svaki se zahtjev za ponovnim rasporedom ili opozivom odbija. Ako se nalog za plaćanje ne namiri, sudionikovi zahtjevi odmah se uzimaju u obzir.

9. Upotreba ICM-a

(1) ICM se može upotrebljavati za unos naloga za plaćanje.

(2) ICM se može upotrebljavati za dobivanje informacija i upravljanje likvidnošću.

(3) S iznimkom uskladištenih naloga za plaćanje i informacija o statičnim podacima, samo su podaci u vezi s trenutnim radnim danom dostupni preko ICM-a. Zasloni su ponuđeni samo na engleskom jeziku.

(4) Informacije se pružaju u načinu „na upit" (engl. *pull mode*), što znači da svaki sudionik mora tražiti da mu se informacije pružaju. Sudionici redovito provjeravaju ICM tijekom radnog dana zbog važnih poruka.

(5) Dostupan je samo način „korisnik-do-aplikacije" (U2A) za sudionike koji se koriste internetskim pristupom. U2A dopušta izravnu komunikaciju između sudionika i ICM-a. Informacije se prikazuju u pregledniku koji se izvodi na PC sustavu. Daljnje su pojedinosti opisane u Priručniku za korisnike ICM-a.

(6) Svaki sudionik ima najmanje jednu radnu stanicu s internetskim pristupom radi pristupanja ICM-u preko U2A.

(7) Prava na pristup ICM-u dodjeljuju se na osnovi certifikata čija je upotreba podrobnije opisana u točkama od 11. do 14. ovog Dodatka.

(8) Sudionici mogu također upotrebljavati ICM za prijenos likvidnosti:

(a) između PM računa i sudionikovih podračuna i

(b) s PM računa na zrcalni račun koji vodi sporedni sustav.

10. UDFS, Priručnik za korisnike ICM-a i „Priručnik za korištenje usluga certificiranja javnog ključa kod internetskog pristupa"

Daljnje pojedinosti i primjeri koji objašnjavaju navedena pravila sadržani su u UDFS-u i Priručniku za korisnike ICM-a s eventualnim izmjenama koje se objavljuju na internetskoj stranici Hrvatske narodne banke i internetskoj stranici ESB-a na engleskom jeziku i u „Priručniku za korištenje usluga certificiranja javnog ključa kod internetskog pristupa".

11. Izdavanje, privremeno oduzimanje, ponovna aktivacija, opoziv i obnova certifikata

(1) Sudionik zahtijeva od Hrvatske narodne banke izdavanje certifikata kako bi mu se omogućio pristup sustavu TARGET2-HR upotrebom internetskog pristupa.

(2) Sudionik zahtijeva od Hrvatske narodne banke privremenu deaktivaciju i ponovnu aktivaciju certifikata, kao i opoziv i obnovu certifikata, kada imatelj certifikata više ne želi imati pristup sustavu TARGET2 ili ako sudionik okonča svoje aktivnosti u sustavu TARGET2-HR, na primjer zbog spajanja odnosno pripajanja ili preuzimanja.

(3) Sudionik mora primijeniti sve mjere opreza i organizacijske mjere kako bi osigurao da se certifikati upotrebljavaju prema Odluci o dodatnim i izmijenjenim uvjetima za otvaranje i funkcioniranje PM računa u sustavu TARGET2-HR upotrebom internetskog pristupa.

(4) Sudionik odmah obavješćuje Hrvatsku narodnu banku o svim bitnim promjenama svih informacija sadržanih u obrascima dostavljenima Hrvatskoj narodnoj banci u vezi s izdavanjem certifikata.

12. Sudionikovo postupanje s certifikatima

(1) Sudionik osigurava čuvanje svih certifikata i primjenjuje pouzdane organizacijske i tehničke mjere radi izbjegavanja štete trećim stranama i kako bi se osigurao da svaki certifikat upotrebljava samo imatelj certifikata kojemu je izdan.

(2) Sudionik mora odmah pružiti sve informacije koje zahtijeva Hrvatska narodna banka i jamčiti pouzdanost tih informacija. Sudionici su stalno u potpunosti odgovorni za trajnu točnost svih informacija pruženih Hrvatskoj narodnoj banci u vezi s izdavanjem certifikata.

(3) Sudionik preuzima punu odgovornost kako bi osigurao da svi njegovi imatelji certifikata drže njihove dodijeljene certifikate odvojeno od tajnih PIN i PUK kodova.

(4) Sudionik preuzima punu odgovornost kako bi osigurao da ni jedan od njegovih imatelja certifikata ne upotrebljava certifikate za funkcije ili svrhe različite od onih za koje su certifikati izdani.

(5) Sudionik je dužan odmah obavijestiti Hrvatsku narodnu banku o svakom zahtjevu i razlogu za privremenu deaktivaciju, ponovnu aktivaciju, opoziv ili obnovu certifikata.

(6) Sudionik je dužan odmah zatražiti od Hrvatske narodne banke privremenu deaktivaciju svih certifikata ili ključeva sadržanih u njima koji su neispravni ili više nisu u posjedu njihovih imatelja certifikata.

(7) Sudionik je dužan odmah obavijestiti Hrvatsku narodnu banku o svakom gubitku ili krađi certifikata.

13. Sigurnosni zahtjevi

(1) Računalni sustav kojim se sudionik koristi za pristup sustavu TARGET2 upotrebom internetskog sustava smješten je u prostorijama u vlasništvu ili najmu sudionika. Pristup sustavu TARGET2-HR može se dopustiti samo iz tih prostorija te se radi izbjegavanja nedoumica neće dopustiti pristup na daljinu.

(2) Sudionik pokreće softver na računalnom sustavu koji je postavljen i prilagođen u skladu s trenutnim međunarodnim informatičkim sigurnosnim standardima koji kao minimum uključuju zahtjeve podrobnije navedene u podtočki (3) ove točke i točki 14. podtočki (4) ovog Dodatka. Sudionik uspostavlja odgovarajuće mjere, uključujući posebnu antivirusnu zaštitu i zaštitu od zlonamjernog softvera, mjere za sprječavanje lažnog predstavljanja (engl. *anti-phishing*), očvrsnuće sigurnosti i postupke za upravljanje popravljanjem programa. Sve te mjere i postupke sudionik redovno ažurira.

(3) Sudionik uspostavlja enkriptiranu komunikacijsku vezu sa sustavom TARGET2-HR radi internetskog pristupa.

(4) Računalni računi na sudionikovim radnim stanicama ne smiju imati administratorska prava. Prava se dodjeljuju u skladu s načelom „najmanjeg prava”.

(5) Sudionik mora stalno štititi računalne sustave kojima se koristi za internetski pristup sustavu TARGET2-HR, i to na sljedeći način:

(a) Računalne sustave i radne stanice stalno štiti od neovlaštenog fizičkog i mrežnog pristupa upotrebljavajući vatrozid radi zaštite računalnih sustava i radnih stanica od dolaznog internetskog prometa i radnih stanica od neovlaštenog pristupa preko unutarnje mreže. Upotrebljava vatrozid koji štiti od dolaznog prometa, kao i vatrozid na radnim stanicama koji osigurava da samo ovlašteni programi komuniciraju prema van.

(b) Sudionicima se dopušta postavljanje na radne stanice softvera koji je potreban za pristup sustavu TARGET2 i koji je odobren na temelju sudionikove unutarnje sigurnosne politike.

(c) Sudionici stalno osiguravaju da se sve programske aplikacije koje se izvode na radnim stanicama redovito ažuriraju i popravljaju njihovom posljednjom inačicom. To se odnosi posebno na operativni sustav, internetski preglednik i priključke (engl. *plug-ins*).

(d) Sudionici stalno ograničavaju odlazni promet s radnih stanica prema poslovno kritičnim stranicama, kao i prema stranicama potrebnima za utemeljeno i razumno ažuriranje softvera.

(e) Sudionici osiguravaju da su svi kritični unutarnji tijekovi prema radnim stanicama ili od njih zaštićeni od razotkrivanja i zlonamjernih izmjena, posebno ako se datoteke prenose preko mreže.

(6) Sudionik osigurava da se njegovi imatelji certifikata stalno pridržavaju prakse sigurnog pregledavanja, uključujući:

(a) rezerviranje određenih radnih stanica radi pristupa stranicama iste kritične razine i pristupanje tim stranicama samo s tih radnih stanica,

(b) uvijek ponovo pokretati sjednice preglednika prije i nakon pristupanja sustavu TARGET2-HR preko interneta,

(c) provjeravati autentičnost svih serverskih SSL certifikata pri svakoj prijavi u sustav TARGET2-HR preko interneta,

(d) sumnjati na elektroničku poštu za koju se čini da potječe od sustava TARGET2-HR i nikada ne davati šifru certifikata ako se ta šifra traži jer sustav TARGET2-HR nikad neće tražiti šifru certifikata u elektroničkoj pošti ili na drugi način.

(7) Sudionik stalno provodi sljedeća načela upravljanja radi ublažavanja rizika za svoj sustav:

(a) uspostavljanje praksi upravljanja korisnicima koje osiguravaju da se stvaraju samo ovlašteni korisnici i ostaju u sustavu te održavanje točnog i ažuriranog popisa ovlaštenih korisnika,

(b) usklađivanje dnevnog platnog prometa radi otkrivanja odstupanja između odobrenog i stvarnog dnevnog platnog prometa, poslanog i primljenog,

(c) radi osiguranja da imatelj certifikata ne pregledava ni jednu drugu internetsku stranicu u isto vrijeme kada pristupa TARGET2-HR.

14. Dodatni sigurnosni zahtjevi

(1) Sudionik odgovarajućim organizacijskim ili tehničkim mjerama stalno osigurava da korisnički identiteti koji su razotkriveni radi kontrole pristupnih prava (engl. *Access Right Review*) nisu zlorabljeni i posebno da ni jedna neovlaštena osoba ne sazna za njih.

(2) Sudionik mora raspolagati postupkom administriranja korisnika kako bi se osiguralo neposredno i trajno brisanje odnosnog korisničkog identiteta u slučaju da zaposlenik ili drugi korisnik sustava u prostorijama sudionika napusti sudionikovu organizaciju.

(3) Sudionik mora raspolagati postupkom administriranja korisnika te odmah i trajno blokira korisničke identitete koji su na bilo koji način kompromitirani, uključujući slučajeve u kojima su certifikati izgubljeni ili ukradeni ili kada je šifra otuđena pomoću lažnog predstavljanja.

(4) Ako sudionik nakon tri pojave ne može ukloniti sigurnosne pogreške ili pogreške konfiguracije, na primjer one koje potječu od sustava zaraženog zlonamjernim softverom,

nacionalne središnje banke pružatelji SSP-a mogu trajno blokirati sudionikove korisničke identitete.

15. Stupanje na snagu i objava

Ovaj Dodatak objavljuje se na internetskim stranicama Hrvatske narodne banke, a stupa na snagu 1. veljače 2016.

O. br.: 329-020/12-15/BV
Zagreb, 21. prosinca 2015.

G U V E R N E R
HRVATSKE NARODNE BANKE

prof. dr. sc. Boris Vujčić