



НАРОДНА БАНКА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на член 47 став 1 точка 6 од Законот за Народната банка на Република Северна Македонија („Службен весник на Република Северна Македонија“ бр. 158/10, 123/12, 43/14, 153/15, 6/16, 83/18 и „Службен весник на Република Северна Македонија“ бр.110/21) и член 124 став 7 и членот 125 став 3 од Законот за платежни услуги и платни системи („Службен весник на Република Северна Македонија“ бр. 90/22), Советот на Народната банка на Република Северна Македонија донесе

ОДЛУКА **за утврдување на барањата за засилена автентикација** **и** **општи, сигурни и отворени стандарди за комуникација**

I. ОПШТИ ОДРЕДБИ

1. Со оваа одлука поблиску се пропишуваат:

- барањата за засилена автентикација помеѓу давателите на платежните услуги коишто ги одржуваат платежните сметки, давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки, плаќачите, примачите и останатите даватели на платежните услуги за целите на идентификација, автентикација, известување и информирање, заштита на доверливоста и интегритетот на корисничките сигурносни обележја на клиентот, како и исклучоците од примената на барањата за засилена автентикација и
- стандардите за поврзување и сигурна комуникација коишто треба да се применуваат при поврзување на давателот на платежните услуги којшто одржува платежна сметка и овозможува пристап до неа, директно, онлајн, со давателите на услугите за давање информации за платежните сметки, давателите на услугите за иницирање плаќања и давателите на платежните услуги при платежни трансакции засновани на картички, како и условите под кои Народната банка може да овозможи олеснета примена на стандардите за непрекинатост (континуитет).

2. Одделни изрази употребени во оваа одлука го имаат следново значење:

- **„Квалификуван сертификат за електронски печат“** е потврда за електронски печат издадена од давател на квалификувани доверливи услуги којашто ги исполнува условите пропишани со Законот за електронски документи, електронска идентификација и доверливи услуги, а коишто се однесуваат на квалификуван сертификат за електронски печат.
- **„Пренасочување на постапката за автентикација“** (англ. redirection) е метод во кој потврдата на идентитетот на корисникот на платежните услуги кон

давателите на услугите за давање информации за платежни сметки и давателите на услугите коишто иницираат плаќања автоматски се пренасочува кон инфраструктурата (интернет-страница или апликација) на давателот на платежните услуги којшто ги одржува платежните сметки заради внесување на неговите кориснички сигурносни обележја.

- **„Одвојување на постапката за автентикација“** (англ. decoupled) е метод во кој потврдата на идентитетот на корисникот на платежните услуги кон давателите на услугите за давање информации за платежни сметки и давателите на услугите коишто иницираат плаќања автоматски се пренасочува кон друг канал за комуникација поврзан со инфраструктурата на давателот на платежните услуги којшто ги одржува платежните сметки заради внесување на неговите кориснички сигурносни обележја.
- **„Вградување на постапката за автентикација“** (англ. embedded) е метод во кој корисничките сигурносни обележја на корисникот на платежната услуга им се доставени на давателите на услугите за давање информации за платежни сметки и давателите на услугите коишто иницираат плаќања за потврда на идентитетот на корисникот на платежната услуга без да се комуницира со давателот на платежните услуги којшто ги одржува платежните сметки.
- **„Сигурната околина“** ги опфаќа најмалку деловните простории на давателот на платежните услуги, интернет-опкружувањето коешто го обезбедува давателот на платежните услуги или слични безбедни интернет-страници и банкомати што ги користи давателот на платежните услуги, а не се во негова надлежност.
- **„Интерфејс“** е канал за комуникација преку кој давателот на платежната услуга којшто одржува платежни сметки овозможува стандардизирани постапки, протоколи и алатки за поврзување и сигурна комуникација, како и размена на податоци за потребите на давањето на платежните услуги и следењето на платежните трансакции.

II. ОПШТИ БАРАЊА ЗА ПРИМЕНА НА АВТЕНТИКАЦИЈА

3. Давателите на платежните услуги се должни да воспостават механизми за следење на трансакциите коишто им овозможуваат откривање неовластени или измамнички платежни трансакции, за потребата од спроведување на сигурносните мерки од точка 1, став 1, алинеја 1 од оваа одлука.

Механизмите од ставот 1 на оваа точка се засноваат на анализата на платежните трансакции во која се земаат елементи карактеристични за корисникот на платежните услуги во рамките на вообичаено користење на корисничките сигурносни обележја.

4. Давателите на платежните услуги обезбедуваат, со механизмите за следење на платежните трансакции од точката 3 став 1 од оваа одлука, да бидат опфатени најмалку секој од наведените фактори на ризик:
- евидентирани компромитирани или украдени елементи за потврда на идентитетот на корисникот на платежните услуги коишто се користат при автентикацијата;
 - износот на секоја платежна трансакција;
 - невообичаено однесување на корисникот на платежната услуга или утврдена промена во пристапот до платежната сметка, директно, онлајн (пример: измена во вообичаените интернет-адреси на пристапот или неговата брза промена на географската локација во текот на еден или повеќе канали за комуникација, т.н. невозможно патување, промена на уредот од кој се вршат плаќањата, атипични плаќања на корисникот кон одредени категории трговци, невообичаени податоци за платежните трансакции);
 - познати сценарија на измама при обезбедувањето на платежните услуги;
 - присуство на злонамерен софтвер во далечински воспоставениот канал за комуникација при постапка на автентикација.

III. СИГУРНОСНИ МЕРКИ ЗА ПРИМЕНА НА ЗАСИЛЕНА АВТЕНТИКАЦИЈА

Код за автентикација

5. Давателот на платежните услуги е должен да применува засилена автентикација на клиентот, при што засилената автентикација треба да се темели на два или повеќе елементи од следниве категории: знаење (нешто што само клиентот го знае), владение (нешто што само клиентот го поседува) и својственост (нешто што клиентот е) и треба да создаде код за автентикација.

Давателот на платежната услуга го прифаќа кодот за автентикација само еднаш за пристап до платежна сметка достапна онлајн, иницирање електронска платежна трансакција и за вршење други активности коишто се одвиваат преку средства за комуникација на далечина, коишто можат да доведат до ризик од измама при плаќање или други облици на злоупотреби.

6. За потребите од точка 5 од оваа одлука, давателите на платежните услуги се должни да воспостават сигурносни мерки со кои се обезбедува исполнување на секое од следните барања:
- неможност да се дознае информација поврзана со некој од елементите наведени во точка 5 став 1 при откривањето на кодот за автентикација;
 - неможност да се генерира нов код за автентикација, врз основа на сознание за друг таков, претходно создаден код за автентикација;
 - неможност да биде фалсификуван кодот за автентикација.
7. Давателите на платежните услуги се должни да обезбедат автентикација преку создавање соодветен код за автентикација, којшто ги вклучува наведените мерки:
- во случај кога не е успешно создавањето на кодот за автентикација, не смее да постои можност да се дознае кој од елементите од точка 5 од оваа одлука бил погрешен;
 - бројот на последователни неуспешни обиди за автентикација, по којшто пристапот привремено или трајно е оневозможен или е блокиран, не смее да биде поголем од пет во определен временски рок;
 - далечински воспоставениот канал за комуникација е заштитен од откривање на податоците при автентикацијата и од нивна употреба од страна на неовластени лица, во согласност со барањата од глава V од оваа одлука и
 - максималниот период на неактивност на плаќачот по автентикацијата не смее да биде подолг од пет минути.
8. Доколку настане привремено оневозможување или блокирање на пристапот во согласност со точка 7 став 1, алинеја 2, давателот на платежните услуги е должен да ги утврди времетраењето и бројот на повторни обиди според карактеристиките на услугата којашто му се обезбедува на плаќачот, ризиците поврзани со таа услуга, земајќи ги предвид најмалку факторите на ризик наведени во точка 4 од оваа одлука.
- Давателот на платежните услуги е должен да го информира плаќачот за блокирањето на електронскиот платен инструмент пред тоа да стане трајно, а доколку тоа не е можно, веднаш по блокирањето.
- Доколку блокирањето е трајно, давателот на платежните услуги е должен да воспостави сигурносна процедура со која ќе ја отстрани блокадата на електронскиот платен инструмент или да го замени блокираниот електронски платен инструмент со нов.

Динамичко поврзување

9. Во случај кога давателите на платежните услуги применуваат засилена автентикација на клиентот, како дополнувања на барањата од точките 5, 6, 7 и 8 од оваа одлука, тие се должни да воспостават и сигурносни мерки коишто ги исполнуваат следните барања:
- плаќачот е известен за износот на платежната трансакција и за примачот на плаќањето;
 - создадениот код за автентикација е определен специфично за износот на платежната трансакција и примачот на плаќањето коишто плаќачот ги назначил при иницирањето на трансакцијата;

- кодот за автентикација којшто е прифатен од давателот на платежната услуга одговара на оригиналниот наведен износ на платежната трансакција и на идентитетот на примачот на плаќањето назначен од плаќачот;
- секоја промена на износот на платежната трансакција или примачот на плаќањето доведува до поништување на создадениот код за автентикација.

За целите на став 1 од оваа точка, давателите на платежните услуги воспоставуваат сигурносни мерки со кои се обезбедува доверливост, автентичност и интегритет за секоја од следниве информации:

- износот на платежната трансакција и примачот на плаќањето во сите фази на автентикацијата и
- информациите коишто му се прикажани на плаќачот во сите фази на автентикација, вклучувајќи го создавањето, преносот и користењето на кодот за автентикација.

За целите на став 1, алинеја 2 од оваа точка и доколку давателите на платежните услуги применуваат засилена автентикација на клиентите се применуваат следниве барања за кодот на автентикација:

- кај платежните трансакции засновани на картички, за кои плаќачот дал согласност за резервирање точен износ на парични средства, кодот за автентикација е определен специфично за износот за којшто плаќачот дал согласност за резервирање при иницирањето на трансакцијата;
- кај платежните трансакции за кои плаќачот дал согласност да се извршат како серија / група електронски платежни трансакции наменети за еден или повеќе примачи на плаќањата, кодот за автентикација е определен специфично со вкупниот износ на серијата на платежните трансакции и наведените примачи на плаќањата во серијата / групата.

Барања за елементите категоризирани како знаење

10. Давателите на платежните услуги се должни да воспостават мерки за намалување на ризикот од откривање или обелоденување на елементите од категоријата знаење од или на неовластени лица.

Употребата на елементите категоризирани како знаење од страна на плаќачот подлежи на примена на мерки за намалување на ризикот од нивно откривање од страна на неовластени лица.

Барања за елементите категоризирани како владение

11. Давателите на платежните услуги се должни да воспостават мерки за намалување на ризикот од користење на елементите од категоријата владение од страна на неовластени лица.

Употребата на елементите категоризирани како владение од страна на плаќачот подлежи на примена на мерки коишто имаат за цел да се спречи нивно репродуцирање.

Барања за уредите и софтверот коишто се поврзани со елементите категоризирани како својственост

12. Давателите на платежните услуги се должни да воспостават мерки за намалување на ризикот од користење на елементите од категоријата својственост од неовластени лица, а коишто се вчитуваат на уреди и софтвер за таа намена, доставени на плаќачот.

Употребата на елементите категоризирани како својственост од страна на плаќачот подлежи на примена на мерки коишто се наменети за спречување неовластен пристап, како и гарантирање на отпорноста на уредите и софтверот на кои се вчитуваат.

Независност на елементите

13. Давателите на платежните услуги коишто применуваат засилена автентикација на клиентите преку употреба на елементите во согласност со точките 10, 11 и 12 од оваа одлука, се должни да воспостават мерки со кои се обезбедува откривањето на тајноста на еден од елементите да не доведе до загрозување на останатите.

Давателите на платежните услуги при употребата на кој било елемент од засилената автентикација или при создавањето код за автентикација преку користење повеќенаменски уред, се должни да воспостават сигурносни мерки за намалување на ризикот од злоупотреба на уредот.

За потребите од став 2 од оваа точка, давателите на платежните услуги за намалување на ризикот ги применуваат следниве мерки:

- користење одделни сигурни околинис за извршување со помош на софтверот инсталиран на повеќенаменскиот уред;
- механизми со кои се заштитува софтверот или уредот од промени од страна на плаќачот или од трето лице и
- во случај на утврдена промена на софтверот или уредот, постоење на механизми за намалување на последиците од неа.

IV. ИСКЛУЧОЦИ ОД ПРИМЕНАТА НА ЗАСИЛЕНАТА АВТЕНТИКАЦИЈА НА КЛИЕНТОТ

Информации за платежната сметка

14. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука и кога корисникот на платежната услуга има пристап до платежната сметка од далечина, директно, онлајн, без објавување чувствителни податоци за плаќањата, во случаите кога се бара информација за:

- состојбата на една или повеќе назначени платежни сметки, или
- извршените платежни трансакции во последните 90 дена преку назначените платежни сметки од страна на корисникот.

15. За целите на примената на точката 14 од оваа одлука, давателите на платежните услуги не може да применуваат исклучок од засилената автентикација на клиентот, доколку е исполнет барем еден од следниве услови:

- корисникот на платежната услуга за првпат пристапува од далечина, директно, онлајн, до информациите од точка 14 од оваа одлука;
- поминати се повеќе од 90 дена од последниот пат кога корисникот на платежната услуга пристапил далечински, директно, онлајн, до информациите наведени во точка 14, став 1, алинеја 2 од оваа одлука, со примена на засилената автентикација.

Бесконтактни плаќања на терминали на продажно место

16. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука и доколку плаќачот иницира бесконтактна електронска платежна трансакција преку средствата за комуникација на далечина под наведените услови:

- поединечниот износ на бесконтактната електронска платежна трансакција преку средствата за комуникација на далечина не надминува 3000 денари;
- вкупниот износ на претходните бесконтактни електронски платежни трансакции иницирани со помош на платниот инструмент којшто поседува бесконтактна функционалност во периодот од датумот на последната примена на засилената автентикација на клиентот не надминува 9000 денари; или
- бројот на последователни бесконтактни електронски платежни трансакции иницирани преку платниот инструмент којшто поседува бесконтактна функционалност во периодот од последната примена на засилената автентикација не е поголем од пет.

Самоуслужни терминали за плаќање на услугите за превоз и надоместок за паркирање

17. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука и доколку плаќачот иницира електронска платежна трансакција преку средствата за комуникација на далечина на самоуслужен терминал за потребите на плаќањето на услугите за превоз или надоместок за паркирање.

Листа на одобрени примачи на плаќањето

18. Давателите на платежните услуги применува засилена автентикација на клиентот во случај кога плаќачот изготвува или менува листа на одобрени примачи на плаќањето, преку давателот на платежните услуги којшто ја одржува платежната сметка.

На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука, ако плаќачот иницира платежна трансакција, а примачот на плаќањето е дел од листата од став 1 од оваа точка.

Повторување трансакции

19. Давателите на платежните услуги применуваат засилена автентикација на клиентот, ако плаќачот изготвува, менува или за првпат иницира серија повторливи електронски платежни трансакции со ист износ и ист примач на плаќањето.

На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука, при иницирањето на секоја идна платежна трансакција како дел од последователната серија на платежните трансакции од став 1 од оваа точка.

Кредитни трансфери помеѓу сметки на исто физичко или правно лице

20. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, под услов да ги почитуваат барањата дефинирани со точка 4 од оваа одлука, доколку плаќачот иницира кредитен трансфер и притоа плаќачот и примачот се исто физичко или правно лице и тие сметки се одржуваат од ист давател на платежните услуги што одржува платежни сметки.

Трансакции со мала вредност

21. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, доколку при иницирањето електронска платежна трансакција преку средствата за комуникација на далечина, за која се исполнети следниве услови:
- износот на електронската платежна трансакција преку средствата за комуникација на далечина не надминува 1200 денари; и
 - вкупниот износ на претходните електронски платежни трансакции преку средствата за комуникација на далечина коишто плаќачот ги иницирал од последната примена на засилената автентикација на клиентот не надминува 6000 денари или
 - бројот на претходните електронски платежни трансакции преку средствата за комуникација на далечина коишто плаќачот ги иницирал од последната примена на засилена автентикација на клиентот не надминува пет последователни електронски платежни трансакции преку средствата за комуникација на далечина.

Корпоративни сигурносни постапки и протоколи на плаќања

22. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентите правни лица коишто иницираат електронски платежни трансакции со помош на наменски постапки и протоколи на плаќање коишто им се достапни само на плаќачите кои не се потрошувачи, доколку тие постапки или протоколи гарантираат еквивалентно ниво на сигурност во согласност со Законот.

Анализа на ризикот од трансакција

23. На давателите на платежните услуги им е дозволено да применуваат исклучок од засилената автентикација на клиентот, доколку плаќачот иницира електронска платежна трансакција преку средствата за комуникација на далечина, за која давателот на платежните услуги утврдил дека е со низок ризик, во согласност со механизмите за следење на трансакциите предвидени со точка 4 став 1 алинеја 4 од оваа одлука.

Платежната трансакција од став 1 од оваа точка е со низок ризик, ако се исполнети следниве услови:

- стапката на измама за тој тип трансакција, пресметана во согласност со точка 24 и известувањата од давателот на платежните услуги, е еднаква или пониска од референтната стапка на измама, наведени во табелата во Анексот бр. 1, којшто е во прилог на оваа одлука за ставките „електронски платежни трансакции со платен инструмент заснован на картичка“ и „електронски кредитни трансфери“ соодветно;
- износот на трансакцијата не го надминува соодветниот вредносен праг за исклучок наведен во табелата од Анексот бр. 1, во прилог на оваа одлука;
- давателите на платежните услуги по извршената анализа на ризикот во реално време не утврдиле ниту една од следниве појави: невообичаено плаќање или однесување на плаќачот; информации за невообичаено користење на уредот / софтверот за пристап на плаќачот; присуство на злонамерен софтвер во кој било далечински воспоставен канал за комуникација во процесот на автентикација; познати сценарија на измама при давањето на платежните услуги; невообичаена локација на плаќачот; и високоризична земја на примачот.

Давателите на платежните услуги коишто имаат намера да применуваат исклучок од засилената автентикација на клиентите за електронска платежна трансакција преку средствата за комуникација од далечина, врз основа на став 2 од оваа точка, се должни да ги земат предвид најмалку следниве фактори на ризик:

- претходни шеми на трошење на поединечните корисници на платежните услуги;
- историјата на платежните трансакции на секој од корисниците на платежните услуги коишто ги нуди давателот на платежните услуги;
- локацијата на плаќачот и земјата на примачот за времетраење на платежната трансакција преку средствата за комуникација на далечина во случај кога уредите или софтверот за пристап се овозможени од страна на давателот на платежната услуга;
- утврдување на невообичаени шеми на плаќања од страна на корисникот на платежните услуги имајќи ја предвид неговата историја на плаќањата.

Давателот на платежните услуги е должен да ги комбинира сите наведени фактори на ризик при пресметката на вкупната оценка на ризикот за секоја трансакција, за да утврди дали за тоа плаќање треба да примени засилена автентикација.

Пресметка на стапката на измама

24. Давателот на платежната услуга за секој вид трансакција наведена во табелата во Анексот бр. 1, во прилог на оваа одлука, обезбедува вкупните стапки на измама коишто

се однесуваат и на платежните трансакции коишто се потврдени со примената на засилената автентикација на клиентот и на оние коишто се извршуваат во согласност со примената на исклучоците наведени во точките 18, 19, 20, 21, 22 и 23 од оваа одлука, да се еднакви или пониски од референтната стапка на измама за истиот вид платежна трансакција наведени во табелата во Анексот бр. 1, во прилог на оваа одлука.

Вкупната стапка на измама за секој вид трансакција наведена во табелата во Анексот бр. 1, во прилог на оваа одлука, се пресметува на квартална основа, како вкупна вредност на сите неовластени или измамнички трансакции преку средствата за комуникација од далечина, без разлика дали има поврат на парични средства, поделена со вкупната вредност на сите електронски платежни трансакции преку средства за комуникација на далечина за истиот вид трансакции, без разлика дали е применета засилената автентикација на клиентите или се извршени со примена на исклучоците наведени во точките 18, 19, 20, 21, 22 и 23 од оваа одлука.

Пресметката на стапките на измама од ставот 2 на оваа точка е предмет на ревизорски преглед предвиден со точка 27 од оваа одлука со кој се обезбедува нивната целосност и точност.

Методологијата и моделот за пресметка на стапките на измама коишто се користат од страна на давателот на платежните услуги, како и стапките на измама соодветно се документираат и се достапни на барање на Народната банка.

Престанок на примената на исклучоците од анализата на ризикот на трансакциите

25. Давателите на платежните услуги коишто ги применуваат исклучоците од точка 23 од оваа одлука веднаш ја известуваат Народната банка, доколку една од стапките за следење на измамите за кој било од видовите на платежните трансакции наведени во табелата во Анексот бр. 1, во прилог на оваа одлука, ја надминува важечката референтна стапка на измама и притоа доставуваат опис на мерките што ќе ги преземат за повторно да се обезбеди усогласеност на стапката на измама којашто ја следат со важечките референтни стапки на измама.

Давателите на платежните услуги се должни веднаш да прекинат да ги применуваат исклучоците наведени во точка 23 од оваа одлука, за сите видови платежни трансакции наведени во табелата во Анексот бр. 1, во прилог на оваа одлука, во одредениот праг на исклучок, доколку стапката на измама којашто ја следат за времетраење на два последователни квартала ја надминува референтната стапка на измама што се применува за тој вид електронска платежна трансакција во прагот на исклучок.

По престанувањето со примената на исклучоците од точка 23 од оваа одлука и во согласност со ставот 2 од оваа точка, давателите на платежните услуги не смеат повторно да го користат тој исклучок, сè додека нивната пресметана стапка на измама не е еднаква или е под референтните стапки на измама за тој вид платежна трансакција наведени во табелата во Анексот бр. 1, во прилог на оваа одлука, во тој праг на исклучок во текот на еден квартал.

Доколку давателите на платежните услуги имаат намера повторно да го применуваат исклучокот наведен во точка 23 од оваа одлука, пред да почнат да го применуваат во разумен рок, ја известуваат Народната банка со доказ за повторна усогласеност на

нивната стапка на измама, со применливата референтна стапка на измама за тој праг за исклучок, во согласност со став 3 од оваа точка.

Следење

26. За да може да се применуваат исклучоците од точките 14, 15, 16, 17, 18, 19, 20, 21, 22 и 23 од оваа одлука, давателите на платежните услуги ги евидентираат и ги следат следниве податоци за секој вид платежни трансакции, со поделба на платежните трансакции коишто се извршуваат преку средствата за комуникација од далечина и оние коишто не се извршуваат преку средствата за комуникација на квартална основа:
- вкупната вредност на неавторизираните или измамничките платежни трансакции, вкупната вредност на сите платежни трансакции и пресметаните стапки на измама, вклучувајќи распределба на платежните трансакции коишто се иницирани со примена на засилена автентикација и во рамките на секој исклучок;
 - просечна вредност на платежните трансакции, вклучувајќи и распределба на платежните трансакции иницирани со примена на засилена автентикација на клиентот и во рамките на секој исклучок;
 - број на платежните трансакции за кои се примениле исклучоци и нивниот процент во однос на вкупниот број платежни трансакции.

Давателите на платежните услуги ги доставуваат резултатите од следењето во согласност со ставот 1 од оваа точка, на барање на Народната банка.

Ревидирање

27. Давателите на платежните услуги коишто применуваат исклучок од засилената автентикација, во согласност со точка 23 од оваа одлука, се должни да спроведат ревизија на методологијата, моделот и на пријавените стапки на измама.

Давателите на платежните услуги се должни да ја извршат ревизијата од став 1 од оваа точка првата година по примената на исклучоците од точка 23 од оваа одлука и најмалку на секои следни три години или почесто, или на барање на Народната банка.

V. ДОВЕРЛИВОСТ И ИНТЕГРИТЕТ НА КОРИСНИЧКИТЕ СИГУРНОСНИ ОБЕЛЕЖЈА

Општи барања

28. Давателите на платежните услуги обезбедуваат доверливост и интегритет на корисничките сигурносни обележја на корисниците на платежните услуги, вклучувајќи ги и кодовите за автентикација, за време на сите фази на автентикација.

За потребите на ставот 1 од оваа точка, давателите на платежните услуги се должни да ги исполнат следниве барања:

- корисничките сигурносни обележја се прикриени и не се во целост читливи, при внесување од страна на корисникот на платежните услуги за целите на автентикација;

- корисничките сигурносни обележја во податочен формат и криптографските материјали коишто се однесуваат на нивното шифрирање не се снимаат во читлив формат;
- тајниот криптографски материјал е заштитен од неовластено откривање.

Давателите на платежните услуги ја документираат постапката на управување со криптографскиот материјал, со којшто корисничките сигурносни обележја се шифрираат или на друг начин се прават нечитливи.

Давателите на платежните услуги се должни да обезбедат обработката и пренасочувањето на корисничките сигурносни обележја и кодовите за автентикација коишто се создадени во согласност со главата III од оваа одлука, да се одвиваат во сигурна околина и во согласност со соодветни и широко прифатени индустриски стандарди усвоени од меѓународни или европски тела за стандардизација.

Изготвување и доставување на корисничките сигурносни обележја

29. Давателите на платежните услуги се должни да обезбедат изготвувањето на корисничките сигурносни обележја да биде во сигурна околина.

Давателите на платежните услуги ги намалуваат ризиците од неовластено користење на корисничките сигурносни обележја, уредите и софтверот за автентикација по нивно губење, кражба или нивно копирање пред да бидат доставени до плаќачот.

Поврзување со давателот на платежната услуга

30. Давателите на платежните услуги обезбедуваат дека само корисникот на платежната услуга е поврзан, на сигурен начин, со доделените кориснички сигурносни обележја на уредите и софтверот за автентикација.

За целите на став 1 од оваа точка, давателите на платежните услуги ги исполнуваат следниве барања:

- поврзувањето на идентитетот на корисникот на платежните услуги со корисничките сигурносни обележја, уредите и софтверот за автентикација се изведува во сигурна околина за која е одговорен давателот на платежните услуги;
- поврзувањето на идентитетот на корисникот на платежните услуги со корисничките сигурносни обележја и софтверот за автентикација, преку средствата за комуникација на далечина се врши со примена на засилена автентикација.

Доставување на корисничките сигурносните обележја, уреди и софтвер за автентикација

31. Давателите на платежните услуги се должни да обезбедат доставувањето на корисничките сигурносни обележја, уредите и софтверот за автентикација на корисниците на платежните услуги да се одвива на сигурен начин, имајќи ги предвид

ризиците поврзани од неовластено користење во случај на нивно губење, кражба или копирање.

За целите на ставот 1 од оваа точка, давателите на платежните услуги ги применуваат следниве мерки:

- ефикасни и безбедни постапки за доставување со кои се обезбедува корисничките сигурносни обележја, уреди и софтвер за автентикација да се доставуваат до легитимниот корисник на платежните услуги;
- механизми коишто на давателот на платежните услуги му овозможуваат проверка на автентичноста на софтверот за автентикација, којшто на корисникот на платежните услуги му е испорачан преку јавно достапна комуникациска мрежа, како што е интернет;
- постапките за испорака во случај кога корисничките сигурносни обележја се испорачуваат надвор од просториите на давателот на платежните услуги или преку средствата на комуникација на далечина, со кои се обезбедува: неовластено лице да не може да добие повеќе од едно корисничко сигурносно обележје и уреди или софтвер за автентикација кога се испорачуваат преку ист канал; испорачаните кориснички сигурносни обележја, уреди и софтвер за автентикација задолжително бараат нивна активација пред да бидат употребени;
- постапките за задолжителна активација на корисничките сигурносни обележја и уреди или софтвери за автентикација, пред нивната прва употреба, овозможуваат нивно активирање во сигурна околина, во согласност со постапките за поврзување од точка 30 од оваа одлука.

Обновување на корисничките сигурносни обележја

32. Давателите на платежните услуги се должни да обезбедат обновувањето или повторното активирање на корисничките сигурносни обележја да е во согласност со постапките за издавање, поврзување и доставување на корисничките сигурносни обележја и уредите за автентикација дефинирани во точките 29, 30 и 31 од оваа одлука.

Уништување, деактивација и отповикување

33. Давателите на платежните услуги обезбедуваат ефикасни процеси за примена на следниве сигурносни мерки:

- сигурно уништување, деактивација или отповикување на корисничките сигурносни обележја, уредите и софтверот за автентикација;
- доколку давателот на платежните услуги доставува уред и софтвер за автентикација за повеќекратна употреба, пред повторното користење од друг корисник на платежните услуги се воспоставува, се документира и се спроведува сигурно повторно користење на уредот или софтверот;
- деактивација или отповикување на информациите поврзани со корисничките сигурносни обележја, коишто се чуваат во системите и базите на податоци на давателите на платежните услуги и во зависност од случаите и во други јавни регистри.

VI. ОПШТИ, СИГУРНИ И ОТВОРЕНИ СТАНДАРДИ ЗА КОМУНИКАЦИЈА

Општи барања за идентификација при комуникација

34. Давателите на платежните услуги се должни да обезбедуваат сигурна идентификација за време на комуникацијата помеѓу уредот на плаќачот и уредот на примачот којшто прифаќа електронски платежни трансакции и вклучувајќи ги меѓу останатите и терминалите за плаќање.

Давателите на платежните услуги обезбедуваат ефикасно намалување на ризикот од погрешно насочување на комуникацијата кон неовластени лица при користење мобилни апликации и други интерфејси коишто на корисникот на платежните услуги му нудат платежни услуги.

Општи барања за следење на платежните трансакции при комуникација

35. Давателите на платежните услуги воспоставуваат постапки со кои се обезбедува следење на сите платежни трансакции и останати интеракции помеѓу корисникот на платежните услуги, другите даватели на платежните услуги и субјекти, вклучувајќи ги и трговците, при обезбедувањето на платежните услуги и обезбедува информации за сите значајни настани за електронски платежни трансакции во сите фази од нивното извршување и нивна достапност по извршувањето на трансакциите.

За целите од ставот 1 на оваа точка, давателите на платежните услуги се должни да обезбедат дека секој канал за комуникација којшто е воспоставен кон корисникот на платежните услуги, другите даватели на платежните услуги и субјекти, вклучувајќи ги и трговците, ги содржи следниве ставки:

- единствена идентификациска ознака на каналот за комуникација;
- детално евидентирање на трансакцијата, вклучувајќи број на трансакција, електронски временски жиг и останати релевантни податоци за трансакцијата.

Посебни барања за општите, сигурни и отворени стандарди за комуникација

Интерфејси за пристап

36. Давателите на платежните услуги коишто ги одржуваат платежните сметки, а коишто на плаќачот му овозможуваат пристап до платежна сметка, директно, онлајн, воспоставуваат најмалку еден интерфејс којшто ги исполнува следниве барања:

- давателите на услугите за давање информации за платежните сметки, давателите на услугите за иницирање плаќања и давателите на платежните услуги што издаваат платни инструменти засновани врз картички, се идентификуваат кон давателот на платежните услуги којшто ја одржува платежната сметка;
- давателите на услугите за давање информации за платежните сметки комуницираат на сигурен начин кога бараат и примаат информации за една или повеќе назначени платежни сметки и платежните трансакции поврзани со нив;

- давателите на услугите за иницирање плаќања комуницираат на сигурен начин при иницирање платен налог од платежната сметка на плаќачот, прием на повратна информација при иницирањето на платежната трансакција и сите информации за извршувањето на платежната трансакција коишто се достапни до давателите на платежните услуги коишто ја одржуваат платежната сметка.

37. За потребите на автентикација на корисниците на платежните услуги, интерфејсот дефиниран во точка 36 од оваа одлука, на давателите на услугите за давање информации за платежни сметки и давателите на услугите за иницирање на плаќањата, им овозможува да се потпрат на постапките за автентикација коишто давателот на платежните услуги којшто ја одржува платежната сметка му ги дава на корисникот на платежните услуги.

Интерфејсот за пристап ги исполнува најмалку следниве барања:

- врз основа на дадена согласност од корисникот на платежната услуга, давателот на услугите за иницирање плаќања или давателот на услугите за давање информации за платежни сметки, му наложува на давателот на платежните услуги којшто ја одржува платежната сметка да започне со постапка на автентикација;
- каналите за комуникација помеѓу давателот на платежните услуги којшто ја одржува платежната сметка, давателот на услугите за давање информации за платежни сметки, давателот на услугите за иницирање плаќања и кој било корисник на платежните услуги се воспоставуваат и се одржуваат за време на постапката на автентикација;
- обезбедува интегритет и доверливост на корисничките сигурносни обележја и кодовите за автентикација пренесувани од или преку давателот на услугите за иницирање плаќања или давателот на услугите за давање информации за платежните сметки.

38. Давателите на платежните услуги коишто ги одржуваат платежните сметки се должни да ги усогласат своите интерфејси со стандардите за структурата на податоците и нивните модели, протоколите на апликативно, транспортно и авторизациско ниво, со примена на широко прифатени индустриски стандарди усвоени од меѓународни или европски тела за стандардизација.

Давателите на платежните услуги коишто ги одржуваат платежните сметки обезбедуваат техничка документација за своите интерфејси, со наведување на збирот од постапките, протоколите и алатките коишто им се потребни на давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и на давателите на платежните услуги за издавање платни инструменти засновани на картичка, за воспоставување интероперабилност помеѓу сопствените системи со системите на давателите на платежните услуги коишто ги одржуваат платежните сметки.

Давателите на платежните услуги коишто ги одржуваат платежните сметки на барање на давателите на услугите за иницирање плаќања, даватели на услугите за давање информации за платежните сметки, давателите на платежните услуги за издавање платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции или давателот на платежните услуги кој поднесол барање за

добивање дозвола за давање платежни услуги, без надоместок да ја стават на располагање документацијата од став 2 на оваа точка и на својата јавна интернет-страница да објават резиме од документацијата, најмалку пет месеци пред датумот на примена наведен во точка 67 од ова одлука или пред предвидениот датум за започнување на употреба на интерфејсот, доколку датумот на започнување на употреба на интерфејсот е по датумот наведен во истата точка.

39. Давателите на платежните услуги коишто ги одржуваат платежните сметки обезбедуваат сите промени на техничката документација за своите интерфејси да бидат достапни до давателите на услугите за иницирање плаќања, даватели на услугите за давање информации за платежните сметки, давателите на платежните услуги коишто издаваат платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции или давателот на платежните услуги кој поднесол барање за добивање дозвола за давање платежни услуги, освен во вонредни услови.

Промената на техничката документација за интерфејсот ќе биде достапна колку што е можно порано, а најмалку три месеци пред да се спроведе промената.

Давателите на платежните услуги во случај на измени во интерфејсот наметнати од вонредни услови се должни да ги документираат постапките и на барање да ги достават до Народната банка.

40. Давателите на платежните услуги коишто ги одржуваат платежните сметки се должни да обезбедат техничка платформа и поддршка, заради тестирање на поврзувањето и функционалностите на софтверите и апликациите на давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки, на давателите на платежните услуги коишто издаваат платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции или давателот на платежните услуги кој поднесол барање за добивање дозвола за давање платежни услуги.

Техничката платформата за тестирање треба да биде достапна најмалку пет месеци пред датумот на примена наведен во точка 67 од оваа одлука или пред предвидениот датум за започнување на употребата на интерфејсот, ако датумот на започнување на употреба на интерфејсот е по датумот наведен во истата точка.

На техничката платформа за тестирање не смее да се споделуваат чувствителни податоци за плаќања.

Користење интерфејси

41. Давателите на платежните услуги коишто ги одржуваат платежните сметки воспоставуваат интерфејс, во согласност со барањата од точките 36, 37, 38, 39 и 40 од оваа одлука, преку:
- обезбедување наменски интерфејс или
 - користење на интерфејсот на давателите на платежните услуги од точка 36 од оваа одлука, којшто се применува за автентикација и комуникација со корисниците на платежните услуги којшто тој го обезбедува.

Барања за наменскиот интерфејс

42. Под услов да се исполнети барањата од точките 36, 37, 38, 39, 40 и 41 од оваа одлука, давателите на платежните услуги коишто ги одржуваат платежните сметки коишто воспоставиле наменски интерфејс се должни да го обезбедат истото ниво на расположливост, ефикасност, вклучително и поддршка, како и за интерфејсот којшто се користи за пристап на корисниците на платежните услуги до платежната сметка, директно, онлајн.

43. Давателите на платежните услуги коишто ги одржуваат платежните сметки, коишто воспоставиле наменски интерфејс, дефинираат транспарентни клучни показатели за ефикасност и целно ниво на услуги, кои и во поглед на расположливоста и разменетите податоци согласно точките 62, 63, 64, 65 и 66 од оваа одлука, се еднакво строги, како оние за интерфејсот кој го користат корисниците на нивните платежни услуги.

При следењето на нивото на услуги, расположливоста и ефикасноста, давателите на платежните услуги коишто ги одржуваат платежните сметки ги следат насоките дадени во Анексот бр. 2, прилог на оваа одлука.

44. Давателите на платежните услуги коишто ги одржуваат платежните сметки и воспоставиле наменски интерфејс се должни да обезбедат тој да не создава попречувања во обезбедувањето на услугите за иницирање плаќања и услуги за давање информации за платежните сметки.

Како попречувања од став 1 на оваа точка, се третираат следниве случаи:

- кога давателите на платежните услуги од точка 36 од оваа одлука немаат можност да ги употребуваат корисничките сигурносни обележја, коишто давателите на платежните услуги коишто ги одржуваат платежните сметки им ги доставиле на своите корисници;
- барања за повторна автентикација;
- барања за дополнителна проверка на дозволите впишани во регистарот на платежните институции;
- барања за дополнителна проверка за дадена согласност којашто корисниците на платежните услуги им ја дале на давателите на услугите за иницирање плаќања и давателите на услугите за давање информации за платежните сметки.

Давателот на платежните услуги којшто ги одржува платежните сметки е должен на барање на Народната банка да достави извештај дека наменскиот интерфејс не создава попречување при обезбедувањето на услугите за иницирање плаќања и услуги за давање информации за платежните сметки, во согласност со насоките од Анексот бр. 5, во прилог на оваа одлука.

45. За потребите на точките 42 и 43 од оваа одлука, давателите на платежните услуги коишто ги одржуваат платежните сметки ја следат расположливоста и ефикасноста на наменскиот интерфејс.

Давателите на платежните услуги коишто ги одржуваат платежните сметки објавуваат на својата интернет-страница квартални статистички податоци за расположливоста и

ефикасноста на наменскиот интерфејс и на интерфејсот којшто го користат неговите корисници на платежните услуги.

При објавувањето на статистичките податоци за расположливоста и ефикасноста на наменскиот интерфејс и интерфејсот којшто го користат неговите корисници на платежните услуги, давателите на платежните услуги коишто ги одржуваат платежните сметки ги следат насоките дадени во Анексот бр. 3, во прилог на оваа одлука.

46. Давателот на платежните услуги којшто ги одржува платежните сметки е должен да спроведе стрес-тестирање на отпорноста на наменскиот интерфејс, според насоките дадени во Анексот бр. 4, во прилог на оваа одлука.

Во рамките на стрес-тестирањето на отпорноста давателите на платежните услуги коишто ги одржуваат платежните сметки се должни да го утврдат влијанието коешто го имаат врз расположливоста и ефикасноста на наменскиот интерфејс и дефинираното ниво на услуга.

Давателот на платежните услуги којшто ги одржува платежните сметки е должен, на барање на Народната банка, да достави сумарен извештај од резултатите од последното спроведено стрес-тестирањето на отпорноста, како и информација за начините со кои се надминати утврдените слабости.

Стандарди за непрекинатост за наменски интерфејс и услови за олеснета примена

47. Давателите на платежните услуги коишто ги одржуваат платежните сметки при дизајнирањето на наменскиот интерфејс вклучуваат стандарди за непрекинатост, преку развивање стратегија, планови за непрекинатост, во случај кога наменскиот интерфејс не функционира во согласност со барањата од точките 42, 43, 44, 45 и 46 од оваа одлука, односно кога е непланирано недостапен или во случај на прекин на неговите системи.

Интерфејсот е непланирано недостапен или се случил прекин на неговите системи, доколку не одговори во рок од 30 секунди на пет последователни барања за пристап до информации за услугите за иницирање плаќање или за давање информации за платежните сметки.

48. Во планот за непрекинатост во работењето е опишан начинот на информирање на давателите на платежните услуги којшто го користат наменскиот интерфејс, за мерките за повторно воспоставување на системите и опис на непосредно достапни можности коишто им се на располагање на давателите на платежните услуги.

49. Давателите на платежните услуги коишто ги одржуваат платежните сметки и давателите на платежните услуги од точка 36 од оваа одлука, се должни без одлагање да ги пријават проблемите кои се јавуваат со наменскиот интерфејс, наведени во точка 47 од оваа одлука и информациите поврзани со надминување на појавените проблеми согласно насоките од Анекс бр.8, прилог на оваа одлука до Народната банка.

50. Како дел од стандардите за непрекинатост, за функционирање во вонредни услови, давателите на платежните услуги од точка 36 од оваа одлука, може да ги користат

интерфејсите кои на корисниците на платежните услуги им се ставени на располагање за автентикација и комуникација со давателот на платежните услуги којшто ги одржува платежните сметки, се додека не се обезбеди потребното ниво на расположливост и ефикасност на наменскиот интерфејс согласно точките од 42 до 46 од оваа одлука.

51. За потребите на точка 50 од оваа одлука, давателите на платежните услуги коишто ги одржуваат платежните сметки обезбедуваат давателите на платежните услуги од точка 36 од оваа одлука, да се идентификуваат со постапките за автентикација кои давателите на платежните услуги коишто ги одржуваат платежните сметки ги обезбедуваат на корисникот на платежните услуги.

Доколку давателите на платежните услуги од точка 36 од оваа одлука го користат интерфејсот од точка 50 од оваа одлука се должни:

- да преземат неопходни мерки со кои се обезбедува дека не пристапуваат, не складираат или не обработуваат податоци за други цели, освен за обезбедување на услугата којашто е побарана од корисникот на платежните услуги;
- да продолжат да ги исполнуваат законските обврски во врска со правилата за пристап до платежната сметка во случај на иницирање плаќање и при добивање информации за платежната сметка;
- да евидентираат податоци до кои се пристапува преку интерфејсот којшто давателот на платежната услуга којшто ги одржува платежните сметки го одржува за потребите на корисниците на своите платежни услуги и на барање и без одлагање, да ги достават записите од евидентирани податоци до Народната банка;
- на барање на Народната банка и без неоправдано одлагање, да го објаснат начинот на користењето на интерфејсот којшто на корисниците на платежните услуги им е даден за користење при пристап до нивната платежна сметка, директно, онлајн;
- на соодветен начин да ги информираат давателите на платежните услуги коишто ги одржуваат платежните сметки.

52. Доколку давателите на платежните услуги коишто ги одржуваат платежните сметки се одлучиле за користење наменски интерфејс со олеснета примена на стандардите за непрекинато за кој не се применуваат барањата од точка 50 од оваа одлука, треба да го исполнат следново:

- усогласеност со барањата за наменскиот интерфејс од точка 42 до точка 46 од оваа одлука;
- наменскиот интерфејс да е дизајниран и тестиран во согласност со барањата од точка 40 од оваа одлука;
- наменскиот интерфејс имал широка употреба од давателите на платежните услуги при услуги за давање информации за платежна сметка, за иницирање плаќања и за потврда на расположливите средства за плаќања со платежни картички, во период од најмалку три месеци;
- сите проблеми коишто се појавиле во функционирањето на наменскиот интерфејс се надминати без неоправдано одлагање.

Давателот на платежните услуги којшто ги одржува платежните сметки е должен на барање на Народната банка, да обезбедат потврда за исполнетост на барањата од став

1 на оваа точка, во согласност со насоките од Анексот бр. 6, Анексот бр. 7 и Анексот бр. 8, во прилог на оваа одлука.

53. Доколку давателите на платежните услуги коишто ги одржуваат платежните сметки не ги исполнуваат во целост барањата од точка 52 во период поголем од две последователни календарски недели, тие се должни во најкраток можен рок, а најдоцна во рок од два месеци, да воспостават постапки за примена на стандардите за непрекинатост од точка 50 од оваа одлука.

Сертификати

54. За потребите на идентификацијата од точка 36 став 1 алинеја 1 од оваа одлука, давателите на платежните услуги користат квалификувани сертификати за електронски печат или квалификуван сертификат за автентичност на интернет-страница, во согласност со Законот за електронски документи, електронска идентификација и доверливи услуги.
55. Квалификуваните сертификати за електронски печати или за автентичност на интернет-страница од точка 54 од оваа одлука вклучуваат на меѓународно разбирлив јазик специфични обележја за секоја од следниве ставки:
- тип на давател на платежните услуги којшто може да има една или повеќе од следниве улоги: одржување на платежните сметки; иницирање плаќања; давање информации за платежните сметки; издавање платни инструменти засновани на картички;
 - регистарски број на давателот на платежните услуги од регистарот на платежните институции и име на надлежниот орган каде што е регистриран давателот на платежните услуги.
56. Обележјата од точка 55 од оваа одлука не влијаат врз интероперабилноста и валидноста на квалификуваните сертификати за електронските печати или за автентичноста на интернет-страницата.

Сигурност на каналот за комуникација

57. Давателите на платежните услуги коишто одржуваат платежни сметки, давателите на платежните услуги за издавање платни инструменти засновани на картички, давателите на услугите за давање информации за платежните сметки и давателите на услугите за иницирање плаќања при размената на податоци на далечина помеѓу сите страни вклучени во каналот за комуникација применуваат сигурно шифрирање, користејќи широко прифатени индустриски стандарди, за заштита на доверливоста и интегритетот на податоците.
58. Давателите на услугите за издавање платни инструменти засновани на картички, давателите на услугите за давање информации за платежните сметки и давателите на услугите за иницирање плаќања се должни да го одржуваат времетраењето на каналот за комуникација којшто е овозможен од давателите на платежните услуги коишто ги одржуваат платежните сметки, што е можно пократко и активно да го прекинат таквиот канал веднаш по завршувањето на бараната активност.

59. Во случај на паралелни канали за комуникација со давателот на платежните услуги којшто ги одржува платежните сметки, давателите на услугите за иницирање плаќања и давателите на услугите за давање информации за платежните сметки, овозможуваат нивно сигурно поврзување со релевантните воспоставени канали за комуникација на корисниците на платежните услуги, за да се спречи можноста пораките или информациите коишто се разменуваат помеѓу нив да бидат погрешно пренасочени.

60. Во комуникацијата со давателот на платежните услуги којшто ја одржува платежната сметка, давателите на услугите за давање информации за платежните сметки, давателите на услугите за иницирање плаќања и давателите на платежните услуги што издаваат платни инструменти засновани на картички ги обезбедуваат следниве елементи:

- корисниците на платежните услуги и соодветниот канал за комуникација, за да се направи разлика помеѓу различните барања од исти корисници на платежните услуги;
- уникатно идентификување на иницирана платежна трансакција, при користење на услугите на иницирање на плаќањата;
- уникатно идентификување на барање за потврда на расположливоста на износот на парични средства, заради извршување на трансакцијата за плаќање со картичка.

61. Давателите на услугите коишто ги одржуваат платежните сметки, давателите на услугите за давање информации за платежните сметки, давателите на услугите за иницирање плаќања и давателите на платежните услуги што издаваат платежни инструменти засновани на картички, при пренесувањето на корисничките сигурносни обележја и кодовите за автентикација, обезбедуваат тие да не се директно или индиректно читливи од ниту еден нивен вработен, во ниту еден момент.

Во случај на утврдено нарушување на доверливоста на корисничките сигурносни обележја во надлежност на давателите на платежните услуги наведени во став 1 на оваа точка, тие без непотребно одлагање го информираат корисникот на платежните услуги и издавачот на корисничките сигурносни обележја.

Размена на податоци

62. Давателите на платежните услуги коишто ги одржуваат платежните сметки ги исполнуваат следниве барања:

- на давателите на услугите за давање информации за платежни сметки им ги даваат истите информации за назначените платежни сметки и платежните трансакции коишто се поврзани со нив, а коишто на корисникот на платежните услуги му се достапни онлајн и не се содржани чувствителни податоци за плаќања;
- веднаш по приемот на налогот за плаќање, на давателите на услугите за иницирање плаќања им ги даваат истите информации за иницирањето и извршувањето на платежната трансакција коишто му се дадени или му се ставени на располагање на корисникот на платежните услуги, исто како и во

случај кога трансакцијата би била иницирана директно од корисникот на платежните услуги;

- на барање на давателите на платежните услуги, веднаш и со едноставна потврда со „да“ или „не“, им потврдуваат дали износот потребен за извршување на платежната трансакција е расположлив на платежната сметка.

63. Во случај на непредвиден настан или грешка при процесот на идентификација, автентикација или размена на податоците, давателот на платежните услуги којшто ги одржува платежните сметки им праќа известување на давателите на услугите за иницирање на плаќања, давателите на услугите за давање информации за платежните сметки и на давателите на платежните услуги што издаваат платежни инструменти засновани на картички, во кое се објаснува причината за непредвидениот настан или грешка.

Доколку давателот на платежните услуги којшто ги одржува платежните сметки обезбедува наменски интерфејс во согласност со точките 42, 43, 44, 45 и 46 од оваа одлука, интерфејсот создава пораки за настаните од став 1 од оваа точка коишто давателот на платежните услуги ги открил и е должен да ги достави до останатите даватели на платежните услуги коишто учествуваат во каналот за комуникација.

64. Давателот на услугите за давање информации за платежните сметки е должен да воспостави соодветни и ефикасни механизми со кои се спречува пристапот до информациите, освен до оние коишто се однесуваат на назначената платежна сметка и платежните трансакции поврзани со нив за кои корисникот на платежната услуга дал согласност.

65. Давателите на услугите за иницирање плаќања се должни да им ги обезбедат на давателите на платежните услуги за одржување на платежните сметки истите информации коишто му се побарани на корисникот на платежните услуги при директно иницирање на платежната трансакција.

66. Давателите на услугите за давање информации за платежните сметки можат да пристапат до информациите од назначените платежни сметки и платежните трансакции поврзани со нив, коишто се одржуваат од давателите на платежните услуги коишто ги одржуваат платежните сметки, во кој било од наведените случаи:

- кога корисникот на платежната услуга активно ги бара тие информации;
- кога корисникот на платежната услуга не ги бара активно тие информации, не повеќе од четири пати во текот на 24 часа, освен ако не е договорена поголема фреквенција помеѓу давателот на услугите за давање информации за платежните сметки и давателот на платежните услуги којшто ги одржува платежните сметки, со согласност на корисникот на платежните услуги.

VII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

67. Давателите на платежните услуги коишто се основани до денот на примената на оваа одлука се должни да го усогласат своето работење со барањата на оваа одлука најдоцна до 19 февруари 2024 година.

По исклучок на ставот 1 на оваа точка, давателите на платежните услуги коишто се основани до денот на примената на оваа одлука и коишто ги одржуваат платежните сметки се должни:

- да обезбедат техничка платформа и поддршка, заради тестирање на поврзувањето и функционалностите на интерфејс, во согласност со точка 40 од оваа одлука и потврда на усогласеност со законските барања во однос на дизајнот на наменскиот интерфејс и збирни резултати од тестирањето, во согласност со насоките од Анексот бр. 6, во прилог на оваа одлука, најмалку пет месеци пред датумот на усогласување на своето работење со барањата на оваа одлука, но не подоцна од 30 септември 2023 година;
- да достават извештај дека наменскиот интерфејс не создава попречување при обезбедувањето на услугите за иницирање плаќања и услуги за давање информации за платежните сметки, најмалку два месеца пред датумот на усогласување на своето работење со барањата на оваа одлука, но не подоцна од 31 декември 2023 година;
- да достават збиен извештај од резултатите од спроведеното стрес-тестирање на отпорноста, како и информација за начините со кои се надминати утврдените слабости, најмалку еден месец пред датумот на усогласување на своето работење со барањата на оваа одлука, но не подоцна од 31 јануари 2024 година.

68. Оваа одлука влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

**О бр.02-15/XXII-7/2022
28 декември 2022 година
Скопје**

**Гувернер и
претседавач
на Советот на Народна банка на
Република Северна Македонија
д-р Анита Ангеловска-Бежоска**

Прилози:

Анекс бр.1	-	„Референтни стапки на измама“
Анекс бр.2	-	„Следење на расположливоста и ефикасноста на наменскиот интерфејс“
Анекс бр.3	-	„Објавување статистички податоци“
Анекс бр.4	-	„Стрес-тестирање на отпорноста“
Анекс бр.5	-	„Извештај дека наменскиот интерфејс не создава попречување“
Анекс бр.6	-	„Дизајнирање и тестирање на наменскиот интерфејс“
Анекс бр.7	-	„Широка употреба на наменскиот интерфејс“
Анекс бр.8	-	„Информација за надминување на проблемите“

Анекс бр.1
„Референтни стапки на измама“

Референтни стапки на измама во %		
Вредност на прагот за исклучок (во денари)	Електронски платежни трансакции со платен инструмент заснован на картичка	Електронски кредитни трансфери
до 30.000	0.01	0.005
до 15.000	0.06	0.01
до 6000	0.13	0.015

Анекс бр. 2

„Следење на расположливоста и ефикасноста на наменскиот интерфејс“

1. Давателите на платежните услуги коишто ги одржуваат платежните сметки се должни за потребите на следењето на расположливоста и ефикасноста на наменскиот интерфејс да ги дефинираат најмалку следниве клучни показатели:
 - Време на непречено функционирање на наменскиот интерфејс на дневна основа (англ. uptime per day);
 - Време на достапност на наменскиот интерфејс на дневна основа (англ. downtime per day);
 - Просечно дневно време за иницирање плаќање;
 - Просечно дневно време за давање информации за платежни сметки;
 - Просечно дневно време потребно за побараната потврда во формат „да“ или „не“ од давателот на платежните услуги за издавање платни инструменти засновани на картичка;
 - Дневна стапка на доставени погрешни одговори (англ. daily error response rate).
2. За пресметка на показателите за расположливоста и ефикасноста на наменскиот интерфејс од точка 1 од овој анекс, давателите на платежните услуги коишто ги одржуваат платежните сметки се должни:
 - Времето на непречено функционирање да го пресметаат како разлика помеѓу 100% и времето на достапност;
 - Времето на достапност да го пресметаат, во проценти, како вкупен број секунди на достапност на наменскиот интерфејс дефинирана со точка 3 од овој анекс во период од 24 часа (изразен во секунди) каде што полноќ е почетокот и крајот на периодот;
 - Просечното дневно време за иницирање плаќање (изразено во милисекунди) се пресметува како вкупно време на доставување на информациите во согласност со точка 62, став 1 алинеја 2 од оваа одлука, поделено со бројот на такви барања во периодот од 24 часа, каде што полноќ е почеток и крај на периодот;
 - Просечно дневно време за давање информации за платежни сметки (изразено во милисекунди) се пресметува како вкупно време на достава на информациите согласно точка 62, став 1 алинеја 1 од оваа одлука, поделено со бројот на такви барања во период од 24 часа, каде што полноќ е почетокот и крајот на периодот;
 - Просечно дневно време потребно за побараната потврда во формат „да“ или „не“ од давателот на платежните услуги за издавање платни инструменти засновани на картичка (изразено во милисекунди) се пресметува како вкупно време на доставување на информациите во согласност со точка 62, став 1 алинеја 3 од оваа одлука, поделено со бројот на такви барања во период од 24 часа, каде што полноќ е почетокот и крајот на периодот;
 - Дневната стапка на доставени погрешни одговори да ја пресметаат како број на погрешни одговори во текот на денот доставени од давателот на платежните услуги којшто ги одржува платежните сметки до давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка поделен со вкупниот број доставени барања во текот на денот од претходно наведените даватели.

3. Наменскиот интерфејс се третира како недостапен кога на пет последователни услуги за иницирање плаќања, услуга за давање информација за платежна сметка или потврдување расположливост на износ на парични средства, интерфејсот нема да одговори во рок од 30 секунди, независно дали барањата се упатени од еден или повеќе даватели на услугата за иницирање плаќања, даватели на услугата за давање информации за платежните сметки и даватели на платежните услуги за издавање платни инструменти засновани на картичка.

Давателот на платежната услуга којшто ги одржува платежните сметки го пресметува времето на достапност од моментот на првото барање во низата на пет последователни барања на кое не одговорил во рок од 30 секунди, доколку во периодот на петте барања немало ниту едно барање на кое е доставен одговор успешно.

Анекс бр. 3

„Објава на статистички податоци“

1. Давателот на платежните услуги којшто ги одржува платежните сметки е должен на својата јавна интернет-страница да го стави на располагање планот за квартална објава на дневните статистички податоци за расположливоста и ефикасноста на наменскиот интерфејс и за интерфејсите коишто се користат од корисниците на платежните услуги за пристап до нивните платежни сметки, директно, онлајн.
2. При објавувањето на планот, давателот на платежната услуга којшто ги одржува платежните сметки ја наведува и интернет-страницата за објавување на статистичките податоци, како и датумот на нивното прво објавување.
3. Врз основа на објавата на статистичките податоци, давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка на дневна основа ги користат за споредба на расположливоста и ефикасноста на наменскиот интерфејс со расположливоста и ефикасноста на интерфејсите коишто давателот на платежните услуги којшто ги одржува платежните сметки им ги става на располагање на своите корисници на платежните услуги за пристап до нивните платежни сметки директно, онлајн.

Анекс бр.4

„Стрес-тестирање на отпорноста“

1. Давателот на платежните услуги којшто ги одржува платежните сметки е должен да спроведе, на секои три години, соодветно стрес-тестирање на отпорноста на наменскиот интерфејс, и тоа за:
 - неговата способност да им овозможи пристап на повеќе даватели на услугите за иницирање плаќања, даватели на услугите за давање информации за платежните сметки и даватели на платежните услуги за издавање платни инструменти засновани на картичка,
 - неговата способност успешно да обработи, во краток временски период, исклучително голем број барања добиени од давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка;
 - неговото користење од исклучително голем број канали за комуникација за иницирање плаќања, давање информации за платежните сметки и потврда на расположливоста на износот на паричните средства, воспоставени во исто време; и
 - неговата можност соодветно да им одговори на барањата за големо количество податоци.

Анекс бр. 5

„Извештај дека наменскиот интерфејс не создава попречување“

1. Давателот на платежните услуги којшто ги одржува платежните сметки подготвува извештај дека наменскиот интерфејс не создава попречување, којшто содржи:
 - збирна информација за методите коишто ги поддржува наменскиот интерфејс и коишто се спроведуваат во постапките за автентикација на корисникот на платежните услуги, односно методите за пренасочување (англ. redirection), одвојување (англ. decoupled), вградување (англ. embedded) или нивна комбинација.
 - образложение за причините поради кои методите коишто се спроведуваат во постапка за автентикација на корисникот на платежните услуги не се третираат за попречување и начините на кои давателите на услугите коишто иницираат плаќања и давателите на услугите за давање информации за платежните сметки врз база на тие методи можат да се потпрат на постапките на автентикација коишто на своите корисници на платежните услуги им ги овозможува давателот на платежните услуги којшто ги одржува платежните сметки;
 - потврда дека наменскиот интерфејс не е причина за непотребно одложување или попречување во текот на корисничките активности при пристап до неговата платежна сметка со посредство на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки или давателите на платежните услуги за издавање платни инструменти засновани на картичка или појава на некои други причинители, вклучувајќи непотребни дополнителни чекори или употреба на нејасен или комплексен јазик, поради кој корисниците на платежните услуги се откажуваат од употребата на услугите на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки или давателите на платежните услуги за издавање платни инструменти засновани на картичка.
2. Во рамките на образложението од точка 1 став 1 алинеја 2 од овој анекс, давателот на платежната услуга којшто ги одржува платежните сметки доставува потврда за следново:
 - дека наменскиот интерфејс не е пречка давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки да се потпрат и да ги користат постапките на автентикација коишто давателот на платежната услуга којшто ја одржува платежната сметка им ги обезбедува на своите корисници на платежните услуги;
 - дека нема дополнителни барања или регистрации од страна на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки или давателите на платежните услуги за издавање платни инструменти засновани на картичка;
 - дека давателот на платежните услуги којшто ја одржува платежната сметка не спроведува дополнителна проверка на согласноста којашто корисникот на платежните услуги им ја дал на давателите на услугите за иницирање

плаќања или на давателите на услугите за давање информации за платежните сметки за пристап до информациите за платежната сметка којашто давателот на платежната услуга ја одржува, или поради иницирање плаќања и

- дека не се спроведува проверка на согласноста којашто корисникот на платежните услуги им ја дал на давателите на платежните услуги за издавање платни инструменти засновани на картичка, за потврда на расположливоста на износот на парични средства.

Анекс бр.6

„Дизајнирање и тестирање на наменскиот интерфејс“

1. Давателите на платежните услуги коишто ја одржуваат платежната сметка се должни за потврда на усогласеноста со законските барања во однос на дизајнот на наменскиот интерфејс, да достават на барање на Народна банка:
 - потврда дека наменскиот интерфејс ги исполнува регулаторните барања за пристапот до платежната сметка и размената на податоци, којшто вклучува: техничка документација, опис на неговата функционалност и образложение за тоа како нивната примена ги исполнува регулаторните барањата и
 - информација за тоа дали и на кој начин е воспоставена соработката на давателот на платежната услуга којшто ја одржува платежната сметка со давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка.
2. Давателот на платежната услуга којшто ја одржува платежната сметка е должен при тестирањето на наменскиот интерфејс да им ја стави на располагање техничката документација за наменскиот интерфејс на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции или на давателот на платежните услуги којшто поднесол барање за добивање дозвола за давање платежни услуги.
3. Давателите на платежните услуги коишто ја одржуваат платежната сметка, на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции или на давателот на платежните услуги којшто поднесол барање за добивање дозвола за давање платежни услуги е должен да им овозможи платформа за тестирање, т.е. наменскиот интерфејс да се тестира во сигурна, одделна околина во која не се користат реални податоци за корисниците на платежните услуги и со која ќе се потврди најмалку следново:
 - воспоставени се стабилни и сигурни канали за комуникација;
 - се обезбедува размена на соодветни квалификувани сертификати помеѓу давателите на платежните услуги коишто ја одржуваат платежната сметка и давателите на услугите коишто иницираат плаќања, даватели на услугите за давање информации за платежните сметки и даватели на платежните услуги коишто издаваат платни инструменти засновани на картичка коишто се впишани во регистарот на платежните институции;
 - се обезбедува испраќање и примање на пораки за грешки;
 - давателите на услугите коишто иницираат плаќања може да испраќаат налози за иницирање плаќања и притоа давателите на платежните услуги коишто ја одржуваат платежната сметка по нивниот прием можат соодветно да одговорат;

- давателите на услугите за давање информации за платежните сметки може да испраќаат барања за пристап до податоците на корисниците на платежните услуги и притоа давателите на платежните услуги коишто ја одржуваат платежната сметка по нивниот прием, соодветно можат да ги достават бараните информации;
 - давателите на платежните услуги за издавање платни инструменти засновани на картичка и давателите на услугите за иницирање плаќања може да испраќаат барања до давателите на платежните услуги коишто ја одржуваат платежната сметка на кое тие одговараат со едноставна потврда со „да“ или „не“, т.е. дали износот потребен за извршување на платежната трансакција е расположлив на платежната сметка;
 - давателите на услугите коишто иницираат плаќања и даватели тена услугите за давање информации за платежните сметки може да се потпрат на сите постапки на автентикација коишто давателите на платежните услуги коишто ја одржуваат платежната сметка им ги обезбедуваат на корисниците на платежните услуги.
4. Давателите на платежните услуги коишто ја одржуваат платежната сметка се должни, на барање на Народната банка, да достават збирни резултати од тестирањето за секое барање од точка 3 од овој анекс, вклучително и бројот на давателите на услугите коишто иницираат плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги коишто издаваат платни инструменти засновани на картичка коишто ја користеле платформата за тестирање, повратните информации коишто давателите на платежните услуги коишто ја одржуваат платежната сметка ја добиле од нив, податоците за утврдените проблеми и начините за нивно надминување.

Анекс бр.7

„Широка употреба на наменскиот интерфејс“

1. Давателите на платежните услуги коишто ја одржуваат платежната сметка се должни за потврда на широката употреба на наменскиот интерфејс, на барање на Народната банка, да достават:
 - опис на употребата на наменскиот интерфејс во периодот од најмалку три месеци, вклучително и: бројот на давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и давателите на платежните услуги за издавање платни инструменти засновани на картичка коишто го користеле наменскиот интерфејс и бројот на барањата доставени од нивна страна преку наменскиот интерфејс на давателот на платежните услуги којшто ги одржува платежните сметки, како и бројот на оние на кои тој одговорил;
 - потврда дека давателот на платежната услуга којшто ги одржува платежните сметки ги презел сите потребни мерки за широка употреба на наменскиот интерфејс, вклучително и објавувањето извештаи за неговата расположливост и ефикасност преку објавување статистички податоци на интернет-страниците и социјалните мрежи.

Анекс бр. 8

„Информација за надминување на проблемите“

1. Давателите на платежните услуги коишто ја одржуваат платежната сметка се должни, за потврда за преземените мерки за надминување на проблемите коишто се појавиле во функционирањето на наменскиот интерфејс, на барање на Народната банка, да достават:
 - информација за воведените системи или постапки за следење, решавање и надминување на пријавените проблеми, особено од давателите на услугите за иницирање плаќања, давателите на услугите за давање информации за платежните сметки и даватели на платежните услуги за издавање платни инструменти засновани на картичка; и
 - образложение за проблемите пријавени од наведените даватели во став 1 алинеја 1 од оваа точка од анексот, коишто не се надминати во согласност со дефинираните нивоа на услуга.