На основу члана 75г Закона о платним услугама („Службени гласник РС“, бр. 139/2014, 44/2018 и 64/2024) и члана 15. став 1. и члана 63. став 3. Закона о Народној банци Србије („Службени гласник РС“, бр. 72/2003, 55/2004, 85/200 – др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018), Извршни одбор Народне банке Србије доноси

О Д Л У К У
О ТЕХНИЧКИМ СТАНДАРДИМА ЗА ПОУЗДАНУ АУТЕНТИФИКАЦИЈУ КОРИСНИКА И ЗАЈЕДНИЧКИМ И БЕЗБЕДНИМ ОТВОРЕНИМ СТАНДАРДИМА КОМУНИКАЦИЈЕ

I. ОСНОВНЕ ОДРЕДБЕ

1. Овом одлуком утврђују се захтеви које су пружаоци платних услуга дужни да испуњавају за успостављање и спровођење мера сигурности при пружању платних услуга, а којима се обезбеђује да ти пружаоци:

1) примењују поуздану аутентификацију корисника платних услуга (у даљем тексту: корисник);
2) примењују изузећа од поуздане аутентификације корисника;
3) заштите поверљивост и интегритет персонализованих сигурносних елемената корисника;
4) успоставе заједничке и безбедне отворене стандарде комуникације између пружалаца платних услуга који воде платне рачуне, пружалаца услуга иницирања плаћања, пружалаца услуга пружања информација о рачуну, платиоца, примаоца плаћања и других пружалаца платних услуга.

2. Поједини појмови у смислу ове одлуке имају следеће значење:

1) ***поуздана аутентификација корисника*** означава аутентификацију употребом два или више елемената, односно комбинације тих елемената, који морају бити међусобно независни – што значи да откривање једног елемента не умањује поузданост других елемената – која је осмишљена тако да штити поверљивост података о аутентификацији, а елементи који се употребљавају при овој аутентификацији морају спадати у најмање две од следећих категорија:
– категорија знања (нешто што корисник зна) – подразумева употребу елемента који само корисник зна (нпр. лозинке, личног идентификационог броја (енг. PIN), одговора на специфично питање, шаблона брзог превлачења екрана и сл.),
– категорија поседовања (нешто што корисник поседује) –

подразумева употребу елемента који само корисник поседује (нпр. уређаја или броја телефона који је евидентиран и доказан слањем једнократних лозинки (енг. OTP – *One Time Password*), уређаја који је доказан путем дигиталног потписа или стандардизоване дводимензионалне ознаке – QR кôда (енг. *QR – Quick Response*), криптографског кључа, апликације која је доказано повезана са уређајем и сл.),

– категорија својствености (нешто што корисник јесте) – подразумева употребу елемента који је својствен само кориснику (нпр. биометријске карактеристике, као што је отисак прста, очна дужица, глас и сл. или одређене радње или понашања које се због начина њиховог извођења препознају као искључиво корисникове, као што је потпис, рукопис, начин притиска тастера, начин куцања и сл.);

2) ***електронска платна трансакција*** означава платну трансакцију иницирану и извршену на начин који укључује коришћење електронске платформе или уређаја, а не обухвата платне трансакције инициране платним налогом на папиру;

3) ***интерфејс*** означава логичку компоненту информационо--комуникационог система преко које се, у складу са унапред дефинисаним скупом рутина и протокола, успоставља канал комуникације и врши размена информација с другим системима;

4) ***онлајн повезивање*** је повезивање између пружаоца и корисника одређене услуге путем јавно доступне комуникационе мреже (нпр. интернета);

5) ***платна картица*** означава платни инструмент у облику физичке или електронске картице који се користи за иницирање платне трансакције, који омогућава имаоцу тог инструмента плаћање робе и услуга преко прихватног уређаја или иницирањем платне трансакције на даљину и/или који омогућава исплату готовог новца, односно коришћење других услуга на банкомату или другом самоуслужном уређају;

6) ***платни инструмент заснован на платној картици*** и платна апликација имају значење утврђено законом којим се уређују међубанкарске накнаде и посебна правила пословања код платних трансакција на основу платних картица;

7) појмови ***аутентификација***, ***персонализовани сигурносни елементи (креденцијали)***, ***осетљиви подаци о плаћању***, ***платна трансакција на даљину*** и ***трансфер одобрења*** имају значење утврђено Законом о платним услугама (у даљем тексту: Закон);

8) **електронска комуникациона мрежа** има значење утврђено законом којим се уређују електронске комуникације.

II. ПОУЗДАНА АУТЕНТИФИКАЦИЈА КОРИСНИКА

1. Општи захтеви за аутентификацију

Механизми за праћење трансакција

3. Пружаоци платних услуга дужни су да успоставе ефикасне механизме за праћење трансакција који ће им омогућити да идентификују неодобрено или преварно иницирање платне трансакције, односно злоупотребе код тих трансакција, у циљу примене мера сигурности из тачке 1. одредбе под 1) и 2) ове одлуке.

Механизми из става 1. ове тачке заснивају се на анализи платних трансакција која узима у обзир елементе који су типични за одређеног корисника у оквиру његове уобичајене употребе персонализованих сигурносних елемената.

Пружаоци платних услуга дужни су да обезбеде да механизми за праћење трансакција укључују најмање следеће факторе ризика:

1) списак компромитованих или украдених елемената за аутентификацију;
2) износ сваке платне трансакције;
3) познате случајеве превара које се дешавају при коришћењу, односно пружању платних услуга;
4) знакове који указују на присуство злонамерног софтвера у било којој фази поступка аутентификације;
5) записе о употреби уређаја или софтвера за приступ који су достављени кориснику и неуобичајена употреба уређаја или софтвера за приступ, ако је те уређаје, односно софтвер том кориснику обезбедио пружалац платних услуга.

Преиспитивање мера сигурности

4. Спровођење мера сигурности из тачке 1. ове одлуке код пружаоца платних услуга документују, периодично тестирају, оцењују и проверавају ревизори са искуством у области безбедности информационо-комуникационих система и платних услуга који су независни у обављању ових послова унутар пружаоца платних услуга (интерни ревизори) или те послове обављају независно од пружаоца платних услуга (спољни ревизори).

Ревизија из става 1. ове тачке врши се најмање једном годишње, као и након значајних промена у информационо-комуникационом систему.

Изузетно од става 1. ове тачке, када пружалац платних услуга примењује изузетак од поуздане аутентификације из тачке 20. ове одлуке – проверу методологије, модела и извештавања о злоупотребама/преварама који се односе на ту примену мора спровести спољни ревизор током прве године примене тог изузетка, као и најмање на сваке три године током његове примене или чешће – ако то захтева Народна банка Србије.

Ревизија из става 1. ове тачке садржи оцену и извештај о усклађености мера сигурности пружаоца платних услуга са захтевима утврђеним овом одлуком. Пружалац платних услуга дужан је да тај извештај на захтев достави Народној банци Србије.

2. Мере сигурности за примену поуздане аутентификације корисника

Кôд за проверу аутентичности

5. Ако пружалац платних услуга примењује поуздану аутентификацију корисника, та аутентификација треба да буде заснована на два или више елемената који су утврђени у тачки 2. одредба под 1) ове одлуке и чија примена треба да резултира генерисањем кôда за проверу аутентичности.

Кôд за проверу аутентичности из става 1. ове тачке може бити прихваћен само једном од стране пружаоца платних услуга, када платилац користи тај кôд за приступ платном рачуну преко интернета, за иницирање електронске платне трансакције или да би извршио друге активности путем интернета, односно уређаја који се може користити за комуникацију на даљину, које са собом могу носити ризик од преварних радњи у вези с плаћањем или других видова злоупотреба.

За потребе примене ст. 1. и 2. ове тачке, пружалац платних услуга усваја мере сигурности које обезбеђују испуњеност следећих услова:

1) да се откривањем кôда за проверу аутентичности не може утврдити ниједна информација о било ком елементу из става 1. ове тачке;
2) да није могуће генерисање новог кôда за проверу аутентичности на основу сазнања о било ком другом претходно генерисаном кôду за проверу аутентичности;
3) да се кôд за проверу аутентичности не може фалсификовати.

Пружалац платних услуга обезбеђује да примена аутентификације путем кôда за проверу аутентичности укључује следеће мере:

1) ако се кôд за проверу аутентичности у смислу става 1. ове тачке неуспешно генерише при аутентификацији ради приступа платном рачуну на даљину, иницирања електронских платних трансакција на даљину или вршења других активности путем интернета, односно уређаја који се може користити за комуникацију на даљину а које могу имати утицај на испољавање ризика од преварних радњи или друге злоупотребе у вези са извршењем платне трансакције – да није могуће утврдити који од елемената из става 1. ове тачке није био исправан;

2) да број узастопних неуспешних покушаја аутентификације, након кога се радње из члана 75в став 1. Закона привремено или трајно блокирају – није већи од пет;

3) да обезбеди да време важења кôда за проверу аутентичности буде ограничено на период који је потребан за обављање аутентификације, а који није дужи од 180 секунди;

4) да су комуникационе сесије заштићене од крађе или неовлашћеног увида у податке који се преносе током аутентификације, као и од руковања од стране неовлашћених лица у складу са одредбама Главе III ове одлуке;

5) да најдужи период током ког платилац не предузима никакве радње након што се аутентификује за приступ платном рачуну – није дужи од пет минута.

У случају привремене блокаде из става 4. одредба под 2) ове тачке, трајање те блокаде и број поновних покушаја утврђују се на основу обележја услуге која се пружа кориснику и свих релевантних ризика, узимајући у обзир најмање факторе ризика из тачке 3. став 3. ове одлуке.

Пружалац платних услуга дужан је да пре него што блокада из става 4. одредба под 2) и става 5. ове тачке постане трајна, о томе обавести платиоца.

Пружалац платних услуга дужан је да успостави безбедну процедуру на основу које платилац може почети да поново користи електронски платни инструмент након његове трајне блокаде из става 6. ове тачке.

Динамичко повезивање

6. Када пружалац платних услуга примењује поуздану аутентификацију корисника у случају иницирања платне трансакције на даљину, поред захтева из тачке 5. ове одлуке, дужан је да примењује и мере сигурности којима се обезбеђује следеће:

1) да је платилац обавештен о износу платне трансакције и о

примаоцу плаћања;

2) да је кôд за аутентификацију посебно генерисан баш у односу на износ платне трансакције и примаоца плаћања које је платилац назначио при иницирању те трансакције;

3) да кôд за аутентификацију који је пружалац платних услуга прихватио одговара изворно наведеном износу платне трансакције и идентитету примаоца плаћања које је платилац назначио;

4) да свака промена износа или примаоца плаћања доводи до поништавања генерисаног кôда за аутентификацију.

Ради поступања у складу са ставом 1. ове тачке, пружалац платних услуга успоставља мере сигурности којима се обезбеђује поверљивост, аутентичност и интегритет:

1) података о износу платне трансакције и примаоцу плаћања током свих фаза поуздане аутентификације корисника;

2) информација које се приказују платиоцу током свих фаза поуздане аутентификације корисника, укључујући генерисање, пренос и употребу кôда за проверу те аутентичности.

Ради поступања у складу са ставом 1. ове тачке, морају бити испуњени следећи захтеви за кôд за аутентификацију:

1) у случају платне трансакције на основу платне картице за коју је платилац дао сагласност за тачан износ новчаних средстава која ће се резервисати у складу с чланом 49а став 1. Закона, кôд за аутентификацију посебно је генерисан баш у односу на износ за чије је резервисање платилац дао сагласност и који је при иницирању трансакције назначио;

2) у случају платних трансакција за које је платилац дао сагласност за извршење низа електронских платних трансакција на даљину, упућених према једном или више прималаца плаћања, кôд за аутентификацију посебно је генерисан баш у односу на укупан износ низа платних трансакција и за назначене примаоце плаћања.

Захтеви за елементе који припадају категорији знања

7. Пружалац платних услуга дужан је да успостави мере за ублажавање ризика да неовлашћена лица непосредно или преко других лица открију елементе за поуздану аутентификацију корисника који припадају категорији знања.

При употреби елемената из става 1. ове тачке од стране платиоца, пружалац платних услуга примењује мере за ублажавање ризика ради спречавања откривања тих елемената неовлашћеним лицима.

Захтеви за елементе који припадају категорији поседовања

8. Пружалац платних услуга дужан је да успостави мере за ублажавање ризика да неовлашћена лица употребе елементе за поуздану аутентификацију корисника који припадају категорији поседовања.

При употреби елемената из става 1. ове тачке од стране платиоца, пружалац платних услуга примењује мере за ублажавање ризика којима се спречава репликација тих елемената.

Захтеви за уређаје и софтвер који су повезани са елементима који припадају категорији својствености

9. Пружалац платних услуга дужан је да успостави мере за ублажавање ризика да неовлашћена лица открију елементе за поуздану аутентификацију корисника који припадају категорији својствености а које учитавају приступни уређаји и софтвер који су дати платиоцу.

Пружалац платних услуга дужан је да обезбеди најмање да при коришћењу приступних уређаја и софтвера из става 1. ове тачке постоји веома низак ниво вероватноће да се неовлашћено лице нађе у својству платиоца уместо самог платиоца, односно да такво лице буде аутентификовано као платилац.

При употреби елемената из става 1. ове тачке од стране платиоца, пружалац платних услуга примењује мере којима се гарантује отпорност приступних уређаја и софтвера на неовлашћену употребу тих елемената у случају приступа тим уређајима и софтверу.

Независност елемената за поуздану аутентификацију корисника

10. Пружалац платних услуга дужан је да обезбеди да се при употреби елемената за поуздану аутентификацију корисника из тач. 7. до 9. ове одлуке примењују и мере којима се обезбеђује да неовлашћено коришћење, односно компромитација једног од тих елемената, у погледу технологије, алгоритама и параметара, не умањује поузданост осталих елемената.

Пружалац платних услуга, у случају употребе било којег елемента за поуздану аутентификацију корисника или самог кôда за проверу аутентичности преко вишенаменског уређаја, дужан је да успостави мере сигурности ради ублажавања ризика који би могао настати услед злоупотребе вишенаменског уређаја.

Ради поступања у складу са ставом 2. ове тачке, пружалац платних услуга дужан је да успостави следеће мере за ублажавање ризика:

1) коришћење одвојених безбедних окружења за извршавање, помоћу софтвера инсталираног на вишенаменском уређају;
2) механизме којима се обезбеђује да платилац или трећа страна не могу да модификују софтвер или уређај;
3) механизме којима се у случају модификације софтвера или уређаја ублажавају последице те модификације.

3. Изузеци од примене захтева за поуздану аутентификацију корисника

Непосредан приступ информацијама о платном рачуну код пружаоца платних услуга који води рачун

11. Пружалац платних услуга који води рачун корисника није дужан да примени поуздану аутентификацију корисника при онлајн приступу корисника том платном рачуну ако у сваком случају поступа у складу са општим захтевима за аутентификацију из тачке 3. ове одлуке и под условом да тај приступ не доводи до откривања осетљивих података о плаћању и да је ограничен на увид у:

1) стање на једном или више утврђених платних рачуна; или
2) платне трансакције извршене у последњих 90 дана преко једног или више утврђених платних рачуна.

Пружалац платних услуга не може да користи изузетак од примене поуздане аутентификације из става 1. ове тачке ако је испуњен најмање један од следећих услова:

1) корисник први пут приступа информацијама из тог става;
2) прошло је више од 180 дана од када је корисник последњи пут приступио информацијама из тог става уз примену поуздане аутентификације тог корисника.

Посредан приступ информацијама о платном рачуну путем пружаоца услуга пружања информација о рачуну

12. Пружалац платних услуга не примењује поуздану аутентификацију корисника при приступу корисника његовом платном рачуну преко интернета путем пружаоца услуга пружања информација о рачуну – ако у сваком случају поступа у складу са општим захтевима за аутентификацију из тачке 3. ове одлуке и под условом да тај приступ не доводи до

откривања осетљивих података о плаћању и да је ограничен на увид у:

1) стање на једном или више утврђених платних рачуна; или
2) платну трансакцију извршену у последњих 90 дана преко једног или више утврђених платних рачуна.

Изузетно од става 1. ове тачке, пружалац платних услуга дужан је да примени поуздану аутентификацију из тог става ако је испуњен најмање један од следећих услова:

1) корисник први пут приступа информацијама из тог става;
2) прошло је више од 180 дана од када је корисник последњи пут приступио информацијама из тог става уз примену поуздане аутентификације тог корисника.

Изузетно од става 1. ове тачке, када за то има објективно оправдане и доказиве разлоге који се односе на неовлашћен или преварни приступ рачуну – пружалац платних услуга може да примењује поуздану аутентификацију корисника када корисник приступа свом рачуну преко интернета путем пружаоца услуга пружања информација о рачуну. У том случају, пружалац платних услуга дужан је да на захтев Народне банке Србије документује и оправда разлоге за примену поуздане аутентификације корисника.

Пружалац платних услуга који води рачун и који је успоставио наменски интерфејс из тачке 32. ове одлуке није дужан да примењује изузетак из става 1. ове тачке за непредвиђене околности из тачке 35. став 5. те одлуке када не примењује изузетак из тачке 11. ове одлуке путем директног интерфејса који се користи за аутентификацију и комуникацију с његовим корисницима.

Бесконтактна плаћања на продајном месту

13. Ако поступа у складу са општим захтевима из тачке 3. ове одлуке, пружалац платних услуга није дужан да примени поуздану аутентификацију корисника када платилац иницира бесконтактну електронску платну трансакцију, уз испуњеност најмање једног од следећих услова:

1) појединачни износ бесконтактне електронске платне трансакције не прелази 6.000 динара, а укупна вредност претходних бесконтактних електронских платних трансакција које су иницране платним инструментом који поседује бесконтактну функцију у периоду од датума последње примене поуздане аутентификације корисника не прелази 18.000 динара;

2) број узастопних бесконтактних електронских платних трансакција које су иницране платним инструментом који поседује бесконтактну функцију, у периоду од последње примене поуздане аутентификације тог корисника – није већи од пет.

Самоуслужни терминали за плаћање превоза и накнада за паркирање

14. Ако поступа у складу са општим захтевима из тачке 3. ове одлуке, пружалац платних услуга није дужан да примени поуздану аутентификацију корисника када платилац иницира електронску платну трансакцију на самоуслужном терминалу за плаћање услуга превоза или накнада за паркирање.

Поуздани примаоци плаћања

15. Пружалац платних услуга примењује поуздану аутентификацију корисника када платилац креира или мења листу поузданих прималаца плаћања преко пружаоца платних услуга који води рачун.

Ако поступа у складу са општим захтевима из тачке 3. ове одлуке, пружалац платних услуга није дужан да примени поуздану аутентификацију корисника када платилац иницира платну трансакцију, а прималац плаћања се налази на листи поузданих прималаца плаћања из става 1. ове тачке коју је претходно креирао платилац.

Понављајуће трансакције

16. Пружалац платних услуга примењује поуздану аутентификацију корисника када платилац креира, мења или први пут иницира платне трансакције које се са истим износом и истим примаоцем плаћања понављају у одређеним временским интервалима (низ поновљених платних трансакција).

Ако поступа у складу са општим захтевима из тачке 3. ове одлуке, пружалац платних услуга није дужан да примени поуздану аутентификацију корисника при иницирању свих накнадних платних трансакција које су саставни део низа поновљених платних трансакција из става 1. ове тачке.

Трансфери одобрења између платних рачуна чији је ималац исто физичко или правно лице

17. Ако поступа у складу са општим захтевима из тачке 3. ове одлуке, пружалац платних услуга није дужан да примени поуздану

аутентификацију корисника у случају иницирања трансфера одобрења када су платилац и прималац плаћања исто физичко или правно лице и када се оба платна рачуна воде код истог пружаоца платних услуга.

Трансакције мале вредности

18. Пружалац платних услуга није дужан да примени поуздану аутентификацију корисника када платилац иницира електронску платну трансакцију на даљину – ако су испуњени следећи услови:

1) да износ електронске платне трансакције на даљину не прелази 3.600 динара; и

2) да укупна вредност претходних електронских платних трансакција на даљину које је платилац иницирао од последње примене поуздане аутентификације корисника не прелази 12.000 динара; или

3) да број претходних узастопних електронских платних трансакција на даљину које је платилац иницирао од последње примене поуздане аутентификације корисника није већи од пет.

Сигурни корпоративни процеси и протоколи плаћања

19. Пружалац платних услуга није дужан да примени поуздану аутентификацију корисника у односу на правна лица и предузетнике који иницирају електронске платне трансакције, ако је омогућио да се те трансакције иницирају коришћењем наменских процеса или протокола плаћања који су стављени на располагање само платиоцима који нису потрошачи, и ако је најмање 30 дана пре дана почетка пружања платне услуге која укључује такво иницирање електронских платних трансакција – о томе обавестио Народну банку Србије и доставио јој доказе да ти процеси или протоколи плаћања обезбеђују нивое безбедности који су најмање једнаки захтевима који су у том погледу утврђени Законом и овом одлуком.

Анализа ризика трансакције

20. Пружалац платних услуга није дужан да примени поуздану аутентификацију корисника када платилац иницира електронску платну трансакцију на даљину за коју је пружалац платних услуга утврдио да представља низак ризик, у складу с механизмима за праћење платних трансакција из тачке 3. ове одлуке.

Електронска платна трансакција представља низак ризик у смислу става 1. ове тачке ако су испуњени следећи услови:

1) стопа преваре за ту врсту трансакције пријављена у

извештајима пружаоца платних услуга и израчуната у складу с тачком 21. ове одлуке – једнака је референтној стопи преваре датој у Прилогу 1, који је одштампан уз ову одлуку и њен је саставни део, или је нижа од те стопе;

2) износ трансакције не прелази релевантну вредност прага изузећа која је утврђена у Прилогу 1;

3) пружалац платних услуга спровођењем анализе ризика у реалном времену није утврдио ниједно од следећег:

– неуобичајени образац потрошње или понашања платиоца;

– неуобичајене информације о приступу уређају/софтверу од стране платиоца;

– примену малициозног програмског кôда у било којој сесији спровођења процедуре аутентификације корисника;

– познати сценарио преваре у вези с пружањем платних услуга;

– неуобичајену локацију платиоца;

– високоризичну локацију примаоца плаћања.

Пружалац платних услуга који намерава да електронске платне трансакције на даљину из става 1. ове тачке изузме од примене поуздане аутентификације корисника на основу процене да представљају низак ризик, дужан је да узме у обзир најмање следеће факторе ризика:

1) претходне обрасце потрошње конкретног корисника на чије би се платне трансакције тај изузетак примењивао;

2) историју платних трансакција свих корисника платних услуга тог пружаоца платних услуга;

3) локацију платиоца и примаоца плаћања у тренутку иницирања платне трансакције, ако приступни уређај или софтвер обезбеђује тај пружалац платних услуга;

4) идентификацију неуобичајених образаца плаћања конкретног корисника на чије би се платне трансакције овај изузетак примењивао, узимајући у обзир историју плаћања тог корисника.

Пружалац платних услуга утврђује оцену ризика за сваку појединачну трансакцију узимајући у обзир све факторе ризика из става 3. ове тачке, како би утврдио да ли конкретно плаћање треба да одобри без поуздане аутентификације корисника.

Израчунавање стопа преваре

21. Пружалац платних услуга дужан је да обезбеди да су укупне стопе преваре за електронске платне трансакције на даљину на основу платних картица и за електронске трансфере одобрења на даљину, којима су обухваћене платне трансакције које су извршене применом поуздане аутентификације корисника и трансакције извршене применом изузетака

из тач. 15. до 20. ове одлуке – једнаке референтној стопи преваре за ту врсту трансакције датој у Прилогу 1 или ниже од те стопе.

Укупна стопа преваре за сваку врсту трансакције из става 1. ове тачке израчунава се као укупна вредност неодобрених трансакција на даљину или трансакција на даљину повезаних с преварним радњама, без обзира на то да ли су средства враћена или не, подељена са укупном вредношћу свих платних трансакција на даљину за ту врсту трансакције, без обзира на то да ли су оне извршене применом поуздане аутентификације корисника или применом изузетака из тач. 15. до 20. ове одлуке, на тромесечној основи (90 дана).

Пружалац платних услуга документује методологију и моделе које користи за израчунавање стопа преваре из става 1. ове тачке, као и добијене стопе преваре, и на захтев их доставља Народној банци Србије.

Престанак примене изузећа на основу анализе ризика трансакције

22. Пружалац платних услуга који не примењује поуздану аутентификацију корисника у складу с тачком 20. ове одлуке дужан је да Народној банци Србије без одлагања пријави ако стопа преваре за одређену категорију платних трансакција из Прилога 1 буде виша од референтне стопе преваре утврђене за ту категорију платних трансакција у том прилогу, као и да истовремено достави опис мера које намерава да предузме како би обезбедио да стопа преваре за ову категорију платних трансакција не буде виша од те референтне стопе.

Пружалац платних услуга из става 1. ове тачке дужан је да без одлагања примењује поуздану аутентификацију корисника за све платне трансакције наведене у Прилогу 1 у одређеном распону вредности прага изузећа, када стопа преваре коју прати за два узастопна тромесечја пређе референтну стопу преваре која је применљива за тај платни инструмент или за ту врсту платне трансакције у том распону вредности прага изузећа.

У случају из става 2. ове тачке, пружалац платних услуга дужан је да поуздану аутентификацију корисника спроводи све док израчуната стопа преваре коју прати за једно тромесечје не буде једнака референтној стопи преваре за ту врсту платне трансакције у том распону вредности прага изузећа или нижа од ње.

Пружалац платних услуга који намерава поново да престане да примењује поуздану аутентификацију корисника у складу с тачком 20. ове одлуке – дужан је да најкасније 30 дана пре тог намераваног

престанка о томе обавести Народну банку Србије и да уз то обавештење достави доказе о поновној усклађености стопе преваре коју прати с референтном стопом преваре за тај распон вредности прага изузећа у складу са ставом 3. ове тачке.

Праћење платних трансакција

23. Пружалац платних услуга који не примењује поуздану аутентификацију корисника у складу с тач. 11. до 20. ове одлуке дужан је да, најмање на тромесечној основи, с детаљним прегледом платних трансакција на даљину и платних трансакција које се не извршавају на даљину – за сваку врсту платне трансакције евидентира и прати следеће податке:

1) укупну вредност неодобрених платних трансакција или платних трансакција повезаних с преварним радњама у складу са одредбама Закона којима се уређују услови и начин извршења платне трансакције, као и укупну вредност свих платних трансакција и добијене стопе преваре, укључујући детаљан преглед платних трансакција које су инициране применом поуздане аутентификације корисника и применом сваког појединачног изузећа у складу са одредбама ове одлуке;
2) просечну вредност трансакције, укључујући расподелу платних трансакција иницираних применом поуздане аутентификације корисника и применом сваког појединачног изузећа у складу са одредбама ове одлуке;
3) за свако појединачно изузеће које се примењује у складу са одредбама ове одлуке – број платних трансакција за које је примењено изузеће и њихов проценат у укупном броју платних трансакција.

Пружалац платних услуга податке о резултатима праћења из става 1. ове тачке на захтев доставља Народној банци Србије.

4. Поверљивост и интегритет персонализованих сигурносних података корисника

Општи захтеви за поверљивост и интегритет персонализованих сигурносних елемената

24. Пружалац платних услуга дужан је да обезбеди поверљивост и интегритет персонализованих сигурносних елемената корисника, укључујући кôдове за аутентификацију, током свих фаза те аутентификације.

Ради поступања у складу са ставом 1. ове тачке, пружалац платних услуга обезбеђује испуњеност следећих захтева:

1) персонализовани сигурносни елементи морају бити прикривени током приказа и не смеју бити у потпуности читљиви када их корисник уноси током аутентификације;

2) персонализовани сигурносни подаци у формату рачунарских података, као и криптографски материјали повезани са шифровањем персонализованих сигурносних података чувају се у шифрованом облику као текст који није читљив.

3) тајни криптографски материјал мора бити заштићен од неовлашћеног откривања.

Пружалац платних услуга дужан је да документује процес управљања криптографским материјалом који се користи да се персонализовани сигурносни подаци шифрују или на други начин учине нечитљивим.

Пружалац платних услуга обезбеђује да се обрада и преусмеравање персонализованих сигурносних података и кôдова за аутентификацију корисника који су генерисани у складу с тач. 5. до 10. ове одлуке – врше у безбедном окружењу у складу с прописима којима се уређује ову област и поузданим и општепризнатим стандардима који се примењују на ове радње при пружању платних услуга.

Креирање и пренос персонализованих сигурносних података

25. Пружалац платних услуга дужан је да обезбеди да се персонализовани сигурносни елементи стварају у безбедном окружењу.

Пружалац платних услуга дужан је да – пре уручивања, односно достављања платиоцу персонализованих сигурносних елемената и уређаја и софтвера за аутентификацију корисника – примени мере за ублажавање ризика од неовлашћене употребе тих елемената, уређаја и софтвера као последице њиховог губитка, крађе или копирања.

Повезивање с корисником

26. Пружалац платних услуга дужан је да обезбеди да је само корисник, и то на сигуран начин, повезан с персонализованим сигурносним елементима, уређајима и софтвером за аутентификацију тог корисника.

Ради поступања у складу са ставом 1. ове тачке, пружалац платних услуга дужан је да обезбеди следеће:

1) повезивање идентитета корисника с персонализованим

сигурносним елементима (креденцијалима), уређајима и софтвером који се користе за аутентификацију корисника врши се у безбедном окружењу за које је одговоран пружалац платних услуга, што обухвата најмање просторије пружаоца платних услуга, интернет окружење које обезбеђује пружалац платних услуга или безбедне интернет странице (веб-сајтови) које користи пружалац платних услуга и услуге банкомата које користи пружалац платних услуга, узимајући у обзир ризике у вези са уређајима и основним компонентама који се користе у процесу повезивања а за које пружалац платних услуга није одговоран;

2) повезивање идентитета корисника с персонализованим сигурносним елементима (креденцијалима), уређајима и софтвером који се користе за аутентификацију корисника које се врши на даљину – обавља се уз примену поуздане аутентификације корисника.

Достављање персонализованих сигурносних елемената, уређаја и софтвера за аутентификацију корисника

27. Пружалац платних услуга дужан је да обезбеди да се достављање персонализованих сигурносних елемената, уређаја и софтвера за аутентификацију корисника обавља на сигуран начин, којим се води рачуна о ризицима повезаним с неовлашћеном употребом у случају њиховог губитка, крађе или копирања.

Ради поступања у складу са ставом 1. ове тачке, пружалац платних услуга дужан је да примењује најмање следеће мере:

1) ефикасне и безбедне механизме доставе којима се обезбеђује достављање персонализованих сигурносних елемената, уређаја и софтвера за аутентификацију законитом кориснику;

2) механизме који пружаоцу платних услуга омогућавају да провери аутентичност софтвера за аутентификацију корисника који је достављен кориснику преко интернета;

3) аранжмане којима се, у случају достављања персонализованих сигурносних елемената изван пословних просторија пружаоца платних услуга или са удаљености, обезбеђује да:

– неовлашћено лице не може добити више од једног обележја персонализованих сигурносних елемената, уређаја или софтвера за аутентификацију корисника када се испоручују истим каналом,

– достављени персонализовани сигурносни елементи, уређаји и софтвер за аутентификацију корисника захтевају активацију пре употребе;

4) аранжмане којима се, у случају обавезне активације персонализованих сигурносних елемената, уређаја или софтвера за аутентификацију корисника, пре њихове прве употребе, обезбеђује да се активација одвија у безбедном окружењу, у складу с тачком 26. ове одлуке.

Обнављање и поновна активација персонализованих сигурносних елемената

28. Пружалац платних услуга дужан је да обезбеди да се обнављање или поновна активација персонализованих сигурносних података спроводи у складу са захтевима за креирање, повезивање и достављање персонализованих сигурносних података и уређаја за аутентификацију из тач. 25. до 27. ове одлуке.

Уништење, деактивација и опозив

29. Пружалац платних услуга дужан је да успостави ефикасне процесе којима обезбеђује примену следећих сигурносних мера:

1) сигурно уништење, деактивацију или опозив персонализованих сигурносних података, уређаја и софтвера за аутентификацију корисника;
2) када пружалац платних услуга ставља на располагање уређаје и софтвер за аутентификацију корисника који су намењени за вишекратну употребу – успоставља се, документује и спроводи сигурна поновна употреба уређаја или софтвера, пре њиховог стављања на располагање другом кориснику;
3) деактивацију или опозив информација повезаних са персонализованим сигурносним елементима сачуваним у системима и базама података пружаоца платних услуга и, када је применљиво, јавним регистрима.

III. ЗАЈЕДНИЧКИ И БЕЗБЕДНИ ОТВОРЕНИ СТАНДАРДИ КОМУНИКАЦИЈЕ

1. Општи захтеви за комуникацију

Захтеви за идентификацију

30. Пружалац платних услуга дужан је да обезбеди безбедну идентификацију током комуникације између уређаја који користи платилац и уређаја које користи прималац плаћања за примање електронских плаћања, укључујући терминале за плаћање, али не ограничавајући се на њих.

Пружалац платних услуга дужан је да примени такве мере којима ће обезбедити да су ефикасно ублажени ризици од погрешног усмеравања комуникације према неовлашћеним лицима у мобилним апликацијама и другим интерфејсима који корисницима нуде електронске платне услуге.

Могућност праћења

31. Пружалац платних услуга дужан је да успостави процесе којима се обезбеђује могућност праћења свих платних трансакција и других интеракција с корисником, другим пружаоцима платних услуга и другим субјектима, укључујући трговце, у вези с пружањем платне услуге и да обезбеди накнадне (лат. *ex post*) информације о свим догађајима релевантним за електронску платну трансакцију у свим различитим фазама.

Ради поступања у складу са ставом 1. ове тачке, пружалац платних услуга обезбеђује да се за сваку комуникациону сесију која је успостављена с корисником, другим пружаоцима платних услуга и другим субјектима, укључујући трговце, користе:

1) јединствени идентификатор комуникационе сесије;
2) сигурносни механизми за детаљно креирање евиденције о трансакцији, укључујући број трансакције, електронски временски жиг трансакције и све друге релевантне податке о трансакцији;
3) електронски временски жиг комуникационе сесије.

Електронски временски жиг из става 2. одредбе под 2) и 3) ове тачке мора бити заснован на јединственом временском систему и синхронизован са извором референтног времена у Републици Србији.

2. Посебни захтеви за заједничке и сигурне отворене стандарде комуникације

Општи захтеви у вези са приступним интерфејсима

32. Пружалац платних услуга који води рачуне и који платиоцу нуди платни рачун којем се може приступити онлајн – дужан је да обезбеди најмање један приступни интерфејс који испуњава следеће захтеве:

1) пружаоци услуге пружања информација о рачуну, пружаоци услуге иницирања плаћања и пружаоци платних услуга који издају платни инструмент на основу платне картице могу да се идентификују пред пружаоцем платних услуга који води рачуне;
2) пружаоци услуге пружања информација о рачуну могу сигурно да комуницирају када захтевају и примају информације о једном или више утврђених платних рачуна и с њима повезаним платним трансакцијама;
3) пружаоци услуге иницирања плаћања могу сигурно да комуницирају када иницирају платни налог с платног рачуна платиоца и када примају све информације о иницирању платне трансакције и све информације о извршењу платне трансакције које су доступне пружаоцу

платне услуге који води рачуне.

Ради аутентификације корисника, интерфејс из става 1. ове тачке мора да омогући пружаоцима услуге пружања информација о рачуну и пружаоцима услуге иницирања плаћања коришћење свих процедура за аутентификацију корисника које пружалац платних услуга који води рачун пружа кориснику.

Интерфејс из става 1. ове тачке мора да испуњава најмање следеће захтеве:

1) пружалац услуге иницирања плаћања или пружалац услуге пружања информација о рачуну може дати инструкцију пружаоцу платних услуга који води рачун да покрене аутентификацију корисника на основу сагласности корисника;

2) комуникационе сесије између пружаоца платних услуга који води рачун, пружаоца услуге пружања информација о рачуну, пружаоца услуге иницирања плаћања и било којег појединачног корисника успостављају се и одржавају током целокупног поступка аутентификације тог корисника;

3) обезбеђени су интегритет и поверљивост персонализованих сигурносних података и кôдова за проверу аутентичности које пружалац услуге иницирања плаћања или пружалац услуге пружања информација о рачуну преноси или се преко њега преносе.

Сва комуникација између пружалаца услуге пружања информација о рачуну и пружалаца услуге иницирања плаћања и пружалаца платних услуга који води рачун одвија се путем наменских интерфејса развијених од стране Народне банке Србије.

Пружалац платних услуга који води рачуне обезбеђује тестно окружење, укључујући и подршку, за тестирање повезивања и функционисања које овлашћеним пружаоцима услуге иницирања плаћања, пружаоцима услуге пружања информација о рачуну и пружаоцима платних услуга који издају платни инструмент на основу платне картице или лицима која су Народној банци Србије поднела захтев за давање дозволе за пружање било које од тих платних услуга омогућава тестирање њихових софтвера и апликација који се користе за пружање платних услуга корисницима платних услуга.

Тестно окружење из става 5. ове тачке треба да омогући тестирање интерфејса на начин утврђен тачком 5. став 5. из Прилога 2, који је одштампан уз ову одлуку и њен је саставни део, и треба да буде доступно пре датума одређеног за стављање у употребу приступног интерфејса из става 1. ове тачке.

Тестно окружење из става 5. ове тачке не може да се користи за размену осетљивих информација, а нарочито осетљивих података о плаћању.

У случају да интерфејс из става 1. ове тачке није усклађен са захтевима утврђеним овом одлуком, пружалац платних услуга који води рачуне дужан је да обезбеди да пружање услуга иницирања плаћања и информација о рачуну у било којем тренутку није спречено нити поремећено до нивоа који би значио да пружаоци тих услуга нису усклађени са захтевима из тачке 35. ст. 6. и 7. ове одлуке.

Народна банка Србије у вези с наменским интерфејсом из става 4. ове тачке обезбеђује тестно окружење, сходном применом одредаба ст. 5 до 7. ове тачке.

Опције за успостављање приступног интерфејса

33. Пружалац платних услуга који води рачуне дужан је да успостави један или више интерфејса из тачке 32. ове одлуке, успостављањем наменског интерфејса, омогућавањем коришћења наменског интерфејса из тачке 32. став 4. ове одлуке или дозвољавањем пружаоцима платних услуга из тачке 32. став 1. ове одлуке коришћења интерфејса који се употребљавају за проверу аутентичности корисника и комуникацију с корисницима пружаоца платних услуга који води рачуне.

Обавезе у вези с наменским интерфејсом

34. Не доводећи у питање одредбе тач. 32. и 33. ове одлуке, пружалац платних услуга који води рачуне и који је успоставио везу са наменским интерфејсом – дужан је да у сваком тренутку обезбеди исти ниво доступности и перформанси, укључујући и подршку, као интерфејси који су корисницима стављени на располагање за директан онлајн приступ њиховим платним рачунима.

Пружалац платних услуга који води рачуне а који је успоставио везу са наменским интерфејсом утврђује транспарентне кључне индикаторе перформанси и циљне нивое услуга које пружа путем наменског интерфејса, који су најмање подједнако строги као они који су дефинисани за интерфејс који користе корисници његових платних услуга, и то како у погледу доступности тако и у погледу података који се размењују у складу с тачком 38. ове одлуке.

Пружалац платних услуга врши тестирање отпорности на стрес у вези са пружањем услуга путем наменског интерфејса из става 2. ове тачке.

Пружалац платних услуга који води рачуне а који је успоставио везу са наменским интерфејсом обезбеђује да се путем тог интерфејса не стварају препреке за пружање услуге иницирања плаћања и пружање услуге пружања информација о рачуну.

Препреке из става 4. ове тачке, нарочито обухватају онемогућавање пружаоцима платних услуга из тачке 32. став 1. ове одлуке да употребљавају сигурносне податке које су пружаоци платних услуга који воде рачуне издали својим корисницима, наметање преусмеравања на функцију за проверу аутентичности или друге функције пружаоца платних услуга који води рачуне, захтевање додатних одобрења и регистрација, осим оних утврђених Законом, или захтевање додатних провера сагласности које су корисници дали пружаоцима услуге иницирања плаћања и пружаоцима услуге пружања информација о рачуну.

Народна банка Србије успоставља наменске интерфејсе из тачке 32. став 4. ове одлуке у складу са захтевима утврђеним овом тачком и на начин да омогући пружаоцима платних услуга из тачке 32. став 1. ове одлуке да испуне обавезе утврђене овом одлуком.

Народна банка Србије прати доступност и перформансе наменског интерфејса из тачке 32. став 4. ове одлуке и на својој интернет страници објављује тромесечне статистичке податке о доступности и перформансама наменских интерфејса.

Пружалац платне услуге који води рачуне дужан је да прати доступност и перформансе и да на својој интернет страници објављује тромесечне статистичке податке о интерфејсима које користе корисници његових платних услуга.

Мере у случају непредвиђених околности у вези с наменским интерфејсом

35. Успостављање наменског интерфејса из тачке 32. став 4. ове одлуке укључује израду стратегије и планова у вези с мерама за непредвиђене околности у случају да интерфејс не функционише у складу с тачком 34. ове одлуке, као и у случају да дође до непланиране недоступности интерфејса или до квара система.

Претпоставља се да је дошло до непланиране недоступности наменског интерфејса или до квара система у смислу става 1. ове тачке, ако се на пет узастопних захтева за приступ информацијама ради пружања услуге иницирања плаћања или пружања услуге информација

о рачуну не одговори у року од 30 секунди.

Мере за непредвиђене околности из става 1. ове тачке укључују планове за информисање и комуникацију с пружаоцима платних услуга који користе наменски интерфејс о мерама за опоравак система и опис одмах доступних алтернативних решења које ти пружаоци платних услуга могу користити у међувремену.

Пружаоци платних услуга који воде рачуне, као и пружаоци платних услуга из тачке 32. став 1. ове одлуке дужни су да, без одлагања, Народној банци Србије пријаве проблеме у вези с наменским интерфејсом из ст. 1. и 2. ове тачке.

Пружалац платних услуга који води рачуне дужан је да успостави механизам за непредвиђене околности, којим се пружаоцима платних услуга из тачке 32. став 1. ове одлуке омогућава да користе интерфејсе који су стављени на располагање његовим корисницима платних услуга за аутентификацију корисника и комуникацију с њим, све док се не обезбеди ниво доступности и перформанси наменског интерфејса из тачке 33. ове одлуке.

Ради поступања у складу са ставом 5. ове тачке, пружалац платних услуга који води рачуне обезбеђује да се пружаоци платних услуга из тачке 32. став 1. ове одлуке могу идентификовати и да могу да користе процедуре за аутентификацију које пружалац платних услуга који води рачун пружа кориснику.

Пружаоци платних услуга из тачке 32. став 1. ове одлуке при коришћењу интерфејса из става 5. ове тачке дужни су да:

1) предузимају неопходне мере како би обезбедили да не приступају подацима, не чувају податке или не обрађују податке у друге сврхе осим за пружање услуге у складу са захтевом корисника;

2) обезбеде поступање у складу с правилима из члана 46б став 2. и 46в став 2. Закона;

3) евидентирају податке којима се приступа преко интерфејса којим управља пружалац платних услуга који води рачуне за потребе корисника његових платних услуга и без одлагања доставе податке из те евиденције Народној банци Србије на њен захтев;

4) на захтев Народне банке Србије без одлагања образложе употребу интерфејса који је корисницима стављен на располагање за директан онлајн приступ њиховим платним рачунима;

5) на одговарајући начин обавештавају пружаоца платних услуга који води рачуне о коришћењу интерфејса.

Народна банка Србије може да одреди да пружалац платних услуга који води рачуне а који користи наменски интерфејс није дужан да успостави механизам за непредвиђене околности из става 5. ове тачке, ако на основу информација и података које достави тај пружалац платних услуга у вези са интерфејсом који је стављен на располагање његовим корисницима платних услуга за аутентификацију корисника и комуникацију с њим испуњавају следеће услове:

1) приступни интерфејс које тај пружалац платних услуга ставља на располагање испуњава исте услове у погледу нивоа доступности и перформанси, укључујући и подршку, као и додатне захтеве утврђене у Прилогу 2 ове одлуке;

2) приступни интерфејс је осмишљен и тестиран у складу с тачком 32. ст. 5. до 7. ове одлуке на начин који је прихватљив пружаоцима платних услуга из тачке 32. став 5. ове одлуке;

3) пружаоци платних услуга користили су тај интерфејс најмање три месеца ради пружања услуге информација о рачуну, услуге иницирања плаћања и пружања потврде о расположивости средстава за плаћања на основу платних картица.

Ако пружалац платне услуге из става 8. ове тачке не испуњава услове из одредаба под 1) и 4) тог става – дужан је да успостави механизам за непредвиђене околности из става 5. те тачке, најкасније у року од два месеца од утврђивања неиспуњености тих услова.

Сертификати

36. Ради идентификације из тачке 32. став 1. одредба под 1) ове одлуке, пружаоци платних услуга дужни су да користе квалификовани сертификат за електронски печат или квалификовани сертификат за аутентикацију веб сајта, у смислу закона којим се уређују електронски документ, електронска идентификација и услуге од поверења у електронском пословању а који ће издавати Народна Банка Србије.

Сертификат из става 1. ове тачке мора да, на српском или енглеском језику, садржи и следеће податке:

1) улогу пружаоца платних услуга и то:
   – вођење рачуна,
   – иницирање плаћања,
   – пружање информација о рачуну, и/или
   – издавање платних инструмената на основу платних картица;
2) назив „Народна банка Србије“ као означење органа који је пружаоцу платних услуга издао дозволу за пружање платних услуга.

Подаци из става 2. ове тачке не могу утицати на међусобну компатибилност (интероперабилност) и признавање квалификованих сертификата за електронски печати или аутентикацију веб сајта.

Сигурност комуникационе сесије

37. Пружаоци платних услуга који воде рачуне, пружаоци услуге пружања информација о рачуну, пружаоци услуге иницирања плаћања и пружаоци платних услуга који издају платни инструмент на основу платне картице – дужни су да обезбеде да се при размени података преко интернета примењује сигурно шифровање између учесника у комуникацији током целе комуникационе сесије, употребом општепризнатих техника шифровања, ради заштите поверљивости и интегритета података.

Пружаоци услуге пружања информација о рачуну, пружаоци услуге иницирања плаћања и пружаоци платних услуга који издају платни инструмент на основу платне картице дужни су да, у највећој могућој мери, ограниче трајање приступних сесија које нуде пружаоци платних услуга који воде рачуне и активно прекидају сесију чим је захтевана радња завршена.

У случају одржавања паралелних мрежних сесија с пружаоцем платних услуга који води рачуне, пружаоци услуге пружања информација о рачуну и пружаоци услуге иницирања плаћања дужни су да обезбеде да су те сесије сигурно повезане са одговарајућим сесијама успостављеним с једним или више корисника, како би се спречила могућност погрешног усмеравања порука или информација које се размењују током комуникације.

Ради спречавања могућности погрешног усмеравања порука или информација које се размењују током комуникације, пружаоци услуге пружања информација о рачуну, пружаоци услуге иницирања плаћања и пружаоци платних услуга који издају платни инструмент на основу платне картице дужни су да с пружаоцем платних услуга који води рачуне обезбеде недвосмислену референцу за сваку од следећих ставки:

1) једног или више корисника и одговарајућу комуникациону сесију како би се разликовали различити захтеви истог, односно истих корисника;

2) за услуге иницирања плаћања – јединствено идентификовану иницирану платну трансакцију;

3) за потврду расположивости средстава – јединствено идентификовани захтев у вези са износом потребним за извршење платне трансакције на основу платне картице.

Пружаоци платних услуга који воде рачуне, пружаоци услуге пружања информација о рачуну, пружаоци услуге иницирања плаћања и пружаоци платних услуга који издају платни инструмент на основу платне картице обезбеђују да ни у једном тренутку при размени персонализованих сигурносних података и кôдова за аутентификацију ти подаци и кôдови нису, ни директно ни индиректно, читљиви запосленом или другом лицу ангажованом код тих пружалаца платних услуга.

У случају компромитовања поверљивости персонализованих сигурносних података, пружаоци платних услуга из става 5. ове тачке у оквиру чијег пружања платних услуга је дошло до тог нарушавања, дужни су да о томе без одлагања обавесте корисника и издаваоца тих персонализованих сигурносних података.

Размена података

38. Пружалац платних услуга који води рачуне дужан је да:

1) пружаоцима услуге пружања информација о рачуну пружа исте информације са утврђених платних рачуна и с њима повезаних платних трансакција које се стављају на располагање кориснику када директно захтева приступ информацијама о рачуну, под условом да те информације не укључују осетљиве податке о плаћању;

2) одмах након пријема платног налога, пружаоцима услуге иницирања плаћања пружа исте информације о иницирању и извршењу платне трансакције које се пружају или стављају на располагање кориснику када директно иницира платну трансакцију;

3) на захтев пружалаца платних услуга, без одлагања, у једноставном „да или не“ формату, потврђује да ли је износ потребан за извршење платне трансакције расположив на платном рачуну платиоца.

У случају неочекиваног догађаја или грешке настале током процеса идентификације, провере аутентичности корисника или размене елемената података – пружалац платних услуга који води рачуне шаље поруку пружаоцу услуге иницирања плаћања или пружаоцу услуге пружања информација о рачуну и пружаоцу платних услуга који издаје платни инструмент на основу платне картице са објашњењем разлога неочекиваног догађаја или грешке.

Када пружалац платних услуга који води рачуне обезбеђује наменски интерфејс у складу с тачком 34. ове одлуке, тај интерфејс мора да омогући прослеђивање порука о неочекиваним догађајима или грешкама које било који пружалац платних услуга који открије такав догађај или грешку треба да достави другим пружаоцима платних услуга који учествују у комуникационој сесији.

Пружалац услуге пружања информација о рачуну мора да располаже прикладним и ефикасним механизмима којима се спречава приступ информацијама, осим информацијама са утврђених рачуна за плаћање и с њима повезаних платних трансакција, уз изричиту сагласност тог корисника.

Пружалац услуге иницирања плаћања доставља пружаоцу платних услуга који води рачуне исте информације које се од корисника траже када директно иницира платну трансакцију.

Пружалац услуге пружања информација о рачуну може, за потребе пружања услуге информација о рачуну, приступити информацијама са утврђених платних рачуна и с њима повезаних платних трансакција које поседују пружаоци платних услуга који воде рачуне – у следећим ситуацијама:

1) када корисник активно захтева те информације;
2) када корисник не захтева активно те информације – не више од четири пута у току 24 часа, осим у случају да је, уз сагласност корисника, могућност веће учесталости захтевања тих информација договорена између пружаоца услуге пружања информација о рачуну и пружаоца платних услуга који води рачун.

IV. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

39. Пружаоци платних услуга дужни су да своје унутрашње акте ускладе са одредбама ове одлуке најкасније месец дана пре почетка њене примене и да у том року Народној банци Србије доставе обавештење о томе, заједно са усклађеним унутрашњим актима.

40. Ова одлука не примењује се на банку која се припаја другој банци, ако је банка којој се банка припаја поднела Народној банци Србије уредан захтев за давање сагласности на то припајање најкасније до дана почетка примене ове одлуке а планирани датум регистрације статусне промене припајања је најкасније 31. децембар 2026. године.

На банку која је најкасније до дана почетка примене ове одлуке доставила Народној банци Србије обавештење и одлуку надлежног органа банке да планира миграцију података на нови систем главних пословних апликација у смислу одлуке којом се уређују минимални стандарди управљања информационим системом финансијске институције – одредбе ове одлуке примењиваће се од 30. јуна 2026. године.

41. Ова одлука ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“, а примењује се од 1. јануара 2026. године.

ИО НБС бр. 84
20. децембра 2024. године
Б е о г р а д

Председавајућа
Извршног одбора Народне банке Србије
Г у в е р н е р
Народне банке Србије

Др Јоргованка Табаковић, с.р.