BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVA
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Në bazë të nenit 35, paragrafi 1 nënparagrafi 1.1, nenit 65 të Ligjit Nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës (Gazeta Zyrtare e Republikës së Kosovës, Nr.77 / 16 gusht 2010), të ndryshuar dhe plotësuar me Ligjin Nr. 05/L -150 (Gazeta Zyrtare e Republikës së Kosovës / Nr. 10 / 03 prill 2017, Prishtinë), dhe në bazë të nenit 98 dhe 135 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave, Bordi i Bankës Qendrore të Republikës së Kosovës, në mbledhjen e mbajtur më 17 dhjetor 2024 miratoi këtë:

RREGULLORE PËR STANDARDET TEKNIKE PËR AUTENTIFIKIM TË THELLUAR TË KLIENTIT DHE STANDARDET E HAPURA, TË PËRBASHKËTA DHE TË SIGURTA TË KOMUNIKIMIT

KAPITULLI I
DISPOZITAT E PËRGJITHSHME

Neni 1
Qëllimi dhe fushëveprimi

1. Qëllimi i kësaj Rregulloreje është përcaktimi i kërkesave që duhet t'i respektojnë ofruesit e shërbimeve të pagesave me qëllim të zbatimit të masave të sigurisë që u mundësojnë atyre:
   1.1. zbatimin e procedurës së autentifikimit të thelluar të klientit në përputhje me nenin 97 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave;
   1.2. përjashtimin nga zbatimi i kërkesave të sigurisë për autentifikimin e thelluar të klientit nëse përmbushen kushtet e specifikuara dhe të kufizuara bazuar në nivelin e rrezikut, shumën dhe përsëritjen e transaksionit të pagesës dhe të kanalit të pagesës që përdoret për ekzekutimin e tij;
   1.3. mbrojtjen e konfidencialitetit dhe integritetit të kredencialeve të personalizuara të sigurisë të PSHP-ve;
   1.4. vendosjen e standardeve të përbashkëta, të hapura dhe të sigurta të komunikimit ndërmjet ofruesve të shërbimeve të pagesave të llogarisë, ofruesve të shërbimeve të inicimit të pagesave, ofruesve të shërbimeve të informacionit të llogarisë, kryerësve të pagesës, marrësve të pagesës dhe ofruesve të tjerë të shërbimeve të pagesave në lidhje me ofrimin dhe përdorimin e shërbimeve të pagesave në zbatim të Pjesa IV të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.
2. Kjo Rregullore zbatohet për ofruesit e shërbimeve të pagesave, siç përcaktohet në nenin 1, paragrafi 1 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.

Neni 2
Përkufizimet

1. Termat dhe përkufizimet e përdorura në këtë Rregullore kanë të njëjtin kuptim si në Ligjin Nr. 08/L-328 për Shërbimet e Pagesave.
2. Përveç paragrafit 1, për qëllime të zbatimit të kësaj Rregulloreje, termat dhe shkurtesat e mëposhtme kanë kuptimin e mëposhtëm:
   2.1. "OSHPLL" nënkupton Ofruesin e Shërbimeve të Pagesave të Llogarisë;
   2.2. "SHILL" nënkupton Shërbimet e Informacionit të Llogarisë;
   2.3. "OSHILL" nënkupton Ofruesin e Shërbimeve të Informacionit të Llogarisë;
   2.4. "BQK" nënkupton Bankën Qendrore të Republikës së Kosovës;
   2.5. "EBA" nënkupton Autoritetin Bankar Evropian;
   2.6. "VPP" nënkupton Vlerën e Pragut të Përjashtimit;
   2.7. "Ligji për Shërbimet e Pagesave" nënkupton Ligjin Nr. 08/L-328 për Shërbimet e Pagesave;
   2.8. "SHIP" nënkupton Shërbimet e Inicimit të Pagesave;
   2.9. "OSHIP" nënkupton Ofruesin e Shërbimeve të Inicimit të Pagesave;
   2.10. "OSHP" nënkupton Ofruesin e Shërbimeve të Pagesave;
   2.11. "PSHP" nënkupton Përdoruesin e Shërbimeve të Pagesave.

Neni 3
Kërkesat e përgjithshme për autentifikimin

1. OSHP-të kanë mekanizma funksionale të monitorimit të transaksioneve që u mundësojnë zbulimin e transaksioneve të pagesave të paautorizuara ose mashtruese me qëllim të zbatimit të masave të sigurisë të përcaktuara në nënparagrafët 1.1 dhe 1.2 të nenit 1.
   1.1. këta mekanizma bazohen në analizën e transaksioneve të pagesave duke marrë parasysh elementet që janë tipike për PSHP në rrethanat e përdorimit normal të kredencialeve të personalizuara të sigurisë.
2. OSHP-të sigurojnë që mekanizmat e monitorimit të transaksioneve të marrin parasysh, të paktën, secilin nga faktorët e mëposhtëm të bazuar në rrezik:
   2.1. listat e elementeve të autentifikimit, të komprometuara ose të vjedhura;
   2.2. shumën e secilit transaksion pagese;
   2.3. skenarët e njohur të mashtrimit në ofrimin e shërbimeve të pagesave;
   2.4. shenjat e infektimit nga programe keqdashëse (*signs of malware infection*) në çdo sesion të procedurës së autentifikimit;
   2.5. në rast se pajisja e qasjes ose softueri ofrohet nga OSHP-ja, regjistrin e përdorimit të pajisjes për qasje ose softuerit të ofruar në PSHP-ja dhe përdorimit jonormal të pajisjes për qasje ose softuerit.

Neni 4
Rishikimi i masave të sigurisë

1. Zbatimi i masave të sigurisë të përcaktuara në nenin 1 të kësaj Rregullore, dokumentohet, testohet, vlerësohet dhe auditohet periodikisht në përputhje me kornizën ligjore në fuqi për OSHP-të nga auditorë me ekspertizë në sigurinë e TIK-ut (teknologji informative dhe komunikimi) dhe pagesave dhe të pavarur nga pikëpamja operacionale brenda ose nga OSHP-ja.
2. Periudha ndërmjet auditimeve të përcaktuara në paragrafin 1 të këtij neni përcaktohet duke marrë parasysh kornizën përkatëse të kontabilitetit dhe auditimit ligjor të zbatueshme për OSHP-në si në vijim:
   2.1. OSHP-të që përdorin përjashtimin e përcaktuar në nenin 18 të kësaj rregullore i nënshtrohen auditimit të metodologjisë, modelit dhe normave të raportuara të mashtrimit të paktën në baza vjetore. Auditori që kryen këtë auditim ka ekspertizë në sigurinë e TIK-ut dhe pagesave dhe është i pavarur në aspektin operacional brenda ose nga OSHP-ja. Gjatë vitit të parë të zbatimit të përjashtimit sipas nenit 18 të kësaj rregullore dhe të paktën çdo 3 vjet më pas, ose më shpesh me kërkesë të BQK-së, ky auditim kryhet nga një auditor i jashtëm i pavarur dhe i kualifikuar.
3. Ky auditim paraqet vlerësimin dhe raportin mbi përputhshmërinë e masave të sigurisë të PSHP-së me kërkesat e përcaktuara në këtë rregullore. Raporti i vihet në dispozicion BQK-së sipas kërkesës.

KAPITULLI II
MASAT E SIGURISË PËR ZBATIMIN E AUTENTIKIMIT TË THELLUAR TË KLIENTIT

Neni 5
Kodi i autentifikimit

1. Kur OSHP-të zbatojnë autentifikim të thelluar të klientit në përputhje me nenin 97 paragrafin 1 të Ligjit për Shërbimet e Pagesave, autentifikimi bazohet në dy ose më shumë elemente të cilat kategorizohen si njohuri, posedim dhe qenësi dhe rezulton në gjenerimin e kodit të autentifikimit:
   1.1. kodi i autentifikimit pranohet vetëm një herë nga OSHP-ja kur kryerësi i pagesës përdor kodin e autentifkimit për të hyrë në llogarinë e tij të pagesës në internet, për të iniciuar një transaksion elektronik pagese ose për të kryer ndonjë veprim përmes një kanali nga distanca që mund të nënkuptojë rrezik për mashtrim me pagesë ose abuzime të tjera.
2. Për qëllim të paragrafit 1 te këtij neni, OSHP-të miratojnë masa sigurie duke siguruar që secila nga kërkesat e mëposhtme plotësohet:
   2.1. asnjë informacion për asnjë nga elementet e përcaktuara në paragrafin 1 nuk mund të nxirret nga shpalosja e kodit të autentifikimit;
   2.2. gjenerimi i kodit të ri të autentifikimit nuk është i mundur bazuar në njohuritë për ndonjë kod tjetër autentifikimi të gjeneruar më parë;
   2.3. kodi i autentifikimit nuk mund të falsifikohet.

3. OSHP-të sigurojnë që autentifikimi me anë të gjenerimit të kodit të autentifikimit përfshin secilën nga masat e mëposhtme:

   3.1. kur autentifikimi për qasje nga distanca, pagesa elektronike nga distanca dhe çdo veprim tjetër përmes një kanali në distancë që mund të nënkuptojë rrezikun e mashtrimit me pagesa ose abuzime të tjera ka dështuar të krijojë një kod autentifikimi për qëllime të paragrafit 1 të këtij neni, nuk është e mundur të identifikohet cili nga elementet e përcaktuara në paragrafin 1 të këtij neni, ishte i pasaktë;

   3.2. numri i përpjekjeve të dështuara të autentifikimit që mund të ndodhin në mënyrë të njëpasnjëshme, pas së cilës veprimet e referuara në nenin 97, paragrafi 1 të Ligjit për Shërbimet e Pagesave bllokohet përkohësisht ose përgjithmonë, nuk shkon përtej pesë përpjekjeve brenda një periudhe të caktuar kohore;

   3.3. sesionet e komunikimit mbrohen nga kapja e të dhënave të autentifikimit të transmetuara gjatë autentifikimit dhe nga manipulimi nga palët e paautorizuara në përputhje me kërkesat në Kapitullin V të kësaj rregullore;

   3.4. koha maksimale pa aktivitet nga kryerësi i pagesës pasi është autentifikuar për qasjen në llogarinë e tij të pagesave në internet nuk duhet të kalojë 5 (pesë) minuta.

4. Kur bllokimi i përcaktuar në nënparagrafin 3.2 në këtë nen është i përkohshëm, kohëzgjatja e atij bllokimi dhe numri i tentativave përcaktohen bazuar në karakteristikat e shërbimit që i ofrohet kryerësit të pagesës dhe të gjitha rreziqet përkatëse të përfshira, duke marrë parasysh, të paktën, faktorët e përcaktuar në nenin 3 paragrafi 2 të kësaj rregulloreje:

   4.1. paguesi lajmërohet përpara se bllokimi të bëhet i përhershëm;

   4.2. kur bllokimi është bërë i përhershëm, vendoset një procedurë e sigurt që i lejon paguesit të rifitojë përdorimin e instrumenteve të bllokuara të pagesave elektronike.

Neni 6
Lidhjet dinamike

1. Kur OSHP-të aplikojnë autentifikim të thelluar të klientit në përputhje me nenin 97, paragrafi 2 të Ligjit për Shërbimet e Pagesave, përveç kërkesave të nenit 5 të kësaj rregulloreje, ata miratojnë gjithashtu masa sigurie që plotësojnë secilën nga kërkesat e mëposhtme:

   1.1. paguesi vihet në dijeni për shumën e transaksionit të pagesës dhe për përfituesin;

   1.2. kodi i gjeneruar i autentifikimit është specifik për shumën e transaksionit të pagesës dhe për të përfituesin , për të cilin paguesi ka rënë dakord në momentin e inicimit të transaksionit;

   1.3. kodi i autentifikimit i pranuar nga OSHP-ja korrespondon me shumën specifike origjinale të transaksionit të pagesës dhe me identitetin e marrësit të pagesës për të cilin është rënë dakord nga paguesi;

   1.4. çdo ndryshim në shumën ose marrësin e pagesës rezulton në pavlefshmërinë e kodit të gjeneruar të autentifikimit.

2. Për qëllim të paragrafit 1 të këtij neni, OSHP-të miratojnë masa sigurie të cilat sigurojnë konfidencialitetin, autentictetin dhe integritetin e secilës prej sa vijon:

   2.1. shumën e transaksionit dhe marrësin e pagesave gjatë të gjitha fazave të autentifikimit;

2.2. informatat e shfaqur te kryerësi i pagesës gjatë të gjitha fazave të autentifikimit, duke përfshirë gjenerimin, transmetimin dhe përdorimin e kodit të autentifikimit.

3. Për qëllimet e nënparagrafit 1.2 të këtij neni dhe ku OSHP-të aplikojnë autentifikim të thelluar të klientit në përputhje me nenin 97, paragrafi 2 të Ligjit për Shërbimet e Pagesave, për kodin e autentifikimit zbatohen kërkesat e mëposhtme:

3.1. për një transaksion pagese nëpërmjet kartelës, për të cilin paguesi ka dhënë pëlqimin për shumën e saktë të fondeve që do të bllokohen në përputhje me nenin 75, paragrafi 1 të Ligjit për Shërbimet e Pagesave, kodi i autentifikimit është specifik për shumën që paguesi ka dhënë pëlqimin për t'u bllokuar dhe që është rënë dakord nga paguesi gjatë inicimit të transaksionit;

3.2. në lidhje me transaksionet e pagesave për të cilat paguesi ka dhënë pëlqimin për të ekzekutuar një grup transaksionesh pagese elektronike në distancë për një ose disa përfitues, kodi i autentifikimit është specifik për shumën totale të grupit të transaksioneve të pagesës dhe për marrësit e specifikuar të pagesës.

Neni 7
Kërkesat e elementeve të kategorizuara si njohuri

1. OSHP-të miratojnë masa për të zbutur rrezikun që elementët e autentifikimit të thelluar të klientit të kategorizuar si njohuri të zbulohen nga palët e paautorizuara ose t'u zbulohen atyre.

2. Përdorimi i këtyre elementeve nga paguesi i nënshtrohet masave zbutëse për të parandaluar shpalosjen e tyre te palët e paautorizuara.

Neni 8
Kërkesat e elementeve të kategorizuara si posedim

1. OSHP-të miratojnë masa për të zbutur rrezikun që elementët e autentifikimit të thelluar të klientit të kategorizuar si posedim të përdoren nga palë të paautorizuara.

2. Përdorimi nga paguesi i këtyre elementeve i nënshtrohet masave të krijuara për të parandaluar përsëritjen e elementeve.

Neni 9
Kërkesat për pajisjet dhe softuerin, të lidhur me elemente të kategorizuara si të qenësishme

1. OSHP-të miratojnë masa për të zbutur rrezikun që elementët e autentifikimit të kategorizuar si të qenësishëm dhe të lexuar nga pajisjet e qasjes dhe softueri, që i ofrohen paguesit, të shpalosen nga palë të paautorizuara. OSHP-të sigurojnë të paktën që këto pajisje të qasjes dhe softuer të kenë një probabilitet shumë të ulët që një palë e paautorizuar të autentifikohet si kryerës i pagesës.

2. Përdorimi nga kryerësi i pagesës i këtyre elementeve i nënshtrohet masave që sigurojnë që këto pajisje dhe softuer garantojnë rezistencë ndaj përdorimit të paautorizuar të elementeve nëpërmjet qasjes në pajisje dhe softuer.

Neni 10
Pavarësia e elementeve

1. OSHP-të sigurojnë që përdorimi i elementeve të autentifikimit të thelluar të klientit të përcaktuar në nenet 7, 8 dhe 9 të kësaj rregullore i nënshtrohet masave që sigurojnë që, për sa i përket teknologjisë, algoritmeve dhe parametrave, shkelja e njërit prej elementeve të mos rrezikojë besueshmërinë e elementeve të tjerë.
2. OSHP-të miratojnë masa sigurie, kur ndonjë nga elementët e autentifikimit të thelluar të klientit ose vetë kodi i autentifikimit përdoret nëpërmjet një pajisjeje me shumë qëllime, për të zbutur rrezikun që do të rezultonte nga kompromet imi i kësaj pajisjeje shumëfunksionale.
3. Për qëllimet e paragrafit 2 të këtij neni, masat lehtësuese përfshijnë secilën nga sa vijon:
   3.1. përdorimin e mjediseve të ndara të sigurta të ekzekutimit përmes softuerit të instaluar brenda pajisjes shumëfunksionale;
   3.2. mekanizmat për të siguruar që softueri ose pajisja nuk është ndryshuar nga paguesi ose nga një palë e tretë;
   3.3. ku janë bërë ndryshime, mekanizmat për t'i zbutur pasojat e tyre.

KAPITULLI III
PËRJASHTIMET NGA AUTENTIFIKIMI I THELLUAR I KLIENTIT

Neni 11
Qasje në informacionin e llogarisë së pagesës drejtpërdrejt me ofruesin e shërbimit të pagesave të shërbimit të llogarisë ose nëpërmjet një ofruesi të shërbimit të informacionit të llogarisë

1. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit, nëse plotësohen kërkesat e përcaktuara në nenin 3 të kësaj rregullore, kur një PSHP hyn drejtpërdrejt në llogarinë e tij të pagesave në internet, me kusht që qasja të kufizohet në një nga artikujt e mëposhtëm në internet pa shpalosjen e të dhënave të ndjeshme të pagesës:
   1.1. gjendjen e një ose më shumë llogarive të caktuara të pagesave;
   1.2. transaksionet e pagesave të kryera në 90 ditët e fundit nëpërmjet një ose më shumë llogarive të caktuara të pagesave.
2. Me përjashtim të paragrafit 1 të këtij neni, OSHP-të nuk përjashtohen nga zbatimi i autentifikimit të thelluar të klientit kur plotësohet një nga kushtet e mëposhtme:
   2.1. PSHP-ja ka qasje online në informacionin e specifikuar në paragrafin 1 të këtij neni për herë të parë;
   2.2. kanë kaluar më shumë se 180 ditë që nga hera e fundit që PSHP-ja ka qasje në internet në informacionin e specifikuar në paragrafin 1 të këtij neni dhe është zbatuar autentifikimi i thelluar i klientit.
3. OSHP-të nuk zbatojnë autentifikim të thelluar të klientit kur PSHP-ja ka qasje në llogarinë e tij të pagesave në internet nëpërmjet një OSHILL, me kusht që qasja të kufizohet në një nga elementët e mëposhtëm në internet pa shpalosjen e të dhënave të ndjeshme të pagesave:

3.1. gjendjen e një ose më shumë llogarive të caktuara të pagesave;

3.2. transaksionet e pagesave të kryera në 90 ditët e fundit nëpërmjet një ose më shumë llogarive të caktuara të pagesave.

4. Me përjashtim të paragrafit 3, OSHP-të zbatojnë autentifikim të thelluar të klientit kur plotësohet një nga kushtet e mëposhtme:

4.1. PSHP-ja ka qasje online në informacionin e specifikuar në paragrafin 3 të këtij neni për herë të parë nëpërmjet OSHILL-së;

4.2. kanë kaluar më shumë se 180 ditë që nga hera e fundit që PSHP-ja ka qasur në internet informacionin e specifikuar në paragrafin 3 të këtij neni nëpërmjet OSHILL dhe u zbatua autentifikimi i thelluar i klientit.

5. Me përjashtim të paragrafit 3 të këtij neni, OSHP-të lejohen të zbatojnë autentifikim të thelluar të klientit kur PSHP-ja ka qasje në llogarinë e saj të pagesave në internet nëpërmjet OSHILL-së dhe OSHP-ja ka arsye të justifikuara objektivisht dhe të evidentuara siç duhet në lidhje me qasjen e paautorizuar ose mashtruese në llogarinë e pagesës. Në një rast të tillë, OSHP-ja dokumenton dhe arsyeton në mënyrë të duhur në BQK, sipas kërkesës, arsyet për zbatimin e autentifikimit të thelluar të klientit.

6. OSHPSHLL-ve që ofrojnë një ndërlidhje të dedikuar siç përcaktohet në nenin 32 të kësaj rregullore nuk u kërkohet të zbatojnë përjashtimin e përcaktuar në paragrafin 3 të këtij neni për qëllimin e mekanizmit të kontingjentit të përcaktuar në nenin 34 paragrafi 4 të kësaj rregullore, në rastet kur nuk zbatojnë përjashtimin e përcaktuar në paragrafët 1 dhe 2 të këtij neni në ndërlidhjen direkte që përdoret për autentifikimin dhe komunikimin me PSHP-të e tyre.

Neni 12
Pagesa pa kontakt në pikën e shitjes

1. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit nëse i plotësojnë kërkesat e përcaktuara në nenin 2 të kësaj rregullore , kur paguesi inicion një transaksion pagese elektronike pa kontakt, me kusht që të plotësohen kushtet e mëposhtme:

1.1. shuma individuale e transaksionit të pagesës elektronike pa kontakt nuk i kalon 50 euro; dhe

1.2. shuma kumulative e transaksioneve të mëparshme të pagesave elektronike pa kontakt të iniciuara me anë të një instrumenti pagese me funksion pa kontakt nga data e aplikimit të fundit të autentifikimit të thelluar të klientit nuk kalon 150 euro; ose

1.3. numri i transaksioneve të njëpasnjëshme të pagesave elektronike pa kontakt të iniciuara nëpërmjet instrumentit të pagesës që ofron një funksionalitet pa kontakt që nga zbatimi i fundit i autentifikimit të thelluar të klientit nuk është më i madh se pesë transaksione.

Neni 13
Terminalet e pambikëqyrura për tarifat e transportit dhe tarifat e parkimit

OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit nëse plotësojnë kërkesat e përcaktuara në nenin 3 të kësaj rregullore, kur paguesi inicion një transaksion pagese elektronike në

një terminal pagese të pambikëqyrur për qëllimin e pagesës së një tarife transporti ose një tarife parkimi.

Neni 14
Përfituesit e besuar

1. OSHP-të zbatojnë autentifikim të thelluar të klientit kur një pagues krijon ose ndryshon një listë të përfituesve të besuar përmes OSHPLL-së së paguesit.
2. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit nëse plotësohen kërkesat e përgjithshme të autentifkimit, kur paguesi inicion një transaksion pagese dhe marrësi i pagesës përfshihet në një listë të përfituesve të besuar të krijuar më parë nga paguesi.

Neni 15
Transaksionet e përsëritura

1. OSHP-të zbatojnë autentifikim të thelluar të klientit kur një pagues krijon, ndryshon ose inicion për herë të parë një seri transaksionesh të përsëritura me të njëjtën shumë dhe me të njëjtin përfitues.
2. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit nëse i plotësojnë kërkesat e përgjithshme të autentifikimit për inicimin e të gjitha transaksioneve të mëpasshme të pagesave të përfshira në serinë e transaksioneve të pagesave të përmendura në paragrafin 1 të këtij neni.

Neni 16
Transfertat e kredisë ndërmjet llogarive të mbajtura nga i njëjti person fizik ose juridik

OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit nëse i plotësojnë kërkesat e përcaktuara në nenin 3 të kësaj rregullore, kur paguesi fillon një transferim kredie në rrethana kur paguesi dhe marrësi janë i njëjti person fizik ose juridik dhe të dyja llogaritë e pagesave mbahen nga i njëjti OSHPLL.

Neni 17
Transaksionet me vlerë të ulët

1. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit, kur paguesi inicion një transaksion pagese elektronike në distancë, me kusht që të plotësohen kushtet e mëposhtme:
   1.1. shuma e transaksionit të pagesës elektronike në distancë nuk kalon 30 euro; dhe
   1.2. shuma kumulative e transaksioneve të mëparshme të pagesave elektronike në distancë të iniciuara nga paguesi që nga aplikimi i fundit i autentifikimit të thelluar të klientit nuk i kalon 100 euro; ose
   1.3. numri i transaksioneve të mëparshme të pagesave elektronike në distancë të iniciuara nga paguesi që nga zbatimi i fundit i autentifikimit të thelluar të klientit nuk i kalon pesë transaksione të njëpasnjëshme individuale të pagesave elektronike në distancë.

Neni 18
Proceset dhe protokollet e sigurta të pagesave të korporatave

OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit, në lidhje me personat juridikë që iniciojnë transaksione të pagesave elektronike përmes përdorimit të proceseve apo protokolleve të dedikuara të pagesave që u vihen në dispozicion vetëm paguesve që nuk janë klientë, kur BQK-ja vlerëson që këto procese ose protokolle garantojnë të paktën nivele ekuivalente sigurie me ato të parashikuara nga Ligji për Shërbimet e Pagesave.

Neni 19
Analiza e rrezikut të transaksionit

1. OSHP-të mund të mos zbatojnë autentifikim të thelluar të klientit kur paguesi inicion transaksion të pagesave elektronike në distancë të identifikuar nga OSHP-ja si transaksion me nivel të ulët rreziku sipas mekanizmave të monitorimit të transaksioneve të parashikuara në nenin 3 dhe në nënparagrafin 2.3 të këtij neni.
2. Transaksioni i pagesës elektronike i përcaktuar në paragrafin 1 konsiderohet se paraqet nivel të ulët rreziku kur plotësohen të gjitha kushtet e mëposhtme:
   2.1. norma e mashtrimit për atë lloj transaksioni, e raportuar nga OSHP-ja dhe e llogaritur në përputhje me nenin 20 të kësaj rregullore, është ekuivalente ose më e ulët se normat referencë të mashtrimit të specifikuara në tabelën e vendosur në shtojcën 1 të kësaj rregullore për "pagesat elektronike me kartelë në distancë" dhe "transferimet elektronike të kredisë në distancë," përkatësisht;
   2.2. shuma e transaksionit nuk e kalon VPP-në përkatëse të specifikuar në tabelën e paraqitur në shtojcën 1 të kësaj rregullore;
   2.3. OSHP-të, si rezultat i kryerjes së një analize të rrezikut në kohë reale, nuk kanë identifikuar asnjë nga elementet e mëposhtme:
      2.3.1. shpenzime jonormale ose model të sjelljes së paguesit;
      2.3.2. informacion të pazakontë në lidhje me pajisjen e qasjes/softuerin e paguesit;
      2.3.3. infektim me program keqdashës (malware) në çdo sesion të procedurës së autentifikimit;
      2.3.4. skenar të njohur mashtrimi në ofrimin e shërbimeve të pagesave;
      2.3.5. vendndodhje jonormale të paguesit;
      2.3.6. vendndodhje me rrezik të lartë të marrësit të pagesës.
3. OSHP-të që synojnë të përjashtojnë transaksionet e pagesave elektronike në distancë nga autentifikimi i thelluar i klientit me arsyetimin se ato paraqesin rrezik të ulët, marrin parasysh të paktën faktorët e mëposhtëm të bazuar në rrezik:
   3.1. modelet e mëparshme të shpenzimeve të PSHP-së individual;
   3.2. historikun e transaksioneve të pagesave të secilit prej PSHP-ve të OSHP-së;

3.3. vendndodhjen e paguesit dhe të marrësit të pagesës në momentin e transaksionit të pagesës në rastet kur pajisja e qasjes ose softueri sigurohet nga OSHP-ja;

3.4. identifikimin e modeleve jonormale të pagesave të PSHP-së në lidhje me historinë e transaksioneve të pagesave të përdoruesit.

4. Vlerësimi i bërë nga OSHP-ja sipas paragrafit të mëparshëm kombinon të gjithë këta faktorë të bazuar në rrezik në një vlerësim rreziku për çdo transaksion individual për të përcaktuar nëse një pagesë specifike duhet të lejohet pa autentifikim të thelluar të klientit.

Neni 20
Llogaritja e normave të mashtrimit

1. Për çdo lloj transaksioni të përcaktuar në tabelën e Shtojcës 1 te kësaj rregullore, OSHP-ja siguron që normat e përgjithshme të mashtrimit që mbulojnë si transaksionet e pagesave të autentifikuara nëpërmjet autentifikimit të thelluar të klientit ashtu edhe ato të ekzekutuara sipas ndonjë prej përjashtimeve të përcaktuar në nenet 14 deri në 19 të kësaj rregullore janë ekuivalente ose më e ulët se norma referuese e mashtrimit për të njëjtin lloj transaksioni pagese të treguar në tabelën e përcaktuar në shtojcës të kësaj rregullore:

   1.1. norma e përgjithshme e mashtrimit për çdo lloj transaksioni llogaritet si vlera totale e transaksioneve të paautorizuara ose mashtruese në distancë, pavarësisht nëse fondet janë rikuperuar apo jo, pjesëtuar me vlerën totale të të gjitha transaksioneve në distancë për të njëjtin lloj transaksionesh, pavarësisht nëse janë të autentifikuara nëpërmjet zbatimit të autentifikimit të thelluar të klientit ose të ekzekutuara në përputhje me përjashtimet e parashikuara në nenet 14 deri në 19 të kësaj rregullore në baza tremujore (90 ditë).

2. Llogaritja e normave të mashtrimit dhe shifrave që rezultojnë vlerësohen nga rishikimi i auditimit të përcaktuara në nenin 4 paragrafi 2 të kësaj rregullore, i cili siguron që ato të jenë të plota dhe të sakta.

3. Metodologjia dhe çdo model i përdorur nga OSHP-ja për t'i llogaritur normat e mashtrimit, si dhe vetë normat e mashtrimit, dokumentohen në mënyrë adekuate dhe vihen plotësisht në dispozicion të BQK-së.

Neni 21
Ndërprerja e përjashtimeve bazuar në analizën e rrezikut të transaksionit

1. OSHP-të që përdorin përjashtimin e përcaktuar në nenin 18 të kësaj rregullore raportojnë menjëherë në BQK kur një nga normat e tyre të mashtrimit të monitoruara, për çdo lloj transaksioni pagese të treguar në tabelën e paraqitur në shtojcën 1 të kësaj rregullore, tejkalon normën referencë të zbatueshme të mashtrimit dhe duhet t'i ofrojë BQK-së një përshkrim të masave që ata synojnë t'i miratojnë për të rivendosur përputhshmërinë e normës të monitoruar të mashtrimit me normën e referencës së aplikuar të mashtrimit.

2. OSHP-të ndërpresin menjëherë përdorimin e përjashtimit të përcaktuar në nenin 19 të kësaj rregullore për çdo lloj transaksioni pagese të treguar në tabelën e përcaktuar në shtojcë në kufirin specifik të përjashtimit, kur shkalla e tyre e monitorimit të mashtrimit tejkalon për dy tremujorë

radhazi normën referuese të mashtrimit, të zbatueshme për atë instrument pagese ose lloj transaksioni pagese në atë interval të pragut të përjashtimit.

3. Pas përfundimit të përjashtimit të përcaktuar në nenin 19, të kësaj rregullore në përputhje me paragrafin 2 të këtij neni, OSHP-të nuk përdorin përsëri atë përjashtim, derisa norma e tyre e llogaritur e mashtrimit të jetë e barabartë ose më e ulët se normat referencë të mashtrimit të zbatueshme për atë lloj transaksioni pagese në atë interval të pragut të përjashtimit për një tremujor.
4. Kur OSHP-të synojnë të përdorin përsëri përjashtimin e përcaktuar në nenin 19 të kësaj rregullore, ata njoftojnë BQK-në në një afat të arsyeshëm kohor dhe para se të përdorin përsëri përjashtimin, duhet të ofrojnë dëshmi të rivendosjes së përputhshmërisë së normës së tyre të mashtrimit të monitoruar me normën referencë të mashtrimit, të zbatueshme sipas intervaleve përkatëse të përjashtimit, në përputhje me paragrafin 3 të këtij neni.

Neni 22
Monitorimi

1. Për të shfrytëzuar përjashtimet e përcaktuara në nenet 11 deri në 19 të kësaj rregullore, OSHP-të regjistrojnë dhe monitorojnë të dhënat e mëposhtme për çdo lloj transaksioni pagese, me një ndarje për transaksionet e pagesave në distancë dhe jo në distancë, të paktën në baza tremujore:
   1.1. vlerën totale të transaksioneve të pagesave të paautorizuara ose me qëllim mashtrimi në përputhje me nenin 64 paragrafin 2 të Ligjit për Shërbimet e Pagesave, vlerën totale të të gjitha transaksioneve të pagesave dhe normën e mashtrimit që rezulton, duke përfshirë një ndarje të transaksioneve të pagesave të nisura përmes autentifikimit të thelluar të klientit dhe sipas secilit prej përjashtimet;
   1.2. vlerën mesatare të transaksionit, duke përfshirë një ndarje të transaksioneve të pagesave të nisura përmes autentifikimit të thelluar të klientit dhe sipas secilit prej përjashtimeve;
   1.3. numrin e transaksioneve të pagesave ku është zbatuar secili prej përjashtimeve dhe përqindjen e tyre në lidhje me numrin total të transaksioneve të pagesave.
2. OSHP-të do t'i vënë në dispozicion të BQK rezultatet e monitorimit në përputhje me paragrafin 1 të këtij neni.

KAPITULLI IV
KONFIDENCIALITETI DHE INTEGRITETI I KREDENCIALEVE TË PERSONALIZUARA TË SIGURISË TË PËRDORUESVE TË SHËRBIMIT TË PAGESËS

Neni 23
Kërkesat e përgjithshme

1. OSHP-të duhet të sigurojnë konfidencialitetin dhe integritetin e kredencialeve të personalizuara të sigurisë të PSHP, duke përfshirë kodet e autentifikimit, gjatë të gjitha fazave të autentifikimit.
2. Për qëllim të paragrafit 1 të këtij neni, OSHP-të duhet të sigurojnë që secila nga kërkesat e mëposhtme është përmbushur:

2.1. Kredencialet e personalizuara të sigurisë shfaqen të maskuara dhe nuk janë të lexueshme në masën e tyre të plotë kur futen nga PSHP gjatë autentifikimit;

2.2. kredencialet e personalizuara të sigurisë në formatin e të dhënave, si dhe materialet kriptografike që lidhen me enkriptimin e kredencialeve të personalizuara të sigurisë nuk ruhen në tekst të thjeshtë;

2.3. materiali sekret kriptografik mbrohet nga zbulimi i paautorizuar.

3. OSHP-të do të dokumentojnë plotësisht procesin në lidhje me menaxhimin e materialit kriptografik të përdorur për të enkriptuar ose për t'i bërë të palexueshme kredencialet e personalizuara të sigurisë.

4. OSHP-të duhet të sigurojnë që përpunimi dhe transmetimi i kredencialeve të personalizuara të sigurisë dhe i kodeve të autentifikimit të gjeneruara në përputhje me Kapitullin II të kësaj rregulloreje, të bëhet në mjedise të sigurta në përputhje me standardet e thelluara dhe të njohura gjerësisht të industrisë.

Neni 24
Krijimi dhe transmetimi i kredencialeve

1. OSHP-të duhet të sigurojnë që krijimi i kredencialeve të personalizuara të sigurisë të kryhet në një mjedis të sigurt në mënyrë që:

1.1. ato do të zbusin rreziqet e përdorimit të paautorizuar të kredencialeve të personalizuara të sigurisë dhe të pajisjeve dhe softuerit të autentifikimitt pas humbjes, vjedhjes ose kopjimit të tyre përpara dorëzimit të tyre te paguesi.

Neni 25
Lidhja me përdoruesin e shërbimit të pagesave

1. OSHP-të duhet të sigurojnë që vetëm PSHP të jetë i lidhur, në mënyrë të sigurt, me kredencialet e personalizuara të sigurisë, pajisjet e autentifikimit dhe softuerin.

2. Për qëllim të paragrafit 1, OSHP-të duhet të sigurojnë që secila nga kërkesat e mëposhtme është përmbushur:

2.1. lidhja e identitetit të PSHP me kredencialet e personalizuara të sigurisë, pajisjet e autentifikimit dhe softuerin kryhet në mjedise të sigurta nën përgjegjësinë e OSHP që përfshijnë të paktën ambientet e OSHP, mjedisin e internetit të ofruar nga OSHP ose uebfaqe të tjera të ngjashme të sigurta të përdorura nga OSHP dhe shërbimet e tij të makinerive të automatizuara dhe duke marrë parasysh rreziqet që lidhen me pajisjet dhe komponentët themelorë të përdorur gjatë procesit të lidhjes që nuk janë nën përgjegjësinë e OSHP;

2.2. lidhja me anë të një mënyre komunikimi në distancë të identitetit të PSHP me kredencialet e personalizuara të sigurisë dhe me pajisjet ose softuerin e autentifikimit kryhet duke përdorur autentifikim të thelluar të klientit.

Neni 26
Dorëzimi i kredencialeve, pajisjeve dhe softuerit të autentifikimit

1. OSHP-të duhet të sigurojnë që dorëzimi i kredencialeve të personalizuara të sigurisë, pajisjeve dhe softuerit të autentifikimit në PSHP të kryhet në një mënyrë të sigurt të krijuar për të adresuar rreziqet që lidhen me përdorimin e tyre të paautorizuar për shkak të humbjes, vjedhjes ose kopjimit të tyre.

2. Për qëllim të paragrafit 1, OSHP-të do të zbatojnë të paktën secilën nga masat e mëposhtme:

   2.1. mekanizma shpërndarjeje efektive dhe të sigurta që sigurojnë që kredencialet e personalizuara të sigurisë, pajisjet dhe softueri i autentifikimit t'i dorëzohen PSHP legjitime;

   2.2. mekanizmat që lejojnë OSHP të verifikojë vërtetësinë e softuerit të autentifikimit të dorëzuar në PSHP me anë të internetit;

   2.3. marrëveshjet që sigurojnë që, kur dorëzimi i kredencialeve të personalizuara të sigurisë kryhet jashtë ambienteve të OSHP ose përmes një mënyre komunikimi në distancë:

      2.3.1. asnjë palë e paautorizuar nuk mund të marrë më shumë se një veçori të kredencialeve të personalizuara të sigurisë, pajisjeve ose softuerit të autentifikimit kur dorëzohen përmes të njëjtit kanal;

      2.3.2. kredencialet e personalizuara të sigurisë të dorëzuara, pajisjet ose softueri i autentifikimit kërkojnë aktivizim përpara përdorimit;

   2.4. marrëveshjet që sigurojnë që, në rastet kur kredencialet e personalizuara të sigurisë, pajisjet ose softueri i autentifikimit duhet të aktivizohen përpara përdorimit të tyre të parë, aktivizimi do të bëhet në një mjedis të sigurt në përputhje me procedurat e shoqërimit të përcaktuara në nenin 25 të kësaj rregullore.

Neni 27
Rinovimi i kredencialeve të personalizuara të sigurisë

OSHP-të duhet të sigurojnë që rinovimi ose riaktivizimi i kredencialeve të personalizuara të sigurisë t'i përmbahet procedurave për krijimin, lidhjen dhe dorëzimin e kredencialeve dhe të pajisjeve të autentifikimit në përputhje me nenet 24, 25 dhe 26 të kësaj rregullore.

Neni 28
Shkatërrimi, çaktivizimi dhe revokimi

1. OSHP-të duhet të sigurojnë që kanë procese efektive për të zbatuar secilën nga masat e mëposhtme të sigurisë:

   1.1. shkatërrimin, çaktivizimin ose revokimin e sigurt të kredencialeve të personalizuara të sigurisë, pajisjeve dhe softuerit të autentifikimit;

   1.2. kur OSHP shpërndan pajisje dhe softuer të ripërdorshëm të autentifikimit, vendoset, dokumentohet dhe zbatohet ripërdorimi i sigurt i një pajisjeje ose softueri përpara se t'i vihet në dispozicion një PSHP tjetër;

1.3. çaktivizimi ose revokimi i informacionit në lidhje me kredencialet e personalizuara të sigurisë të ruajtura në sistemet dhe bazat e të dhënave të OSHP dhe, kur është e nevojshme, në depo publike.

KAPITULLI V
STANDARDET E HAPURA TË PËRBASHKËTA DHE TË SIGURTA TË KOMUNIKIMIT

Nënkapitulli I
Kërkesat e përgjithshme për komunikim

Neni 29
Kërkesat për identifikimin

1. OSHP-të duhet të sigurojnë identifikim të sigurt kur komunikojnë ndërmjet pajisjes së paguesit dhe pajisjeve të pranimit të përfituesit për pagesat elektronike, duke përfshirë por pa u kufizuar në terminalet e pagesave.
2. OSHP-të duhet të sigurojnë që rreziqet e keqorientimit të komunikimit me palët e paautorizuara në aplikacionet celulare dhe ndërfaqet e përdoruesve të shërbimeve të tjera të pagesave që ofrojnë shërbime të pagesave elektronike janë zbutur në mënyrë efektive.

Neni 30
Gjurmueshmëria

1. OSHP-të duhet të kenë procese të vendosura që sigurojnë që të gjitha transaksionet e pagesave dhe ndërveprimet e tjera me PSHP, me OSHP-të e tjera dhe me subjekte të tjera, duke përfshirë tregtarët, në kontekstin e ofrimit të shërbimit të pagesave janë të gjurmueshme, duke siguruar njohuri *ex post* për të gjitha ngjarjet relevante për transaksionin elektronik në të gjitha fazat e ndryshme.
2. Për qëllim të paragrafit 1, OSHP-të duhet të sigurojnë që çdo seancë komunikimi e krijuar me PSHP, OSHP-të e tjera dhe subjektet e tjera, duke përfshirë tregtarët, të mbështetet në secilën nga sa vijon:
   2.1. një identifikues unik i seancës;
   2.2. mekanizmat e sigurisë për regjistrimin e detajuar të transaksionit, duke përfshirë numrin e transaksionit, vulat kohore dhe të gjitha të dhënat përkatëse të transaksionit;
   2.3. vulat kohore të cilat do të bazohen në një sistem të unifikuar të referencës kohore dhe që do të sinkronizohen sipas një sinjali zyrtar kohor.

Nënkapitulli II
Kërkesa specifike për standardet e hapura të përbashkëta dhe të sigurta të komunikimit

Neni 31
Detyrimet e përgjithshme për ndërfaqet e qasjes

1. OSHPLL-të që i ofrojnë një paguesi një llogari pagese që është e qasshme në internet, duhet të kenë të paktën një ndërfaqe që plotëson secilën nga kërkesat e mëposhtme:

   1.1. OSHILL-të, OSHIP-të dhe OSHP-të që lëshojnë instrumente pagese të bazuara në kartë janë në gjendje të identifikohen drejt OSHPLL-së;

   1.2. OSHILL-të janë në gjendje të komunikojnë në mënyrë të sigurt për të kërkuar dhe marrë informacion mbi një ose më shumë llogari të caktuara pagesash dhe transaksione pagesash të lidhura;

   1.3. OSHIP-të janë në gjendje të komunikojnë në mënyrë të sigurt për të inicuar një urdhërpagesë nga llogaria e pagesës së paguesit dhe të marrin të gjitha informacionet për fillimin e transaksionit të pagesës dhe të gjithë informacionin në dispozicion të OSHPLL në lidhje me ekzekutimin e transaksionit të pagesës.

2. Për qëllime të autentifikimit të PSHP, ndërfaqja e përcaktuar në paragrafin 1 të këtij neni do t'i lejojë OSHILL-të dhe OSHIP-të të mbështeten në të gjitha procedurat e autentifikimit të ofruara nga OSHPLL për PSHP.

3. Ndërfaqja e përmendur në paragrafin 1 të këtij neni duhet të paktën të plotësojë të gjitha kërkesat e mëposhtme:

   3.1. një OSHIP ose një OSHILL do të jetë në gjendje të udhëzojë OSHPLL-në të fillojë autentifikimin në bazë të pëlqimit të NJSP-së;

   3.2. seancat e komunikimit ndërmjet OSHPLL, OSHILL, OSHIP dhe çdo PSHP në fjalë do të krijohen dhe mbahen gjatë gjithë autentifikimit;

   3.3. integriteti dhe konfidencialiteti i kredencialeve të personalizuara të sigurisë dhe i kodeve të autentifikimit të transmetuara nga ose nëpërmjet OSHIP ose OSHILL.

4. OSHPLL-të duhet të sigurojnë që ndërfaqet e tyre të ndjekin standardet e komunikimit të lëshuara nga organizatat ndërkombëtare të standardizimit.

   4.1. OSHPLL-të gjithashtu duhet të sigurojnë që specifikimet teknike të cilësdo ndërfaqe të dokumentohen duke specifikuar një sërë rutinash, protokollesh dhe mjetesh të nevojshme nga OSHIP-të, OSHILL-të dhe OSHP-të që lëshojnë instrumente pagese të bazuara në karta për të lejuar softuerin dhe aplikacionet e tyre të ndërveprojnë me sistemet e OSHPLL;

   4.2. OSHPLL-të duhet të paktën, dhe jo më pak se 6 muaj përpara datës së aplikimit të përcaktuar në nenin 40 të kësaj rregulloreje, ose përpara datës së synuar për nisjen në treg të ndërfaqes së qasjes kur nisja bëhet pas datës së përcaktuar në nenin 40, vendos dokumentacionin në dispozicion, pa pagesë, me kërkesë të OSHIP-ve të autorizuara, OSHILL-ve dhe OSHP-ve që lëshojnë instrumente pagese të bazuara në kartelë ose OSHP-ve që kanë aplikuar në BQK për autorizimin përkatës, dhe do të bëjë një përmbledhje të dokumentacionit në dispozicion të publikut. në faqen e tyre të internetit.

5. Përveç paragrafit 4, OSHPLL-të duhet të sigurojnë që, me përjashtim të situatave emergjente, çdo ndryshim në specifikimin teknik të ndërfaqes së tyre t'u vihet në dispozicion OSHIP-ve të autorizuara, OSHILL-ve dhe OSHP-ve që lëshojnë instrumente pagese të bazuara në kartë, ose OSHP-ve që kanë aplikuar në BQK për autorizimin përkatës, paraprakisht sa më shpejt të jetë e mundur dhe jo më pak se 3 muaj përpara se të zbatohet ndryshimi.

   5.1. OSHP-të do të dokumentojnë situatat emergjente ku janë zbatuar ndryshimet dhe do ta vënë dokumentacionin në dispozicion të BQK sipas kërkesës.

6. Me përjashtim të paragrafit 5 të këtij neni, OSHPLL-të do të vënë në dispozicion të OSHP-ve të përcaktuara në këtë nen ndryshimet e bëra në specifikimet teknike të ndërfaqeve të tyre në mënyrë që të jenë në përputhje me nenin 11 paragrafët 3 deri në 6 të kësaj rregullore, jo më pak se 2 muaj përpara këtyre ndryshime të zbatohen.

7. OSHPLL-të do të vënë në dispozicion një strukturë testimi, duke përfshirë mbështetjen, për lidhjen dhe testimin funksional për të mundësuar OSHIP-të e autorizuara, OSHP-të që lëshojnë instrumente pagese të bazuara në karta dhe OSHILL-të, ose OSHP-të që kanë aplikuar për autorizimin përkatës, të testojnë softuerin dhe aplikacionet e tyre të përdorura për ofertë. një shërbim pagese për përdoruesit. Kjo strukturë testimi duhet të vihet në dispozicion jo më vonë se 6 muaj përpara datës së aplikimit të përcaktuar në nenin 40 të kësaj rregullore ose përpara datës së synuar për nisjen në treg të ndërfaqes së qasjes kur nisja bëhet pas datës së përcaktuara në nenin 40.

   7.1. megjithatë, asnjë informacion i ndjeshëm nuk do të ndahet përmes objektit të testimit.

8. BQK-ja do të sigurojë që OSHPLL-të të respektojnë në çdo kohë detyrimet e përfshira në këtë Rregullore në lidhje me ndërfaqen(t) që ato vendosin. Në rast se një ofrues i OSHPLL nuk përmbush kërkesat për ndërfaqet e përcaktuara në këtë Rregullore, BQK-ja do të sigurojë që ofrimi i SHIP-ve dhe SHILL-ve të mos parandalohet ose ndërpritet në masën që ofruesit përkatës të shërbimeve të tilla janë në përputhje me kushtet e përcaktuara në nenin 34 paragrafi 5 të kësaj rregullore.

Neni 32
Opsionet e qasjes në ndërfaqe

OSHPLL-të do të krijojnë ndërfaqen(t) e përcaktuara në nenin 31 të kësaj rregullore me anë të një ndërfaqeje të dedikuar ose duke lejuar përdorimin nga OSHP-të e përcaktuara në nenin 31 paragrafi 1 të kësaj rregullore i ndërfaqeve të përdorura për autentifikimin dhe komunikimin me PSHP-të e OSHPLL-së.

Neni 33
Detyrimet për një ndërfaqe të dedikuar

1. Në përputhje me nenet 31 dhe 32 të kësaj rregullore, OSHPLL-të që kanë vendosur një ndërfaqe të dedikuar duhet të sigurojnë që ndërfaqja e dedikuar të ofrojë në çdo kohë të njëjtin nivel disponueshmërie dhe performancë, duke përfshirë mbështetjen, si ndërfaqet e vëna në dispozicion të PSHP për qasje të drejtpërdrejtë llogarinë e saj të pagesës në internet.

2. OSHPLL-të që kanë krijuar një ndërfaqe të dedikuar duhet të përcaktojnë tregues transparentë të performancës dhe objektiva të nivelit të shërbimit, të paktën po aq të rrepta sa ato të vendosura për ndërfaqen e përdorur nga PSHP-të e tyre si për sa i përket disponueshmërisë ashtu edhe të dhënave të ofruara në përputhje me nenin 37, ndërfaqet, treguesit dhe objektivat do të monitorohen nga BQK-ja dhe do të testohen me stres testim.

3. OSHPLL-të që kanë vendosur një ndërfaqe të dedikuar duhet të sigurojnë që kjo ndërfaqe të mos krijojë pengesa për ofrimin e SHIP dhe SHILL. Pengesat e tilla mund të përfshijnë, ndër të tjera, parandalimin e përdorimit nga OSHP-të e përcaktuara në nenin 31 paragrafi 1 të kredencialeve të lëshuara nga OSHPLL-të për klientët e tyre, imponimin e ridrejtimit të autentifikimit të OSHPLL ose funksione të tjera, duke kërkuar autorizime dhe regjistrime shtesë përveç atyre. të parashikuara në nenet 15 dhe 19 të Ligjit për Shërbimet e Pagesave, ose që kërkojnë kontrolle shtesë të pëlqimit të dhënë nga PSHP-të për ofruesit e SHIP dhe SHILL.

4. Për qëllimet e paragrafëve 1 dhe 2 të këtij neni, OSHPLL-të do të monitorojnë disponueshmërinë dhe performancën e ndërfaqes së dedikuar. OSHPLL-të do të publikojnë në faqen e tyre të internetit statistika tremujore mbi disponueshmërinë dhe performancën e ndërfaqes së dedikuar dhe të ndërfaqes së përdorur nga PSHP-të e saj.

Neni 34
Masat e paparashikuara për një ndërfaqe të dedikuar

1. OSHPSHLL-të do të përfshijnë, në hartimin e ndërfaqes së dedikuar, një strategji dhe plane për masat e paparashikuara për rastet kur ndërfaqja nuk funksionon në përputhje me nenin 33 te kesaj rregullore, nëse ka mungesë të paplanifikuar të ndërfaqes dhe se ka një avari të sistemit. Mosdisponueshmëria e paplanifikuar ose një prishje e sistemit mund të supozohet se ka lindur kur pesë kërkesave të njëpasnjëshme për qasje në informacion për ofrimin e SHIP ose SHILL nuk u përgjigjen brenda 30 sekondave.

2. Masat e emergjencës do të përfshijnë planet e komunikimit për të informuar OSHP-të duke përdorur ndërfaqen e dedikuar të masave për të rivendosur sistemin dhe një përshkrim të opsioneve alternative të disponueshme menjëherë që OSHP-të mund të kenë gjatë kësaj kohe.

3. Si OSHPLL ashtu edhe OSHP-të të përcaktuara në nenin 31 paragrafi 1 të kësaj rregullore do t'i raportojnë BQK pa vonesë problemet me ndërfaqet e dedikuara siç përshkruhet në paragrafin 1 të këtij neni.

4. Si pjesë e një mekanizmi emergjence, OSHP-të e përcaktuara në nenin 31 paragrafi 1 të kësaj rregullore do të lejohen të përdorin ndërfaqet e vëna në dispozicion të PSHP-ve për autentifikimin dhe komunikimin me OSHPLL-të e tyre, derisa ndërfaqja e dedikuar të rikthehet në nivelin e disponueshmërisë dhe përformanca e parashikuar në nenin 33 të kësaj rregullore.

5. Për këtë qëllim, OSHPLL-të duhet të sigurojnë që OSHP-të e përcaktuara në nenin 31 paragrafi 1 të kësaj rregullore të mund të identifikohen dhe mund të mbështeten në procedurat e autentifikimit të ofruara nga OSHPLL për PSHP-në. Kur OSHP-të e përcaktuara në nenin 31 paragrafi 1 përdorin ndërfaqen e përcaktuar në paragrafin 4 të këtij neni, ata:

   5.1. marrin masat e nevojshme për të siguruar që ata të mos kenë qasje, të ruajnë ose përpunojnë të dhëna për qëllime të ndryshme nga ato për ofrimin e shërbimit siç kërkohet nga PSHP;

5.2. të vazhdojë të respektojë obligimet që rrjedhin nga neni 66 paragrafi 3 dhe neni 67 paragrafi 2 i Ligjit për Shërbimet e Pagesave përkatësisht;

5.3. regjistrojnë të dhënat që qasen përmes ndërfaqes së operuar nga OSHPLL për PSHP-të e saj, dhe ofrojnë, sipas kërkesës dhe pa vonesa të panevojshme, dosjet e regjistrit në BQK;

5.4. t'i arsyetojë siç duhet BQK, sipas kërkesës dhe pa vonesa të panevojshme, përdorimin e ndërfaqes së vënë në dispozicion të PSHP-ve për qasje të drejtpërdrejtë në llogarinë e saj të pagesave online;

5.5. informojnë OSHPLL-në në përputhje me rrethanat.

6. BQK-ja, pasi t'i ketë marrë parasysh udhëzimet e duhura nga EBA ose institucione të tjera të Bashkimit Evropian për të siguruar një zbatim të qëndrueshëm të kushteve të mëposhtme, do të përjashtojë OSHPLL-të që kanë zgjedhur një ndërfaqe të dedikuar nga detyrimi për të ngritur mekanizmin e emergjencës i përshkruar në paragrafin 4 të këtij neni ku ndërfaqja e dedikuar plotëson të gjitha kushtet e mëposhtme:

6.1. është në përputhje me të gjitha detyrimet për ndërfaqet e dedikuara siç përcaktohet në nenin 33 të kësaj rregullore;

6.2. është projektuar dhe testuar në përputhje me nenin 31 paragrafi 7 të kësaj rregullore në harmoni me kërkesat e OSHP-ve të përmendura në të;

6.3. është përdorur gjerësisht për të paktën 3 muaj nga OSHP-të për të ofruar SHILL, SHIP dhe për të dhënë konfirmim mbi disponueshmërinë e fondeve për pagesat me kartë;

6.4. çdo problem në lidhje me ndërfaqen e dedikuar është zgjidhur pa vonesa të panevojshme.

7. BQK-ja do të revokojë përjashtimin e përcaktuar në paragrafin 6 të këtij neni kur kushtet në nënparagrafët 6.1 dhe 6.4 të këtij neni nuk plotësohen nga OSHPLL-të për më shumë se 2 javë kalendarike radhazi. BQK-ja do të sigurojë që OSHPLL-ja të krijojë, brenda një kohe sa më të shkurtër dhe më së voni brenda 2 muajsh, mekanizmin e emergjencës të përcaktuara në paragrafin 4 të këtij neni.

Neni 35
Certifikatat

1. Për qëllime identifikimi, siç përcatohet në nenin 31 paragrafi 1 nënparagrafi 1.1 të kësaj rregullore, OSHP-të do të mbështeten në certifikata të kualifikuara për vula dhe nënshkrime elektronike ose certifikata të kualifikuara për autentifikimin e faqeve të internetit, sipas dispozitave të Ligjit Nr. 08/L – 022 për identifikimin elektronik dhe shërbimet e besuara në transaksionet elektronike.

2. Për qëllime të kësaj rregulloreje, numri unik i identifikimit ose numri i regjistrimit siç përmendet në të dhënat zyrtare në përputhje me Ligjin nr. 08/L – 022 për identifikimin elektronik dhe shërbimet e besueshme për transaksionet elektronike, do të jetë numri i autorizimit. të instrumenteve të pagesave të bazuara në karta lëshuese të OSHP-ve, OSHILL-ve dhe OSHIP-ve, përfshirë OSHPLL-të që ofrojnë shërbime të tilla, të disponueshme në regjistrin publik në përputhje me nenin 19 të ligjit për Shërbimet e Pagesave ose që rezultojnë nga licenca ose korniza e autorizimit dhe rregullat e zbatueshme për OSHP-të e tjera të zbatueshme, si bankat.

3. Për qëllimet e kësaj rregulloreje, certifikatat e kualifikuara për vulat elektronike ose për autentifikimin e uebfaqes të përcaktuara në paragrafin 1 te këtij neni do të përfshijnë, në një gjuhë

të zakonshme në sferën e financave ndërkombëtare, atribute specifike shtesë në lidhje me secilën nga sa vijon:

3.1. roli i OSHP, i cili mund të ketë një ose më shumë nga sa vijon:

3.1.1. shërbimi i llogarisë;

3.1.2. fillimi i pagesës;

3.1.3. informacion për llogarinë;

3.1.4. lëshimi i instrumenteve të pagesave me kartelë;

3.2. Banka Qendrore e Kosovës, ku është e regjistruar OSHP-ja.

4. Atributet e përcaktuara në paragrafin 3 të këtij nuk do të ndikojnë në ndërveprimin dhe njohjen e certifikatave të kualifikuara për vulat elektronike ose autentifikimin e faqes në internet.

Neni 36
Siguria e sesionit të komunikimit

1. OSHPLL-të, OSHP-të që lëshojnë instrumentet e pagesave të bazuara në karta, OSHILL-të dhe OSHIP-të duhet të sigurojnë që, kur shkëmbehen të dhëna me anë të internetit, të zbatohet enkriptim i sigurt ndërmjet palëve komunikuese gjatë sesionit përkatës të komunikimit, në mënyrë që të ruhet konfidencialiteti dhe integriteti i të dhënave, duke përdorur teknika të forta dhe të njohura gjerësisht të kriptimit.
2. OSHP-të që lëshojnë instrumente pagese të bazuara në kartë, OSHILL-të dhe OSHIP-të do t'i mbajnë seancat e qasjes të ofruara nga OSHPLL-të sa më të shkurtra që të jetë e mundur dhe do të ndërpresin në mënyrë aktive çdo seancë të tillë sapo të ketë përfunduar veprimi i kërkuar.
3. Gjatë mbajtjes së seancave paralele të rrjetit me OSHPLL-në, OSHILL-të dhe OSHIP-të duhet të sigurojnë që ato sesione të jenë të lidhura në mënyrë të sigurt me sesionet përkatëse të krijuara me PSHP-të, në mënyrë që të parandalohet mundësia që çdo mesazh ose informacion i komunikuar ndërmjet tyre të jetë i gabuar.
4. OSHILL-të, OSHIP-të dhe OSHP-të që lëshojnë instrumente pagese të bazuara në kartë me OSHPLL-në duhet të përmbajnë referenca të qarta për secilin nga pikat e mëposhtme:

4.1. PSHP-ja ose përdoruesit dhe sesioni përkatës i komunikimit për të dalluar disa kërkesa nga i njëjti PSHP ose përdorues;

4.2. për SHIP-të, transaksioni i pagesës i identifikuar në mënyrë unike i iniciuar;

4.3. për konfirmimin e disponueshmërisë së fondeve, kërkesa e identifikuar në mënyrë unike lidhur me shumën e nevojshme për ekzekutimin e transaksionit të pagesës me kartë.

5. OSHPLL-të, OSHILL-të, OSHIP-të dhe OSHP-të që lëshojnë instrumente pagesash të bazuara në kartë, duhet të sigurojnë që kur komunikojnë kredencialet e personalizuara të sigurisë dhe kodet e autentifikimit, këto nuk janë të lexueshme, drejtpërdrejt ose tërthorazi, nga asnjë personel në çdo kohë.
6. Në rast të humbjes së konfidencialitetit të kredencialeve të personalizuara të sigurisë në sferën e tyre të kompetencës, këta ofrues do të informojnë pa vonesë të panevojshme NJSP-në e lidhur me ta dhe lëshuesin e kredencialeve të personalizuara të sigurisë.

Neni 37
Shkëmbimet e të dhënave

1. OSHPLL-të duhet të përmbushin secilën nga kërkesat e mëposhtme:

   1.1. ata do t'u japin OSHILL-ve të njëjtin informacion nga llogaritë e përcaktuara të pagesave dhe transaksionet e pagesave të lidhura që vihen në dispozicion të PSHP kur kërkojnë drejtpërdrejt qasje në informacionin e llogarisë, me kusht që ky informacion të mos përfshijë të dhëna delikate pagesash;

   1.2. ata, menjëherë pas marrjes së urdhërpagesës, do t'i ofrojnë OSHIP-ve të njëjtat informacione për fillimin dhe ekzekutimin e transaksionit të pagesës të ofruar ose vënë në dispozicion të PSHP kur transaksioni është iniciuar drejtpërdrejt nga kjo e fundit;

   1.3. ata, sipas kërkesës, do t'i japin menjëherë OSHP-ve një konfirmim në një format të thjeshtë 'po' ose 'jo', nëse shuma e nevojshme për ekzekutimin e një transaksioni pagese është e disponueshme në llogarinë e pagesës së paguesit.

2. Në rast të një ngjarjeje ose gabimi të papritur që ndodh gjatë procesit të identifikimit, autentifikimit ose shkëmbimit të elementeve të të dhënave, OSHPLL do t'i dërgojë një mesazh njoftimi OSHIP ose OSHILL dhe OSHP që lëshon instrumentet e pagesave të bazuara në kartë, i cili shpjegon arsyeja për ngjarjen ose gabimin e papritur:

   2.1. kur OSHPLL ofron një ndërfaqe të dedikuar në përputhje me nenin 33 të kësaj rregullore, ndërfaqja duhet të sigurojë mesazhe njoftimi në lidhje me ngjarjet ose gabimet e papritura që do t'u komunikohen nga çdo OSHP që zbulon ngjarjen ose gabimin OSHP-ve të tjera që marrin pjesë në seancën e komunikimit.

3. OSHILL-të duhet të kenë mekanizma të përshtatshëm dhe efektivë që pengojnë qasjen në informacione të ndryshme nga llogaritë e përcaktuara të pagesave dhe transaksionet e pagesave të lidhura me to, në përputhje me pëlqimin e qartë të përdoruesit.

4. OSHIP-të do t'u ofrojnë OSHPLL-ve të njëjtat informacione siç kërkohet nga PSHP-ja kur të iniciojnë drejtpërdrejt transaksionin e pagesës.

5. OSHILL-të do të jenë në gjendje t’i qasen informacionit nga llogaritë e caktuara të pagesave dhe transaksionet e pagesave të lidhura të mbajtura nga OSHPLL-të për qëllime të kryerjes së SHILL në njërën nga rrethanat e mëposhtme:

   5.1. sa herë që PSHP kërkon në mënyrë aktive një informacion të tillë;

   5.2. kur PSHP-ja nuk e kërkon në mënyrë aktive një informacion të tillë, jo më shumë se katër herë në një periudhë 24-orëshe, përveç rastit kur është rënë dakord për një frekuencë më të lartë ndërmjet OSHILL dhe OSHPLL, me pëlqimin e PSHP-së.

Neni 38
Shtojca

Pjesë përbërëse e kësaj rregulloreje është Shtojca 1 Norma referuese e mashtrimit.

KAPITULLI VI
DISPOZITAT PËRFUNDIMTARE

Neni 39
Zbatimi, masat përmirësuese dhe ndëshkimet

Çdo shkelje e dispozitave të kësaj Rregulloreje do t'i nënshtrohet masave korrigjuese dhe ndëshkimeve administrative, të përcaktuara në nenin 67 të Ligjit Nr. 03/L-209 për Bankën Qendrore të Republikës së Kosovës të ndryshuar dhe plotësuar me Ligjin Nr. 05/L -150 si dhe nenin 124 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.

Neni 40
Periudha kalimtare

OSHP-të që i nënshtrohen kësaj Rregulloreje, do t'i përshtatin aktivitetet dhe operacionet e tyre me dispozitat e kësaj Rregulloreje jo me vonë se periudha maksimale prej 18 muajsh – periudhë që korrespondon me periudhën tranzitore në nenin 137 të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.

Neni 41
Hyrja në fuqi

Kjo Rregullore hyn në fuqi 10-(dhjetë) ditë pas hyrjes në fuqi të Ligjit Nr. 08/L-328 për Shërbimet e Pagesave.

Dr.sc. Bashkim Nurboja
Kryetar i Bordit të Bankës Qendrore të Republikës së Kosovës

SHTOJCA 1

Norma referuese e mashtrimit (%) për:		
ETV	**Pagesat elektronike në distancë të bazuara në kartë**	**Transfertat elektronike të kreditit në distancë**
500 euro	0,01	0,005
250 euro	0,06	0,01
100 euro	0,13	0,015