KUSHTET E PUNËS PËR PËRDORIMIN E SHËRBIMIT BANKAR DIXHITAL

1. Hyrje

Kushtet e Punës për përdorimin e shërbimit bankar dixhital (këtej e tutje referuar si "**Kushtet e Punës**" *rregullojnë të drejtat dhe detyrimet e Bankës si ofruese e shërbimit dhe të Klientit në lidhje me kontraktimin dhe përdorimin e shërbimit bankar dixhital (këtej e tutje referuar si "Shërbimi".*

2. Përkufizime

- **Banka** – Intesa Sanpaolo Bank Albania, me Zyra qëndrore në Rrugën Ismail Qemali nr 27, Tiranë, Shqipëri,
  Website: www.intesasanpaolobank.al;
  Numra kontakti: tel: +355 4 2276000; 0800600 (falas nga Albtelecom dhe Eagle), +355 692080903;
  Degët e Bankës, lista e të cilave gjendet në faqen zyrtare të Bankës www.intesasanpaolobank.al;
- **Klienti** – nënkupton një klient të Bankës i cili ka të paktën një llogari aktive me Bankën (të cilën e zotëron vetëm dhe/ose është mbajtës i përbashkët me të drejta të plota për të vepruar veç në llogari), i cili kërkon të përdorë shërbimin bankar dixhital.
- **Përdorues** – nënkupton Klientin e miratuar nga Banka për të përdorur shërbimin dixhital
- **Komunikim në distancë** - nënkupton që shërbimi mund të përdoret pa praninë e njëkohëshme fizike të Përdoruesit dhe të Bankës me qëllim aksesimin dhe përdorimin e shërbimit bankar dixhital, përfshirë edhe nënshkrimin e kontratave në distancë: internet banking, mobile banking dhe mënyra të tjera që Banka do të nxjerrë në vazhdimësi.
- **Shërbimi bankar dixhital (shërbimi)** - përfshin mundësinë e kontraktimit dhe përdorimit të shërbimeve financiare dhe bankare përmes mënyrave të komunikimit në distancë, duke mundësuar informacion për gjendjen e llogarisë dhe transaksionet, mundësine e kryerjes së veprimeve bankare dhe duke mundësuar kontraktimin e shërbimeve bankare dhe financiare në formë elektronike (aty ku është e aplikueshme).
- **Pjesa publike e shërbimit** – një pjesë e shërbimit e cila është e disponueshme për të gjithë, përfshirë disa shërbime të përdoruesit, pa qënë nevoja për të aplikuar më parë. Përmban informacion mbi si të familjarizoheni me funksionalitetet e shërbimit, përllogaritësin e kursit dhe informacion mbi kursin e këmbimit të Bankës, listën e ATM-ve, detajet e kontaktit të Bankës. Për përdoruesit e shërbimit, në aplikacionin mobile, mundëson gjithashtu edhe një pamje të përgjithshme të statusit të llogarisë së përzgjedhur, mundësinë për të aktivizuar dhe për të përdorur disa funksionalitete të shërbimit, dhe për të kryer logimin duke përdorur pajisjen e autorizimit #withKEY. Banka rezervon të drejtën për të ndryshuar këtë përmbajtje.
- **Pjesa private e shërbimit** – pjesa e shërbimit që i mundësohet Klientëve të cilët kanë hyrë me sukses në shërbim përmes autentifikimit / autorizimit.
- **Autentifikimi** – identifikimi i Përdoruesit me elementët e personalizuar të sigurisë (kredencialet). Proçesi i autentifikimit lejon verifikimin e përdorimit të një mënyre të veçantë sistemi autentifikimi / autorizimi, përfshirë verifikimin e elementëve të personalizuar të sigurisë dhe kësisoj edhe verifikimin e identitetit të Përdoruesit.
- **Autorizimi –** proçesi i dhënies së miratimit për të ekzekutuar urdhër pagesa, disa kontrata ose për çdo qëllim tjetër që mundësohet nga shërbimi. Nëpërmjet autorizimit, Përdoruesi pranon kushtet që i janë paraqitur (kurdo që aplikohen) përpara autorizimit. Opsioni dhe mënyra e autorizimit varet nga karakteristikat e shërbimit dhe nga analiza e sjelljes së Përdoruesit.
- **Elementët e sigurisë** – nënkuptojnë elementët e sigurtë të cilët përdoren ose për autentifikim ose për autorizim duke përfshirë por pa u kufizuar në SMS OTP (fjalëkalim njëpërdorimësh), kodin PIN, #withKEY (Token Software), ose Token fizik.
- **Kodi i regjistrimit** – një sërë numrash të cilat kërkohen për të aktivizuar aplikacionin mobile, i përbërë nga dy pjesë – kodi i identifikimit dhe kodi i aktivizimit të cilin Banka ja mundëson Përdoruesit përmes kanaleve të ndryshme të cilat mund të jenë SMS, internet banking ose kanale të tjera të përcaktuara nga Banka. Banka mund të mundësojë një pjesë të kodit të regjistrimit përmes shërbimit call center ose përmes degës.
- **Sistemet e autentifikimit / autorizimit** - pajisjet, aplikacionet apo metodat për autentifikim dhe autorizim që mundësojnë aksesin në, ose përdorimin e shërbimeve dixhitale bankare:
  - **#withKEY** – sistemi i autentifikimit dhe autorizimit i integruar në aplikacionin mobile dhe që mundëson aksesin në, ose përdorimin e Shërbimit. Kredenciali për hyrjen në sistem është PIN-i.
  - **Login i zgjuar** - sistemi i autentifikimit dhe autorizimit i cili është i integruar në aplikacionin mobile dhe që mundëson aksesin në, ose përdorimin e Shërbimit përmes dërgimit të një njoftimi 'push', ose përmes dërgimit të një kodi SMS. Përdoruesi mund të zgjedhë të përdorë logimin e zgjuar kur hyn në shërbim. Sistemi i logimit të zgjuar përdoret gjithashtu për implementimin e autorizimit TDS.
  - **Token –** një pajisje fizike e personalizuar që gjeneron fjalëkalime njëpërdorimëshe të aksesueshme përmes PIN-it, i cili shërben për autentifikimin e përdoruesit dhe autorizimin e transaksioneve.
  - **ID e përdoruesit** – një identifikues unik i Përdoruesit i gjeneruar në momentin që nënshkruan për Shërbimin. Përdoret si një nga elementët për të verifikuar identitetin e Përdoruesit kur akseson Shërbimin.
  - **Metodat biometrike** - metodat e autentifikimit dhe autorizimit të bazuara në karakteristikat fizike të Përdoruesit (p.sh. gjurmë gishti, identifikim i fytyrës). Banka, për qëllime të përdorimit të Shërbimeve, mund ti mundësojë

Përdoruesit autentifikimin dhe autorizimin me metoda biometrike në përputhje me mundësitë teknike të Përdoruesit dhe të Bankës. Me qëllim përdorimin e medotave të autentifikimit / autorizimit biometrik, Banka mund të përdorë informacionin personal që Përdoruesi ka ruajtur me një palë të tretë (brenda programit që gjendet në pajisjen e përdorur për të aksesuar Shërbimin) dhe e ka aktivizuar për autentifikim / autorizim brenda Shërbimit (p.sh. gjurmë gishti, identifikim i fytyrës), pa i ruajtur ato në Bankë, dhe as nuk mbledh ose ruan apo përdor parametrat biometrike të Përdoruesit, pa marrë miratimin paraprak të Përdoruesit.

- **Touch ID** – një metodë autentifikimi dhe autorizimi që përdor gjurmën e gishtit të Përdoruesit, e cila është ruajtur më parë në programin e pajisjes mobile të Përdoruesit dhe që suporton një lexues gjurmësh gishtash dhe si rrjedhojë aktivizohet në aplikacionin mobile.
- **Face ID -** një metodë autentifikimi dhe autorizimi që përdor identifikimin e fytyrës së Përdoruesit, e cila është ruajtur më parë në në programin e pajisjes mobile të Përdoruesit dhe që suporton idenfitikimin e fytyrës dhe si rrjedhojë aktivizohet në aplikacionin mobile.

  Përdoruesi mund të përdorë metodat biometrike në varësi të mundësive teknologjike të pajisjes celulare që ka në përdorim.

- **#withSIGN** – Firma Elektronike e Kualifikuar, për qëllimin e këtyre Kushteve të Përgjithshme do të konsiderohet Firma Elektronike e Kualifikuar bazuar në një Çertifikatë të Kualifikuar të lëshuar nga Intesa Sanpaolo S.p.A në cilësinë e Ofruesit të Kualifikuar të Shërbimeve të Besuara sipas një kontrate të veçantë. Çertifikata Elektronike e Kualifikuar përdoret për të firmosur elektronikisht dokumentacionin gjatë kontraktimit të një shërbimi bankar dhe financiar përmes shërbimit dixhital.
- **Fjalëkalim njëpërdorimësh (OTP) –** një seri numrash që gjenerohen sipas kërkesës përmes #withKEY ose përmes një tokeni fizik, që ka një kohëzgjatje të kufizuar dhe e cila mund të përdoret vetëm një herë.
- **Firmosja e të dhënave të transaksionit (Transaction Data Signing – TDS)** – nënkupton një mënyrë të sigurtë autorizimi si për shembull në rast se llogaria e përfituesit nuk është e besuar, ose në rast se analiza e sjelljes tregon se është e nevojshme një mënyrë më e sigurtë autorizimi, etj.

  Ajo kryhet duke përdorur sistemin e autentifikimit / autorizimit te zgjuar të login – si autorizim duke dërguar një mesazh automatik 'push'. Në rast se, për arsye teknike, nuk është e mundur të përdoret kjo proçedurë, atëherë dërgohet si SMS.
  - **Dërgimi i mesazhit 'push'** – një proçedurë autorizimi veprimi në shërbimin dixhital që ndodh në mënyrë të tillë që Përdoruesi përmes aplikacionit internet banking fillon dërgimin e kërkesës 'push' drejt një numri celular që është regjistruar më parë në Bankë dhe është përdorur për të kontraktuar Shërbimin. Njoftimi përmban disa elementë të veprimit (p.sh. Përfituesin, Shumën dhe Kodin).
  - **Autorizimi SMS** - një proçedurë autorizimi veprimi në shërbimin dixhital që ndodh në mënyrë të tillë që Banka dërgon një mesazh SMS në numrin celular të Përdoruesit që është regjistruar më parë në Bankë. Mesazhi SMS përmban disa elementë të veprimit (p.sh. Përfituesin, Shumën dhe Kodin).
- **Limiti** – nënkupton shumën maksimale të disa veprimeve të cilat klienti lejohet të kryejë përmes shërbimit dixhital brenda një dite (në rastin e limitit ditor) dhe brenda një muaji kalendarik (në rastin e limitit mujor).
- **Njoftimet 'Push'** – Njoftimet që i dërgohen Përdoruesit nga Banka në paisjen celulare, në lidhje me produktet, shërbimet dhe ngjarjet, të cilat Përdoruesi ka zgjedhur dhe aktivizuar paraprakisht në seksionin Konfigurime të Shërbimit. Përdoruesi zgjedh nëse do të përdorë ose jo opsionin për të filluar njoftimin dhe zgjedh përkatësisht secilin opsion që dëshiron të aktivizojë brenda shërbimit.
- **Pagesa #withPAY** – një funksionalitet që i mundëson klientit kryerjen e pagesave drejtpërdrejt nga faqja përpara hyrjes e aplikacionit duke përzgjedhur përfituesin nga lista e kontakteve. Në vend të numrit të llogarisë së pritësit, përdoret informacioni i lidhur paraprakisht me përfituesin specifik i cili është regjistruar më parë në komunitetin e pagesave. Informacioni që Përdoruesi mund të lidhë me numrin e llogarisë së veprimit me qëllim implementimin e këtij transaksioni, mund të jetë numri i telefonit, ose ndonjë informacion tjetër të cilin Banka mund ta importojë më pas. Përdoruesi vendos ta përdorë apo jo këtë funksionalitet dhe siguron përkatësisht të dhënat dhe jep miratimin e nevojshëm për të aktivizuar këtë funksionalitet.
- **Transfertë e thjeshtë –** ky funksionalitet i mundëson përdoruesit kryerjen e veprimeve brenda produkteve të tij (llogarive ose llogarive dhe kartave në rastin e pagesës së kartës, etj) pa qënë nevoja për autorizim. Përdoruesi vendos ta aktivizojë apo jo këtë funksionalitet brenda shërbimit.
- **Llogari e besuar** – një funksionalitet që mundëson përmes shërbimit bankar dixhital, pa përdorimin e procedurës së autorizimit të transaksionit, transferta drejt llogarisë së përfituesit të cilin Përdoruesi e ka regjistruar më parë ne listën e Përfituesve dhe e ka klasifikuar si llogari të besuar. Përdoruesi vendos ta aktivizojë apo jo opsionin dhe e autorizon duke vendosur PIN-in ose fjalëkalimin njëpërdorimësh.
- **Gjendje e shpejtë** – funksionalitet që mundëson verifikimin e gjendjes së llogarisë dhe balancës së disponueshme në zonën publike të shërbimit. Përdoruesi vendos ta aktivizojë ose jo këtë funksionalitet dhe përkatësisht zgjedh opsionin brenda shërbimit dhe e autorizon atë dukë përdorur PIN-in ose fjalëkalimin njëpërdorimësh. Në rast se Përdoruesi dëshiron të kontrollojë gjendjen dhe shumën e disponueshme në llogari, e bën këtë duke aksesuar dritaren përkatëse në aplikacionin mobile.
- **Pay&Go** – është bashkëpunimi ndërmjet Bankës dhe kompanisë Pay&Go shpk regjistruar në Shqipëri, që i mundëson klientëve të kryejnë pagesa drejt Partnerëve të Pay&Go ose nëpërmjet ATM-ve të Bankës që gjenden në territorin e Shqipërisë ose përmes shërbimit bankar në celular/internet. Partnerët e Pay &Go janë entitetet financiare dhe/ose tregtare

të cilat kanë firmosur një marrëveshje anëtarësimi me Pay&Go për pagesën e fatyrave të tyre përmes platformës së pagesave të Pay&Go.

3. Kushtet e përdorimit të shërbimit bankar dixhital

Kontrata për përdorimin e Shërbimit mund të firmoset duke u paraqitur në Bankë ose përmes shërbimeve bankare dixhitale ose portalit publik, në momentin që Banka e mundëson këtë opsion.

Çdo klient me të paktën një llogari të hapur në Bankë lejohet të kontraktojë shërbimin bankar dixhital.

Në rast të mbajtësve të përbashkët të llogarisë, Banka do i mundësojë shërbimin dixhital secilit mbajtës llogarie vetëm kur mbajtësit e llogarisë kanë të drejta për të vepruar veç e veç në llogari – me kusht që Banka të firmosë Marrëveshjen me secilin prej mbajtësve të llogarisë që kërkon akses në Shërbim.
Në rast të llogarive të përbashkëta ku mbajtësit e llogarisë kanë të drejta për të vepruar vetëm bashkërisht, shërbimin bankar dixhital nuk iu mundësohet atyre.

Për të përdorur Internet banking, Përdoruesit i kërkohet që ta aksesojë shërbimin nga një kompjuter personal, laptop, tabletë ose nga një pajisje tjetër e përshtatshme (që përmbush kushtet teknike të specifikuara në manualin e përdorimit të internet banking), e cila duhet të jetë e lidhur me Internetin. Për të përdorur aplikacionin mobile, aplikacioni duhet shkarkuar nga dyqani përkatës në një pajisje (që përmbush kushtet teknike të specifikuara në manualin e përdoruesit të mobile banking), e cila duhet të jetë e lidhur me Internetin.

4. Kushtet teknike

Gjatë kontraktimit të shërbimit, Përdoruesi është i detyruar ti bëjë të ditur Bankës numrin e telefonit të pajisjes celulare tek e cila Banka do të dërgojë një pjesë të kodit të regjistrimit (kodit të identifikimit) që nevojitet për të aktivizuar aplikacionin mobile. Përdoruesi duhet gjithashtu ti bëjë të ditur Bankës një adresë emaili tek e cila Banka mund të dërgojë dokumenta që kanë lidhje me Shërbimin, nëse është e nevojshme.

Klienti duhet të garantojë që të gjitha parametrat e shfletuesit janë vendosur siç duhet, në përputhje me kushtet teknike të kërkuara.
Banka nuk do të jetë përgjegjëse për ndonjë dëm që vjen si rezultat i faktit që Përdoruesi nuk ka përdorur në mënyrën e duhur pajisjet apo programin që nevojitet për shërbimin bankar dixhital, domethënë, Klienti nuk e ka aksesuar dhe përdorur shërbimin nga dyqanet e internetit të specifikuara në manual por përmes ndërmjetësimit ose asistencës nga ndonjë faqe apo platformë tjetër, ose në rastin kur Klienti nuk ushtron kujdesin e duhur në zgjedhjen e ambjentit në të cilin do të përdorë shërbimin bankar dixhital. Banka nuk pranon asnjë përgjegjësi për dëmet që vijnë si rezultat i ndotjes së sistemeve IT të Përdoruesit nga viruset.

Banka nuk merr përsipër asnjë përgjegjësi për ndonjë dëm të shkaktuar nga fakti që parametrat e shfletuesit janë të ndryshme nga kushtet e nevojshme teknike.

5. Aksesimi dhe përdorimi i shërbimit përmes aplikacionit mobile

Shkarkimi i aplikacionit

Për të aksesuar dhe përdorur Shërbimin përmes aplikacionit bankar në celular, Përdoruesi duhet të përdorë një pajisje celulare të përshtatshme me kërkesat teknike si dhe të përdorë metodën e identifikimit të zgjedhur nga Klienti dhe të përcaktuar në Marrëveshje.
Përdoruesi e shkarkon aplikacionin mobile nga dyqanet virtuale App Store ose Google Play store, në varësi të platformës celulare që përdor.

Regjistrimi

Pas kontraktimit të Shërbimin, për logimin fillestar në aplikacionin mobile, Përdoruesi duhet të shkarkojë aplikacionin dhe ta instalojë atë në pajisjen celulare si dhe të kryejë proçesin e regjistrimit duke vendosur në fushat respektive të aplikacionit mobile kodin e regjistrimit që nevojitet për aktivizimin e aplikacionit mobile: kodi i marrë nga dega dhe kodi i marrë me SMS në numrin e telefonit të Klientit.

Pas instalimit dhe aktivizimit të aplikacionit përmes futjes së kodit të regjistrimit që i është caktuar Përdoruesit, Përdoruesi përcakton elementin e personalizuar të sigurisë – PIN-in (si dhe aktivizon elementët biometrik të sigurisë si gjurma e gishtit, identifikimi i fytyrës ose ndonjë metodë tjetër biometrike që mundësohet herë pas here), me të cilin, më vonë, do të aksesojë dhe përdorë aplikacionin mobile. PIN-i i shërben Përdoruesit për tu autentifikuar kur hyn në Shërbim nga celulari dhe mund të përdoret gjithashtu, aty ku është e aplikueshme, edhe për të dhënë miratimin e klientit për ekzekutimin e veprimeve dhe kontraktimin e produkteve ose ose për çdo qëllim tjetër që shërbimi mundëson, në përputhje me rregulloret në fuqi.

- Nëse Klienti ka përzgjedhur PIN-in si dhënie miratimi për ekzekutimin e veprimeve dhe për dhënie të miratimeve të tjera, nuk është i nevojshëm autorizimi i tyre më një metodë biometrike.
- Nëse Klienti ka përzgjedhur gjurmën e gishtit për autentifikim dhe për dhënie miratimi për ekzekutimin e veprimeve dhe për dhënie të miratimeve të tjera, nuk është i nevojshëm autorizimi i tyre me një metodë tjetër biometrike ose me PIN.
- Nëse Klienti ka përzgjedhur identifikimin e fytyrës për autentifikim dhe për dhënie miratimi për ekzekutimin e veprimeve dhe për dhënie të miratimeve të tjera, nuk është i nevojshëm autorizimi i tyre më një metodë tjetër biometrike ose me PIN.

Ri-Regjistrimi

Nëse aplikacioni bllokohet, fshihet apo përdoruesi dëshiron të instalojë aplikacionin në një tjetër pajisje mobile në vend të pajisjes ekzistuese, atëherë nevojitet një kod i ri regjistrimi (kod identifikimi dhe aktivizimi) për të riaktivizuar sërisht aplikacionin. Kodi i ri i regjistrimit për aktivizimin e aplikacionit mobile, mund të kërkohet nga Përdoruesi i Shërbimit në degë ose përmes shërbimit Call Center. Përmes kësaj të fundit, kodi mund të merret vetëm në rast se është kryer me sukses identifikimi i Klientit.

Përdorimi i metodave të autentifikimit është në përputhje me procedurat e aplikuara nga Banka për identifikimin e Klientit dhe verifikimin e të drejtave mbi llogarinë bankare. Përtej kësaj Banka nuk verifikon të drejtat e Përdoruesit për të përdorur kredencialet në përputhje me sa më sipër e as rrethanat e këtij përdorimi.

Klienti mban përgjegjësi të plotë në lidhje më të gjitha veprimet bankare dhe me përdorimin e shërbimeve suplementare, duke qënë se kryhen nga Përdoruesi me aplikimin e njërës prej metodave të mësipërme të identifikimit që i janë vënë në dispozicion Përdoruesit.

6. Aksesimi dhe përdorimi i shërbimit përmes internet banking

Për të aksesuar dhe përdorur shërbimet përmes internet banking, Përdoruesi duhet të aksesojë faqen në web.

Aksesi dhe përdorimi i Shërbimit përmes internet banking është i mundur nëse përdoret njëra nga sistemet e mëposhtme të autentifikimit / autorizimit:

#withKEY – nëse klienti ka zgjedhur software token, ai mund të logohet në internet banking vetëm pasi ka shkarkuar dhe regjistruar më parë aplikacionin mobile brenda të cilit është vendosur #withkey i cili do të gjenerojë fjalëkalimet njëpërdorimëshe për autentifikimin / autorizimin, nëse është i aplikueshëm. Përdoruesi akseson faqen e logimit të internet banking dhe autentifikohet duke vendosur ID-në e Përdoruesit ne fushen “ID e Përdoruesit” dhe duke vendosur fjalëkalimin njëpërdorimësh të gjeneruar nga #withKEY në fushën "OTP".

Autorizimi i veprimeve dhe dhënia e pëlqimit, aty ku kërkohet, bëhet duke vendosur fjalëkalimin njëpërdorimësh të gjeneruar nga #withKEY në fushën përkatëse të internet banking. Përjashtim nga kjo proçedurë bëjnë autorizimet TDS, të cilat autorizohen duke përdorur sistemin e autorizimit të logimit të zgjuar.

Token fizik - nëse klienti ka zgjedhur token fizik, ai mund të logohet në internet banking duke vendosur ID-në e Përdoruesit ne fushën “ID e Përdoruesit” dhe duke vendosur fjalëkalimin njëpërdorimësh të gjeneruar nga tokeni fizik në fushën "OTP".

Autorizimi i veprimeve dhe dhënia e pëlqimit, aty ku kërkohet, bëhet duke vendosur fjalëkalimin njëpërdorimësh të gjeneruar nga tokeni fizik në fushën përkatëse të internet banking. Përjashtim nga kjo proçedurë bëjnë autorizimet TDS.

7. Të drejtat, detyrimet dhe përgjegjësitë e përdoruesit

Të drejtat e Përdoruesit

Me anë të firmës elektronike, Klienti mund të kërkojë shërbime të reja ose modifikojë shërbimet që akseson përmes internet banking ose aplikacionit mobile. Pranimi (konfirmimi) i aplikimit nga Banka përbën firmosje të Marrëveshjes ose modifikim të Marrëveshjes fillestare.

Përmes Shërbimit, Klienti do të jetë në gjendje të aksesojë të gjitha produktet dhe shërbimet që ka me bankën dhe të cilat Banka i ka mundësuar për ti parë, kontraktuar dhe mbyllur përmes këtyre kanaleve.

Përdoruesi është i detyruar:

- të ruajë pajisjet dhe të dhënat për autentifikim dhe autorizim në mënyrë që të parandalojë dëmtimin, shkatërrimin, humbjen, mosdisponueshmërinë, vjedhjen apo keqpërdorimin e tyre
- të mos regjistrojë në letër, në mënyrë elektronike apo në ndonjë mjedis tjetër, e as të mos i bëjë të ditur personave të tretë PIN-in, fjalëkalimin dhe ndonjë të dhënë tjetër që shërben për të aksesuar dhe përdorur Shërbimin
- të përdorë sistemin e autentifikimt dhe autorizimit në mënyrë të tillë që të garantojë fshehtësinë: fjalëkalimi, PIN-i dhe të dhënat e gjeneruara nga sistemi i autenfitikimit / autorizimit nuk duhen shkruar, shpërndarë apo bërë të ditura palëve të treta
- ti paguajë Bankës komisionet përkatëse në përputhje me tarifat bankare, në rast se humbet ose dëmton ose nuk e kthen mbrapsht pas përfundimit të kontratës për përdorimin e shërbimit bankar dixhital, tokenin
- të njoftojë Bankën pa vonesë për humbjen, vjedhjen apo keqpërdorimin e pajisjes së autentifikimit / autorizimit, apo pajisjes celulare në të cilën është shkarkuar aplikacioni ose në rast të përdorimit të paautorizuar të tij, dhe Banka, me marrjen e njoftimit do të bllokojë pajisjen e autentifikimit / autorizimit dhe / ose shërbimet.

Detyrimet e sigurisë të Përdoruesit janë si vijon:

- të aksesojë Shërbimin duke përdorur kompjuterin e duhur (hardware dhe software) dhe pajisje komunikimi të cilat janë në përputhje me konfigurimet e publikuara në faqen zyrtare të Bankës dhe / ose në degët e bankës, dhe të cilat janë instaluar dhe përditësuar në përputhje me të gjitha përditësimet e disponueshme nga prodhuesi: sistem operativ, shfletues i internetit, mbrojtës antivirus dhe firewall
- ti përmbahet të gjitha masave të sigurisë për mbrojtjen dhe përdorimin e kompjuterave, pajisjeve celulare dhe pajisjeve të tjera që janë aktivizuar për të përdorur shërbimin, përfshirë:
  - mbrojtjen e aksesit në kompjuter, celular dhe pajisje të tjera duke përdorur një fjalëkalim konfidencial
  - ruajtjen e fshehtësisë së PIN-it për të parandaluar përdorimin e paautorizuar
  - të marrë parasysh faqet që vizitohen në pajisjet që aksesojnë Shërbimin pasi aksesi në disa faqe interneti përfshin një risk të shtuar për infektimin e kompjuterave, pajisjeve celulare dhe pajisjeve të tjera nga programe dashakeqe
  - përditësimi i rregullt i programit antivirus
  - hyrja në Shërbim vetëm duke përdorur URL-në e duhur.
  - kontrolli periodik i njoftimeve të dërguara nga Banka përmes shërbimit si dhe veprimi në përputhje me këto njoftime
  - informimi i menjëhershëm i Bankës në rast ndryshimi të numrit të telefonit për të garantuar një funksionim të sigurtë të Shërbimit (dërgimi i SMS për autorizimin përmes SMS dhe SMS me kodin e identifikimit, i nevojshëm për aktivizimin e aplikacionit mobile)

8. Detyrimet dhe përgjegjësitë e Bankës

Për çdo hyrje të suksesshme në Shërbim, konsiderohet se autorizimi është bërë nga Përdoruesi. Banka do të konsiderojë veprimet e urdhëruara duke përdorur metodat e mësipërme të identifikimit si të miratuara nga Përdoruesi dhe do të përmbushë udhëzimet e dhëna në lidhje me një shërbim duke përdorur metodat e mësipërme të identifikimit, si një udhëzim të dhënë nga Përdoruesi, dhe marrëveshja në lidhje me shërbimin do të krijohet, ndryshohet ose përfundohet nëpërmjet konfirmimit të udhëzimit nga ana e Bankës. Banka nuk shqyrton të drejtën e përdoruesit për të përdorur ID-në e përdoruesit ose fjalëkalimin, apo rrethanat e përdorimit.
Banka rezervon të drejtën për të modifikuar gamën e shërbimeve që lidhen me shërbimet e ndryshme dixhitale. Klienti mund të gjejë informacion të detajuar mbi gamën e shërbimeve, mënyrën se si ato mund të përdoren, dhe mbi kërkesat teknike, në Manualin përkatës të Përdorimit ose mund të informohet nëpërmjet shërbimit bankar dixhital ose në faqen e internetit të Bankës.

Banka nuk do të jetë përgjegjëse për ndonjë dëm që i shkaktohet Përdoruesit për shkak të:

- mosfunksionimit ose funksionimit jo të duhur të kompjuterave, pajisjeve celulare ose pajisjeve të tjera që nuk janë pronë e Bankës të cilat përdoren për të hyrë në shërbim
- avarisë të sistemit kompjuterik ose sistemit operativ të pajisjeve mobile të përdorura për të hyrë në Shërbim
- përdoruesit ose hyrjes së personave të tjerë të paautorizuar në pajisjen e caktuar dhe / ose aplikacionin e autentifikimit / autorizimit
- forcave madhore si lufta, trazirat, aktiviteti terrorist, fatkeqësi natyrore, epidemi, greva, ndërprerje e furnizimit me energji elektrike, probleme në telekomunikacion dhe rrjete të tjera, gabime në transmetim të rrjeteve të telekomunikacionit, vendime dhe veprime të organeve qeveritare, si dhe gjithë rrethanat e ngjashme, ngjarja e të cilave nuk mund t'i atribuohet Bankës ose që janë jashtë kontrollit të Bankës dhe të cilat kanë penguar përdorimin e Shërbimit dixhital.
- humbjes, dëmtimit ose shkatërrimit të të dhënave dhe pajisjeve të Përdoruesit

9. Komisionet

Me nënshkrimin e Marrëveshjes së Shërbimit, Përdoruesi është i detyruar të paguajë komisionet përkatëse për ekzekutimin e veprimeve përmes Shërbimit si dhe tarifave të tjera të përfshira në Kushtet e Punës së Bankës, për gjatë gjithë kohëzgjatjes se Marrëveshjes.

Nëse Përdoruesi nuk ka fonde të mjaftueshme në dispozicion në llogarinë e caktuar, atëherë Banka ka të drejtë të mbajë tarifat / komisionet nga ndonjë llogari / produkt tjetër që klienti ka me Bankën.

Shuma dhe llojet e tarifave dhe kostove të tjera që mund të lindin gjatë përmbushjes së Marrëveshjes përcaktohen në Kushtet e punës së Bankës.

10. Limitet

Për të përdorur shërbimin bankar dixhital, do të aplikohen limite ditore dhe mujore për transaksionet e pagesave kombëtare, ndërkombëtare dhe ndërkufitare. Informacioni mbi shumat e limiteve ditore dhe mujore është në dispozicion të Përdoruesit në të dy Shërbimet Mobile Banking dhe Internet Banking.

Përdoruesi mund të rrisë/zvogëlojë limitet Brenda vlerës standarte të përcaktuar nga Banka ose duke u paraqitur në degë ose përmes shërbimit dixhital. Limiti ditor / mujor i specifikuar në kërkesën e Përdoruesit, aplikohet menjëherë.

Gjatë përdorimit ditor dhe mujor të shërbimit, pagesat në monedha të huaja konvertohen në equivalentin e monedhës së huaj sipas kursit të blerjes së Bankës.

Banka përcakton se cilat lloje veprimesh nuk ndikojnë në uljen e limitit ditor dhe mujor, përkatësisht:

- Transfertë personale (transfertë ndërmjet llogarive të veta në LEK)
- Veprime me kurs (transferta ndërmjet llogarive të veta në monedhë të ndryshme)
- Udhërpagesë periodike
- Debitime direkte (klienti mund të vendosë limitin që dëshiron gjatë krijimit të debitimin direkt)
- Pagesë karte (ripagim i detyrimit të kartës së kreditit)
- Shitja e depozitave
- Transaksione të reja sic mund të pasurohen hera herës

11. Ekzekutimi i veprimeve

Nëpërmjet Shërbimit Banka i mundëson Përdoruesit kryerjen e pagesave brenda dhe jashtë vendit kur të aktivizohen nga Banka. Urdhrat e pagesave të autorizuara përmes shërbimit ekzekutohen në përputhje me informacionin e publikuar në Kushtet e Punës.

Në varësi të llojit të sistemit të autentifikimit dhe autorizimit të përdorur nga Përdoruesi, aprovimi për të ekzekutuar një transaksion pagese, jepet nga Përdoruesi përmes sistemeve të autentifikimit / autorizimit në përputhje me mënyrat e përshkruara në këtë dokument.

Banka lejon Përdoruesin që nëpërmjet Shërbimit të aktivizojë të ashtuquajturën proçedurë për Transferta të shpejta. Pasi Përdoruesi në mënyrë të pavarur ose nëpërmjet Shërbimit të Internet Banking të ISBA zgjedh dhe autorizon përdorimin e këtij funksionaliteti përmes sistemit të autentifikimit / autorizimit që ai / ajo përdor, kur inicion një pagesë, sistemi nuk do ti kërkojë autorizimin individual të pagesës nga Përdoruesi. Përdoruesi në mënyrë të pavarur, përmes shërbimit dixhital mund ta ç'aktivizojë këtë funksionalitet.

Banka lejon Klientin që përmes shërbimit të përcaktojë të ashtuquajturën Llogari të besuar, për të cilën sistemi nuk do të kërkojë ekzekutimin e proçedurës së autorizimit. Një llogari e besuar mund të jetë çdo llogari drejt së cilës Përdoruesi vendos të iniciojë urdhërpagesat pa iu nënshtruar proçesit të autorizimit. Klienti mund ta ç'aktivizojë këtë funksionalitet nëpërmjet shërbimit dixhital.

Banka i jep mundësinë klientit të aktivizojë përmes shërbimit dixhital, funksionalitetin e pagesës #withPAY.

Banka do ti dërgojë Klientit ekstraktin e llogarise/ve apo produkteve të tjera bankare që Klienti ka me Bankën përmes platformës bankare dixhitale, kurdo që ky opsion do të mundësohet. Mënyrat e tjera alternative të marrjes së ekstrakteve bankare, mund të konfigurohen nga vetë Klienti në shërbimin bankar dixhital.

12. Orari i funksionimit të Shërbimit Dixhital

Sistemet janë në dispozicion 24 orë në ditë me përjashtim të mbylljes periodike dhe periudhave të mirëmbajtjes së sistemit. Banka do të informojë Klientin në kohë mbi periudhat e mirëmbajtjes së sistemit.

Gjatë mirëmbajtjes periodike të shërbimit, përdoruesi nuk do të jetë në gjendje të përdorë Shërbimin pjesërisht ose plotësisht. Shërbimet periodike të mirëmbajtjes kryhen në një kohë kur, sipas vlerësimit të Bankës, frekuenca e përdorimit të Shërbimit është më e ulët.

Kohërat e proçesimit të transaksioneve janë të përcaktuara në Kushtet e Punës së Bankës.

Në rast të problemeve teknike ose keqfunksionimeve, banka do të fillojë punën për korrigjimin e defektit brenda 1 dite pune nga identifikimi i problemit.

13. Ndryshimi, kufizimi ose pezullimi i shërbimit

Banka rezervon të drejtën për të ndryshuar, kufizuar ose pezulluar Shërbimin. Ndryshimi i Shërbimit mund të bëhet posaçërisht, por jo ekskluzivisht, në rast të një përmirësimi ose modernizimi teknologjik në lidhje me ndërfaqen e Shërbimit, ndërkohë pezullimi mund të bëhet posaçërisht, por jo ekskluzivisht, në rast të problemeve teknike ose keqfunksionimeve serioze.

Banka do të njoftojë Klientin permes kanalit ose çfarëdo mënyre që ka në dispozicion, pa përjashtuar njoftimin me shkrim, për sa më sipër. Banka nuk mban përgjegjësi për ndonjë dëm që i shkaktohet Klientit për shkak të këtij ndryshimi ose pezullimi.

Banka rezervon të drejtën të kufizojë Shërbimin për arsye sigurie (kufizime sigurie) në rastet e mëposhtme:

- nëse është në interes të mbrojtjes së klientëve, (i) është e nevojshme për arsye sigurie për shkak të një sulmi ndaj sistemit të Bankës, ose (ii) nëse lind një dyshim për abuzim me Shërbimin;
- nëse, sipas gjykimit të Bankës, ekziston arsye për të dyshuar se abuzimi ose përdorimi i paautorizuar ose mashtrimi ka ndodhur duke përdorur të dhënat që kanë të bëjnë me identitetin e klientëve individualë (ID-ja e përdoruesit, fjalëkalimi, kodi PIN), të cilat mund të ndikojnë një sërë klientësh të cilët Banka nuk mund ti identifikojë paraprakisht dhe në gjykimin e Bankës pezullimi ose kufizimi është i nevojshëm në interes të mbrojtjes së klientëve; ose
- në rast të një sulmi masiv ose selektiv (phishing attack), ose dyshimi për një sulm të tillë.

Banka do të njoftojë klientët për fillimin dhe mbarimin e kufizimit në Shërbimin Elektronik, duke ofruar njëkohësisht një informacion të tillë nëpërmjet Shërbimit dhe duke e paraqitur atë në Degët e Bankës dhe në faqen e internetit. Banka nuk do të jetë përgjegjëse për asnjë dëm të drejtpërdrejtë ose të tërthortë shkaktuar Klientit si rezultat i kufizimit të sigurisë.

14. Dispozita të tjera

Kushtet e Punës zbatohen së bashku me Marrëveshjen për përdorimin e shërbimit bankar dixhital, si dhe Kushtet e Punës të Intesa Sanpaolo Bank Albania. Kushtet e Punës të Intesa Sanpaolo Bank Albania mund ti gjeni në të gjitha degët e Bankës si dhe në faqen zyrtare në web www.intesasanpaolobank.al.

15. Politika e Privatësisë

Intesa Sanpaolo Bank Albania, për të mbrojtur më mirë llogarinë tuaj bankare nga rreziku i mashtrimit dhe ose vjedhja e identitetit, do të analizojë në mënyrë anonime të dhënat që kanë lidhje me karakteristikat tuaja të sjelljes gjatë lundrimit në web apo në aplikacionin bankar në celular. Kjo realizohet përmes një pale të tretë ("Pala e Tretë") e cila, për të luftuar krimin kibernetik, siguron zgjidhje për autentifikimin e sjelljes dhe për zbulimin e programeve të dëmshme, duke përmirësuar kësisoj sigurinë e klientit. Kjo zgjidhje i lejon Bankës të aktivizojë zbulimin e anomalive gjatë sesioneve të online banking me qëllim parandalimin dhe zbulimin e mashtrimeve.

Në mënyrë që të kryhet analiza e të dhënave që lidhen me karakteristikat e sjelljes, Pala e Tretë do të krijojë një profil të pseudoanonimizuar i cili konfirmon që personi që po përdor sesionin e online banking është përdoruesi. Një kombinim i faktorëve të sjelljes, pa u mbështetur në të dhënat personale të identifikueshme (PII), përdoret për të krijuar profilin e pseudoanonimizuarpër për shembull, a) tiparet kognitive si koordinimi sy-dorë, modelet e ndërveprimit me pajisjet; b) faktorët psikologjikë si të qënit përdorues i dorës së majtë apo të djathtë, presioni, dridhja e dorës, përmasa e krahut dhe përdorimi i muskulit si dhe c) faktorët kontekstualë si transaksioni, lundrimi në internet dhe modelet e rrjetit e të pajisjes, këtej e tutje referuar si "të Dhënat"".

Të Dhënat mblidhen dhe përpunohen nga Pala e Tretë me qëllim mbrojtjen e subjektit të të dhënave kundër rreziqeve kibernetike dhe aktivitetit mashtrues, si për shembull vjedhja e identitetit dhe programet e dëmshme.
Zgjidhja do të përdoret në interesin tuaj si Klient, me qëllim që të mos jeni viktimë e mashtrimit ose që dikush tjetër të mos përvetësojë identitetin tuaj.

Të Dhënat tuaja do të mbahen për një periudhë e cila nuk tejkalon periudhën e nevojshme për të përmbushur qëllimin për të cilin ato proçesohen, pa cenuar kushtet e ruajtjes të kërkuara me ligj dhe / ose me qëllim të mbrojtjes së disa të drejtave në gjykatat kompetente.
Në veçanti, të Dhënat e mbledhura nga Pala e Tretë, në mënyrë që të krijohet një profil biometrik unik, do të mbahen nga ky i fundit për gjithë kohëzgjatjen e marrëdhënies së Klientit me Bankën dhe përdorimit të aplikacionit mobile të Bankës dhe faqes së internet banking sipas nevojës për ti siguruar Bankës shërbimin e parandalimit të mashtrimeve.

Për të arritur qëllimin e treguar në Seksionin 1 më sipër, Banka do ti komunikojë të Dhënat tuaja Palës së Tretë në mënyrë të enkriptuar duke përdorur identifikues të maskuar, të cilët garantojnë sigurinë dhe konfidencialitetin. Të Dhënat do të përdoren vetëm për qëllime të parandalimit të mashtrimeve dhe nuk do ti bëhen të ditura ndonjë subjekti tjetër përveç Palës së Tretë.

Me firmosjen e Kushteve të Punës, Klienti autorizon Bankën që të proçesojë të dhënat personale, deri në masën e nevojshme dhe brenda qëllimit të synuar, me Pay&Go dhe me çdo partner të Pay&Go për kryerjen e pagesave të faturave të Klientit përmes ATM-ve të Bankës që gjenden në territorin e Shqipërisë ose përmes shërbimit bankar në celular/internet.