Az OTP Bank Nyrt. Magatartási Kódexe az elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról

Az OTP Bank Nyrt. (a továbbiakban: Bank) a Magyar Nemzeti Bank elektronikus úton megkötött írásbeli szerződésekről, megtett írásbeli jognyilatkozatokról szóló Vezetői körlevelének 2.1.6. pontja alapján tájékoztatja ügyfeleit, hogy jelen Magatartási Kódexben ismertetett elektronikus csatornákat alkalmazza a Bank elektronikus úton - akár személyes megjelenés mellett vagy akár távoli elérhetőségen keresztül - megkötött írásbelinek minősülő szerződések megkötésére, illetve egyoldalú jognyilatkozatok megtételére.
Jelen Magatartási Kódex célja, hogy ügyfeleink megismerhessék az elektronikus úton megkötött írásbelinek minősülő szerződésekhez, megtett jognyilatkozatokhoz alkalmazott informatikai rendszereket, azok alapvető funkcióit, biztonsági megoldásait, illetve a szerződések és nyilatkozatok megkötése és megtétele szempontjából legfontosabb további ismérveit.

Az írásbeli alakhoz kötött jognyilatkozat – a hagyományos papír alapú, hétköznapi értelemben vett írásbeli formán túlmenően – a *2013. évi V. törvény - a Polgári Törvénykönyvről* (Ptk.) vonatkozó rendelkezése alapján akkor felel meg a jogszabályi követelményeknek, ha annak közlésére a jognyilatkozatban foglalt tartalom változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának azonosítására alkalmas formában kerül sor. Jelen Magatartási Kódexben nevesített elektronikus csatornákon megtett jognyilatkozatok és megkötött szerződések teljesítik a Ptk. írásba foglaltnak tekintett nyilatkozatokkal szemben támasztott, a fentiekben részletesen kifejtett hármas konjunktív feltételét.

Az írásban kötött szerződés (akár személyes megjelenés mellett vagy akár távoli elérhetőségen keresztül) egy eredeti vagy hiteles példányát a Bank az ügyfél számára minden esetben átadja vagy – a megfelelő biztonsági intézkedések és jogosultságok mellett – mindenkor hozzáférhetővé teszi.
Az elektronikus úton történő, írásba foglaltnak tekintendő szerződéskötést, vagy jognyilatkozat megtételét megelőzően a Bank ügyfeleit honlapján, az adott szolgáltatásra vonatkozó publikus dokumentumokon keresztül elektronikusan írásban tájékoztatja az alábbiakról:

- a szerződéskötés technikai lépéseiről;
- a megkötendő szerződés jogkövetkezményeiről, jelen vonatkozó magatartási kódex és a szerződés ügyfélpéldányának elérhetőségéről (az átadás vagy hozzáférés módjáról);
- azokról az eszközökről, amelyek az adatok elektronikus rögzítése során felmerülő hibák azonosítását és kijavítását a szerződési jognyilatkozat megtételét megelőzően biztosítják;
- a szerződés nyelvéről, amely a felek eltérő rendelkezése hiányában minden esetben a magyar nyelv;
- az adatkezelésről és a felmerülő jogorvoslati lehetőségekről.

Fogyasztónak minősülő ügyféllel elektronikus úton történő szerződéskötés során a Bank *a távértékesítés keretében kötött pénzügyi ágazati szolgáltatási szerződésekről szóló 2005. évi XXV.* törvény tájékoztatásra vonatkozó előírásait mindenkor betartva jár el.

Az elektronikus úton megkötött írásbelinek minősülő szerződésekhez, megtett jognyilatkozatokhoz alkalmazott elektronikus csatornák

1. KÖZÖS SZABÁLYOK

A jelen Magatartási Kódexben ismertetett valamennyi elektronikus csatorna közös jellemzője, hogy működésük során állandó jelleggel magas fokú informatikai védelmi rendszerekkel biztosított ügyfeleink adatainak védelme. Valamennyi elektronikus csatorna esetében biztonságos környezetben történő hálózati kommunikáció, a jogszabályi környezetnek megfelelő ügyfél-azonosítás, titkosítás, szigorú szabályok szerint megvalósuló jogosultságkezelés, folyamatos tevékenység naplózás, rendszeres ellenőrzések és tesztelések, valamint a szoftveres biztonsági elemek mellett megvalósuló fizikai védelmi intézkedések biztosítják a zavartalan és biztonságos működést.

Valamennyi elektronikus csatorna esetében rendelkezik a Bank üzletmenet-folytonossági tervvel, mely akkor lép életbe, ha valamilyen oknál fogva rendszerleállás lépne fel, vagy rendszerleállításra lenne szükség. Ilyen esetben tartalékmechanizmusok helyettesítik és veszik át az érintett rendszer szerepkörét, továbbá az elektronikus csatorna jellegétől és funkciójától függően tájékoztatjuk ügyfeleinket a Bank honlapján és egyéb kapcsolattartásra szolgáló csatornákon egyaránt a helyreállítás várható időpontjáról és a javítás ideje alatt alkalmazott megoldásokról.

Az ütemezett informatikai karbantartásokról előzetesen tájékoztatjuk ügyfeleinket, valamint igyekszünk azokat úgy időzíteni, hogy lehetőség szerint ezzel egyáltalán ne vagy csak a lehető legkisebb mértékű kellemetlenséget okozzuk. A karbantartások és javítások dokumentáltak, továbbá a karbantartással kapcsolatos feljegyzések, dokumentumok rendszeres felülvizsgálaton esnek át.

2. ALÁÍRÓPAD

A Bank speciális digitális Aláírópad használatával teszi lehetővé ügyfelei számára az ügyintézés során keletkező dokumentumok elolvasását és aláírását. A digitális Aláírópadok minden OTP fiókban megtalálhatók, és az ügyfelek számára egyszerű és biztonságos, a Bank számára pedig fenntartható hitelesítési megoldást jelentenek.

Az auditált rendszer egyedülálló módon egy hagyományos kézi aláírásból állít elő egy rendkívül biztonságos elektronikus aláírást, amely megfelel a legszigorúbb jogszabályi követelményeknek is. Minden elektronikusan aláírt dokumentum hiteles példánya az ügyfél bankszámlájához tartozó OTPdirekt internetbanki felületen érhető el.

Az Aláírópad segítségével a regisztrált ügyfelek a leggyakrabban használt dokumentumtípusokat papírmentesen tölthetik ki, ezáltal környezetbarát és kényelmes módon intézhetik banki ügyeiket. Az Aláírópadon elérhető ügyintézési lehetőségek köre folyamatosan bővül.

2.1. Adatbiztonság

Az egyes hardver és szoftver komponensek együttesen fizikai védelemmel rendelkeznek, a hozzáféréseket beléptető, jogosultságkezelő, tűzfal és egyéb védelmi eszközök védik szoftveresen. Az Aláírópad összes konfigurációs állományának védelme szoftveresen elsősorban az operációs rendszer által biztosított beléptető- és jogosultságkezelő rendszer segítségével történik, melyhez a jogosultságokat a Bank rendszergazdái a szigorú belső banki eljárásoknak megfelelően állítják be, figyelembe véve a kliens- és szerver oldali telepítési és frissítési útmutatókat. Ezen felül a konfigurációs állományok mindazon hardveres és szoftveres védelemben részesülnek, mellyel az ezeket tartalmazó számítógép rendelkezik. Kliens és szerver konfigurációs fájlok kezelését a rendszergazdák a banki jogosultságkezelési eljárásokkal összhangban valósítják meg. A külső fenyegetés ellen a Bank lokális adattitkosítást, adatátvitel-, adat szintű titkosítást, valamint csatorna titkosítást is alkalmaz, kiegészítve az OTP Bank teljes infrastruktúrájára értelmezett, valamennyi védelmi eszközzel, mint a tűzfalak, hálózati monitoring eszközök.

2.2. Az ügyfél-azonosítás szabályai

Az aláíró rendszert és funkcióit ügyfeleink azonosítására nem használja a Bank. Az Aláírópadon végzett dokumentum aláírás előtt mindig megtörténik ügyfeleink azonosítása az eljáró ügyintéző által.

2.3. A rendszerből előálló dokumentumok változtathatatlansága

Az aláíró rendszerben keletkező dokumentumok változtathatatlanságát a rendszer zártsága biztosítja. Az aláírási folyamat lépései biztosítják a dokumentumok hitelességét (a folyamat megfelelő pontjain időbélyegek, szervezeti tanúsítványok és titkosított aláírás beágyazások történnek), mely biztonsági lépéseket követően a dokumentumok a Bank archiváló rendszerében pdf szabvány szerint tárolódnak.

2.4. Adatok tárolása, mentése, visszakereshetősége

Az adatbázis és a naplóállomány mentése az aktuális Mentési, Archiválási és Visszatöltési Rend szerint történik. Az aláíró rendszerben keletkező dokumentumokat maga az aláíró rendszer csak átmeneti ideig tárolja, a dokumentumok hosszú távú tárolását a Bank archiváló rendszere biztosítja.

2.5. Visszaélések elleni védelem

Az aláíró rendszerben a visszaélések elleni védelem a rendszer zártsága és a Bank felhasználó- és jogosultságkezelési rendszere által biztosított. Az Aláírópadon végzett tevékenységek naplózásra kerülnek, a főbb naplóesemények a Bank biztonsági napló rendszerébe automatikusan töltődnek, továbbá meghatározott visszaélés gyanús események észlelése esetén a rendszer automatikus riasztást küld. Az Aláírópad eszköz fizikai védelmét kártyás beléptetőrendszer, riasztó és kamerával megfigyelt helyiségek biztosítják.

2.6. Rendszeres ellenőrzések, tesztelések, auditok

A Bank rendszeres felülvizsgálatoknak, ellenőrzéseknek veti alá a rendszert (biztonsági rendszer dokumentáció, külső auditor által végzett zártsági vizsgálat, terheléses teszt, sérülékenységvizsgálat, üzletmenet folytonossági terv, katasztrófa helyreállítási terv). A rendszeren végzett fejlesztések tesztelése a Bank belső működési szabályzata által biztosított.

Külső auditor által jogszabály szerint végzett zártsági, továbbá jogszabályi megfelelést vizsgáló audit és azok rendszeres felülvizsgálata szintén biztosítja a rendszer biztonságos működését.

2.7. Verzióváltások esetén alkalmazott intézkedések, karbantartás

A verzióváltások illetve ütemezett karbantartások, minden esetben a fiókok nyitvatartási idején kívüli időszakokban, banki verzióváltást támogató rendszer segítségével történnek meg.

3. OTPDIREKT / SMARTBANK

OTPdirekt

Az OTPdirekt a Bank Internetbanki szolgáltatása, melynek segítségével a hét minden napján, a nap 24 órájában az OTPdirekt internetes felületén vagy telefonos szolgáltatás használatával rendelkezhet pénzügyei felett. A szolgáltatás funkcióit, illetve a szolgáltatás használatával kapcsolatos releváns információkat a Bank folyamatosan frissíti és közzéteszi a oldalon.

SmartBank

Az OTP Bank Nyrt. elektronikus bankszolgáltatása, amelynek segítségével az OTPdirekt SmartBank szolgáltatás Igénybevevője az arra alkalmas mobil eszközre letöltött alkalmazáson keresztül – sikeres regisztrációt követően – aktív és lekérdező banki tranzakciókat hajthat végre a regisztrációban érintett, az internetes szolgáltatás számlakörébe bevont számláin. Regisztráció nélkül kizárólag az általános banki információk

elérése lehetséges. A szolgáltatás funkcióit, illetve a szolgáltatás használatával kapcsolatos releváns információkat a Bank folyamatosan frissíti és közzéteszi https://www.otpbank.hu/portal/hu/Appok/SmartBank oldalon.

3.1. Adatbiztonság

Ügyféladatok rögzítése a Bank háttérrendszereiben történik, az OTPdirekt/SmartBank rendszerben létrehozott szerződésekben már csak ügyfélazonosítók szerepelnek. Az egyes a rendszer működéséhez szükséges adatbázisokhoz történő hozzáférés a Bank szigorú belső szabályai alapján, jogosultságkezeléssel védetten történik. A külső fenyegetés ellen a Bank lokális adattitkosítást, adatátvitel-, adat szintű titkosítást, valamint csatorna titkosítást is alkalmaz, kiegészítve az OTP Bank teljes infrastruktúrájára értelmezett, valamennyi védelmi eszközzel, mint a tűzfalak, hálózati monitoring eszközök.

3.2. Az ügyfél-azonosítás szabályai

OTPdirekt

OTPdirekt szerződést bankfiókban, ügyintéző segítségével köthet az ügyfél, így tehát a szerződések adatait ügyintéző rögzíti. A már megkötött OTPdirekt szerződések későbbi – korlátozott – módosítására az ügyfélnek önállóan is van jogosultsága a szolgáltatáson keresztül.

A használat során történő ügyfél azonosítás szabályai megfelelnek a 2019.09.14-én hatályba lépett, (EU) 2015/2366 európai parlamenti és tanácsi irányelvnek az erős ügyfél-hitelesítésre, valamint a közös és biztonságos nyílt kommunikációs standardokra vonatkozó szabályozástechnikai standardok tekintetében történő kiegészítéséről szóló, 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelet (továbbiakban PSD2) szabályozás erős ügyfél-hitelesítésre vonatkozó előírásainak, tehát kétfaktoros azonosításra kötelezett mind a bejelentkezés, mind az alkalmazáson belüli pénzügyi művelet, szerződéskötés, módosítás vagy jognyilatkozat tétel. Az erős ügyfél hitelesítés során a jelszó, mint tudás faktor állandó hitelesítési elem. A második faktor (birtoklás) esetében megengedett az SMS-ben kiküldött egyszer használatos kód, valamint a QR kód használata is.

SmartBank

Az ügyfél azonosítás szabályai megfelelnek a PSD2 szabályozás erős ügyfél-hitelesítésre vonatkozó előírásainak, tehát kétfaktoros azonosításra kötelezett mind a regisztráció, mind az alkalmazáson belüli pénzügyi művelet, szerződéskötés, módosítás vagy jognyilatkozat. Az erős ügyfél hitelesítés során az online PIN, mint tudás alapú faktor tekinthető hitelesítési elemnek, mely kiváltható FaceID vagy ujjlenyomat alapú azonosítással. A második faktor (birtoklás) esetében maga a Smartbank kliens birtoklása azonosítja az ügyfelet, amely mögött

a nemzetközi és hazai hatóságok által is elismert PKI (nyilvános kulcsú infrastruktúra) technológia áll.

3.3. Rendszerből előálló dokumentumok változtathatatlansága

Az OTPdirekt szolgáltatásban keletkező dokumentumok változtathatatlanságát a rendszer külső auditor által is elismert zártsága biztosítja. A Bank OTPdirekt szolgáltatásban keletkező dokumentumokat változatlan formában a *Számlakivonatok, szerződések, egyéb dokumentumok* menüpontban, letölthető pdf formátumban biztosítja ügyfelei rendelkezésére.

3.4. Adatok tárolása, mentése, visszakereshetősége

Kliens oldali adattárolás esetében az adatok tárolásának helye a kliens, tehát az ügyfél eszköze. Bank oldali adattárolás esetében a megfelelő adattárolási, adatkezelési jogalap figyelembevételével, a Bank informatikai háttérrendszerei biztosítják az adatok tárolását. A visszakereshetőség lehetősége adott valamennyi alkalmazott háttérrendszerben, valamint a rendszer által generált naplóállományokban. Az OTPdirekt rendszer kizárólag a működéséhez feltétlenül szükséges adatokat tárolja, tehát a belépéshez szükséges adatokat és az alkalmazás által keletkeztetett naplóállományokat. A naplóállományok tartós tárolásának helye nem maga az alkalmazás, hanem a Bank tartós adattároló megoldásai.

3.5. Visszaélések elleni védelem

A PSD2 szabályozásnak való megfelelést is biztosítva a Bank csalásmegelőző rendszere végzi valamennyi pénzügyi és nem pénzügyi tranzakció vizsgálatát, úgy mint bejelentkezési kísérletek, bankkártyás tranzakciók, átutalás jellegű tranzakciók, szolgáltatáson belüli módosítások valós idejű megfigyelése. További védelemként maga a rendszer is számos informatikai ellenőrzési folyamatban szerepel, melynek célja a gépi beavatkozások, brute force jellegű (a titkosító rendszerekkel szemben alkalmazott támadási módszer) támadások hatékony elhárítása.

Továbbá ügyfeleink úgynevezett Mobil Aláírással biztonságosabban használhatják az OTP internetbanki és mobilalkalmazási szolgáltatásait, mert a szolgáltatásainkba történő bejelentkezéskor, vagy tranzakciók indításakor megerősítést kérünk, mely történhet SMS és/vagy QR kód alapján.

3.6. Rendszeres ellenőrzések, tesztelések, auditok

Kritikus rendszerként évi rendszeres felülvizsgálatra kötelezett a rendszer, amely magában foglalja a teljes Biztonsági Rendszer Dokumentáció ismételt engedélyezését, a külső auditor által végzett zártsági vizsgálatot, a kötelező terheléses tesztet és sérülékenység vizsgálatot

egyaránt. A rendszeren végzett fejlesztések tesztelése a Bank belső működési szabályzata által biztosított.

3.7. Verzióváltások esetén alkalmazott intézkedések, karbantartás

A technikai feltételek változásáról a verzióváltással egyidőben tájékoztatjuk ügyfeleinket a vonatkozó hirdetményekben. A karbantartások és javítások ütemezettek, dokumentáltak, továbbá a karbantartással kapcsolatos feljegyzések, dokumentumok rendszeres felülvizsgálaton esnek át. Az ütemezett karbantartásokról előzetesen tájékoztatjuk ügyfeleinket, valamint igyekszünk azokat úgy időzíteni, hogy lehetőség szerint ezzel a legkisebb kellemetlenséget okozzuk ügyfeleinknek.

4. ÚJ INTERNETBANK/MOBILBANK

Az új Internetbank és Mobilbank az OTP Bank Internetbanki és mobilalkalmazási szolgáltatása, amely a Digitális Szolgáltatásokra vonatkozó szerződés megkötése esetén az OTP Bank ügyfelei számára biztosít a kor követelményeinek megfelelő, innovatív elektronikus bankolási megoldást. Az új Internetbank és Mobilbank szolgáltatás, valamint a Digitális Szolgáltatások Szerződés feltétele az ügyfél korábbi, és a regisztráció időpontjában élő, OTPdirekt szolgáltatásra vonatkozó szerződéses jogviszonyának megléte. Az új Internetbank és Mobilbank szolgáltatás folyamatosan bővülő funkcionalitással kerül bevezetésre, az aktuálisan elérhető funkciókról, illetve a bevezetésre kerülő szolgáltatásokról az OTP Bank weboldalán, illetve az ügyfél kapcsolattartásra fenntartott elérhetőségein ad tájékoztatás a Bank.

4.1. Adatbiztonság

Új Internet Bank:

Az alkalmazás kliens oldalon nem tárol olyan adatot, amely felhasználható lenne, például számlaszám, kártya-adatok stb. A hálózati kommunikáció biztonságos csatornán keresztül történik, valamint az eszköz megfelelő azonosítása érdekében a Bank a készülék meghatározott paraméterei alapján egyedi készülék azonosítót képezhet, melyet később csalás megelőzési céllal felhasználhat.

Mobilbank:

A kliens oldali adattárolás a kor információbiztonsági követelményeinek megfelelő AES (Advanced Encryption Standard) titkosítással védve történik.

4.2. Az ügyfél-azonosítás szabályai

Az ügyfél azonosítás szabályai megfelelnek a PSD2 szabályozás erős ügyfél-hitelesítésre vonatkozó előírásainak, tehát kétfaktoros azonosításra kötelezett mind a regisztráció, mind az alkalmazáson belüli pénzügyi művelet, szerződéskötés, módosítás vagy jognyilatkozat tétel. Az erős ügyfél hitelesítés során a jelszó, mint tudás faktor állandó hitelesítési elem. A második faktor (birtoklás) esetében megengedett az ujjlenyomat/FaceId alapú azonosítás, a Push üzenet, az SMS-ben kiküldött egyszer használatos kód, valamint a QR kód használata is. A szerződés megkötésének feltétele, egy e-mail validációval megerősített e-mail cím és egy 8-25 karakter hosszúságú jelszó megadása, valamint az OTP Direkt azonosítókkal történő megerősítés. Bejelentkezés során az azonosításhoz szükséges adatok megadása után a szerver ellenőrzi az adatok helyességét, majd egy olyan rövid lejáratú ún. tokent biztosít, amely a munkamenet végéig hitelesíti a felhasználót.

4.3. Rendszerből előálló dokumentumok változtathatatlansága

A Digitális Szolgáltatásra történő regisztráció, valamint a szolgáltatás részét képező InternetBank és Mobilbank esetében a Bank hitelesen bizonyítja a szerződéses dokumentum ügyfél és Bank oldali elfogadásának tényét, valamint változatlan formában, bármikor visszaidézhető módon tárolja a dokumentumot archívumában. A dokumentum archívum az Internet Bank „Dokumentumaim" menüpontjában érhető el az ügyfelek számára. Az archívumban tárolt dokumentum esetén a rendszer bizonyított zártságán túl, mindkét fél aláírása biztosítja a szerződés érvényességét. A Bank oldaláról az OTP Bank elektronikus aláírása, valamint időbélyege, míg az ügyfél oldaláról a szerződésen feltüntetett ún. hash kód bizonyítja a dokumentum mindkét fél általi elfogadását. Az ügyfél oldali aláírásnak tekintett ún. hash kód egy olyan szám és betűsorozat, amelyet a Bank képez a szerződéskötés pillanatában, az ügyfél által végzett tevékenységekre vonatkozó hiteles rendszernapló állományokból. Szerződéssel kapcsolatos panasz esetén a Bank az ügyfél hitelesítésre, dokumentumok elfogadására és megerősítésre vonatkozó napló állományokból bármikor képes ismét előállítani a szerződésen szereplő szám és betűsorozatot, ezzel bizonyítva a szerződés körülményeit, és a dokumentum valósságát.

4.4. Adatok tárolása, mentése, visszakereshetősége

Kliens oldali adattárolás esetében az adatok tárolásának helye a kliens, tehát az ügyfél eszköze. Bank oldali adattárolás esetében a megfelelő adattárolási, adatkezelési jogalap figyelembevételével, a Bank informatikai háttérrendszerei biztosítják az adatok tárolását. A visszakereshetőség lehetősége adott valamennyi alkalmazott háttérrendszerben, valamint a rendszer által generált naplóállományokban. A rendszerek kizárólag a működéséhez feltétlenül szükséges adatokat tárolják el, tehát a belépéshez szükséges adatokat és az alkalmazás által keletkeztetett naplóállományokat. A naplóállományok tartós tárolásának helye nem maga az adott alkalmazás, hanem a Bank tartós adattároló megoldásai.

4.5. Visszaélések elleni védelem

A PSD2 szabályozás erős ügyfél-hitelesítésre vonatkozó előírásainak való megfelelést is biztosítva a Bank csalásmegelőző rendszere végzi valamennyi pénzügyi és nem pénzügyi tranzakció vizsgálatát, úgy, mint bejelentkezési kísérletek, bankkártyás tranzakciók, átutalás jellegű tranzakciók, szolgáltatáson belüli módosítások valós idejű megfigyelése. További védelemként maga a rendszer is számos informatikai ellenőrzési folyamatban szerepel, melynek célja a gépi beavatkozások, például az ún. brute force jellegű (a titkosító rendszerekkel szemben alkalmazott támadási módszer) támadások hatékony elhárítása.

4.6. Rendszeres ellenőrzések, tesztelések, auditok

Kritikus rendszerként évi rendszeres felülvizsgálatra kötelezett a rendszer, amely magában foglalja a teljes Biztonsági Rendszer Dokumentáció ismételt engedélyezését, a külső auditor által végzett zártsági vizsgálatot és a kötelező terheléses tesztet és sérülékenység vizsgálatot egyaránt. A rendszeren végzett fejlesztések tesztelése a Bank belső működési szabályzata által biztosított.

4.7. Verzióváltások esetén alkalmazott intézkedések, karbantartás

A technikai feltételek változásáról a verzióváltással egyidőben tájékoztatjuk ügyfeleinket a vonatkozó hirdetményekben. A karbantartások és javítások ütemezettek, dokumentáltak, továbbá a karbantartással kapcsolatos feljegyzések, dokumentumok rendszeres felülvizsgálaton esnek át. Az ütemezett karbantartásokról előzetesen tájékoztatjuk ügyfeleinket, valamint igyekszünk azokat úgy időzíteni, hogy lehetőség szerint ezzel a legkisebb kellemetlenséget okozzuk ügyfeleinknek.

A Bank egyik elsőszámú célkitűzése a folyamatos üzemeltetés, maga a rendszer felépítése garantálja a változásokra történő gyors reakciót. Ezen gyors reakció részeként a Bank törekszik az úgynevezett Hotfix alapú hibajavításra, melynek lényege, hogy az üzletmenet folytonosság érdekében a rendszer az esetek döntő többségében leállítás nélkül, ügyfeleink számára kellemetlenség nélkül legyen karbantartható.

5. ELECTRA

Az OTP Direkt Electra Terminál szolgáltatás igénybevételével ügyfeleink saját számítógépükön juthatnak hozzá a legfrissebb banki információkhoz és továbbíthatják fizetési megbízásaikat üzleti partnereiknek. A telepített Electra kliens segítségével kötegelt tranzakciók feladása is lehetséges, offline módon akár banki nyitvatartási időn kívül is a 7 minden napján 24 órában.

5.1. Adatbiztonság

Az Electra szerver komponenseinek, illetve adatainak védelmi alapja a UNIX jogosultságrendszere. Ez biztosítja, hogy illetéktelen felhasználók ne tudják a szerver működését befolyásolni, ne férjenek hozzá a szerveren tárolt adatokhoz, illetve hogy ne legyenek képesek módosítást végezni az Electra szerveren. Az ügyféladat nyilvántartás titkosítva kerül nyilvántartásra, ahogy a telepített kliens oldalon a tárolt adatok és programkomponensek titkosítva szerepelnek.

5.2. Az ügyfél-azonosítás szabályai

A szolgáltatás használatához ügyfélpéldány azonosító szükséges, melynek igénylése csak bankfiókban lehetséges. A telepített alkalmazásba történő belépéshez első alkalommal a szintén a bankfiókban átadott Electra PIN szükséges, melyet az első bejelentkezés során meg kell változtatnia az ügyfélnek. Ezek után a belépéshez és a megbízások aláírásához jelszó vagy a Bank ViCA alkalmazásával történő jóváhagyás szükséges.

5.3. Rendszerből előálló dokumentumok változtathatatlansága

A 5.1. pontban is ismertetettek szerint utólagos módosításra nincs lehetőség.

5.4. Adatok tárolása, mentése, visszakereshetősége

Az adatok tárolása és mentése az OTPdirect Electra szolgáltatás esetén mind a Bank oldalán az Electra szerveren keresztül, mind az ügyfél oldalán a telepített Electra kliensben megtörténik. A telepített kliens esetén 90 napra visszamenőleg kérhető le tranzakciós adat, amely a lekérdezés után tartós tárolásra kerül a kliensben.

5.5. Visszaélések elleni védelem

A rendszer telepítéséhez programpéldány azonosító szükséges, míg a belépéshez/jóváhagyáshoz jelszó vagy ViCA alkalmazás (elektronikus chipkártya) szükséges. További biztonsági intézkedésként Banki oldalon az ügyfél kérésére lehetséges többes aláírási jog beállítása, így a tranzakció jóváhagyásával járó felelősség a vállalkozás által felhatalmazott több felhasználó között megosztható.

A rendszerben végrehajtott tranzakciók hagyományos utalásként a Bank csalás megelőző rendszere által ellenőrzöttek.

5.6. Rendszeres ellenőrzések, tesztelések, auditok

Az Electra szerver és az azt kiszolgáló Banki rendszerek évenkénti felülvizsgálatra kötelezettek, amely tartalmaz minden olyan terhelésre, sérülékenységre és zártságra vonatkozó vizsgálatot, amely törvényhozói oldalról elvárt.

Az ellenőrzések támogatása érdekében mind szerver oldalon, mind kliens oldalon részletes naplózásra kerülnek a tranzakciók, illetve a felhasználói tevékenységek.

5.7. Verzióváltások esetén alkalmazott intézkedések, karbantartás

Az ütemezetten végzett verzióváltásokról, karbantartásokról felugró tájékoztató üzenetekben, illetve a verzióváltás típusától függően úgynevezett faliújság (letölthető PDF levél) üzenetben értesítjük ügyfeleinket.

6. KÖZVETLEN ÉS KÖZVETETT ELEKTRONIKUS ÜGYFÉL-ÁTVILÁGÍTÁSON ALAPULÓ ONLINE SZERZŐDÉSKÖTÉS

Az OTP Bank VideóBank szolgáltatásán keresztüli, **közvetlen elektronikus ügyfél-átvilágítással (továbbiakban VideóBank)**, igényelhető termékek és szolgáltatások: lakossági forint fizetési számla, OTPdirekt szolgáltatás, áruvásárlási és szolgáltatási gyorskölcsön, valamint áruvásárlási és szolgáltatási gyorskölcsön közvetítő partnereknél igénybe vehető hitelkártya. A videóhívás mindössze 15 percet vesz igénybe, mely elindítható számítógépünkről, okostelefonunkról vagy tabletünkről. A szolgáltatás igénybevételéhez mindössze internetkapcsolatra és egy kamerával rendelkező eszközre (asztali számítógép, notebook, okostelefon, táblagép) van szükség, amely megfelel a technikai feltételeknek. A videóhívás-alapú azonosítás elérhető Windows, macOS, iOS és Android operációs rendszereken egyaránt.

Az OTP Bank SmartBank szolgáltatásán keresztüli **közvetett elektronikus ügyfél-átvilágítással (továbbiakban: nem valós idejű ügyfél-átvilágítás)** alig pár perc alatt lehet OTPdirekt szolgáltatással kiegészített új lakossági fizetési számlanyitást kezdeményezni. A szolgáltatás igénybevételéhez mindössze egy, a SmartBank alkalmazás futtatására alkalmas, NFC funkcióval rendelkező okostelefonra és új típusú (chipet tartalmazó) személyi igazolványra vagy biometrikus (chipet tartalmazó) útlevélre van szükség.

Mind a VideóBank, mind a nem valós idejű ügyfél-átvilágítás után a következő banki munkanap végéig feldolgozzuk az igényléseket.

A VideóBankon keresztül történő azonosítás minden hétköznap reggel 8 és este 20 óra között, valamint hétvégén reggel 10 óra és délután 18 óra között érhető el. A nem valós idejű ügyfél-átvilágítás jellegénél fogva a nap 24 órájában, a hét minden napján elérhető. A törvényi

rendelkezések alapján az azonosítás eredményéről 2 munkanapon belül a Bank köteles választ adni.

A VideóBankon és nem valós idejű ügyfél-átvilágításon keresztül elérhető szolgáltatások körét folyamatosan bővítjük, a szolgáltatások körét az aktuális honlapi hirdetmények tartalmazzák.

6.1. Adatbiztonság

A vonatkozó 26/2020 (VIII.25.) MNB rendeletnek megfelelő auditált folyamat, mely a Bank belső szabályozásainak megfelelő zárt rendszerben működik. A Bank vonatkozó honlap oldalán megadott adatok és maga a videó folyam is titkosított csatornán kerül továbbításra (https, TLS).

6.2. Az ügyfél-átvilágítás szabályai

A vonatkozó 26/2020 (VIII.25.) MNB rendeletnek megfelelően a videóhívás során történik az ügyfél azonosítása (közvetlen elektronikus) az ügyfél saját személyazonosító igazolványának, útlevelének vagy vezetői engedélyének és lakcímkártyájának bemutatásával. A 26/2020. (VIII. 25.) MNB rendelet által biztosított lehetőségekkel élve, az OTP Bank lehetővé teszi a SmartBank alkalmazáson keresztüli ún, „selfie" alapú ügyfél-azonosítást, melyben a kor követelményeinek megfelelő módon a SmartBank alkalmazás segítségével történik meg az okmányok beolvasása, a készülék által rögzített arckép összehasonlítása, valamint az ilyen módon (közvetlen elektronikus) azonosított személyek szerződéskötése.

6.3. Rendszerből előálló dokumentumok változtathatatlansága

A keletkező szerződéses dokumentumokat a Bank két digitális aláírással, szervezeti pecséttel és időbélyeggel látja el, továbbá az ügyfél szerződéskötési szándékát alátámasztó videó felvétel vagy „selfie" videó változtathatatlanságát is digitális aláírással biztosítjuk.

6.4. Adatok tárolása, mentése, visszakereshetősége

Rendszeresen mentett, zárt adatbázisban kerülnek eltárolásra az adatok, melyekhez csak a szigorú belső szabályzatok szerinti nyilvántartott jogosultsággal rendelkező személyek férhetnek hozzá. Minden hozzáférésről bejegyzés készül az alkalmazás naplóállományába.

6.5. Visszaélések elleni védelem

A vonatkozó 26/2020 (VIII.25.) MNB rendeletnek megfelelő kártyás beléptető rendszerrel, riasztóval és kamerával védett helyiségben történik a (videós) hívásfogadás, ahol csak az arra jogosult személyek tartózkodhatnak. A nem valós idejű ügyfél-átvilágítás esetében a Bank

zárt rendszerei, illetve külső fél által auditált azonosítási folyamata garantálja a visszaélések elleni hatékony védelmet.

6.6. Rendszeres ellenőrzések, tesztelések, auditok

A rendszer ellenőrzése és tesztelése a Bank belső szabályzatai alapján folyamatos.
A rendszerek auditálása független külső szervezet által, a vonatkozó 26/2020 (VIII.25.) MNB rendeletnek megfelelően az éles indulás előtt megtörtént.

6.7. Verzióváltások esetén alkalmazott intézkedések, karbantartás

A technikai feltételek változásáról a verzióváltással egyidőben tájékoztatjuk ügyfeleinket a vonatkozó hirdetményekben. Az ütemezett karbantartások, illetve verzióváltások a VideóBank nyitvatartási idején kívüli időszakokban történnek, a nem valós idejű ügyfél-átvilágítási folyamat esetében pedig lehetőség szerint üzemszünet nélkül.

7. TELEKOM HITELKÁRTYA

A Telekom Hitelkártya az OTP Bank Nyrt. és a Magyar Telekom Nyrt. által közösen létrehozott hitelkártya program keretében kerül kibocsátásra. A hitelkártya programhoz kapcsolódó Telekom Hitelkártya terméket kizárólag az OTP Bank és a Magyar Telekom közös ügyfelei igényelhetik a Magyar Telekom értékesítési pontjain, Telekom szolgáltatási szerződéshez kapcsolódó készülékvásárlás keretében.

A Telekom Hitelkártya igénylési folyamata teljesen integráltan került kialakításra a Magyar Telekom és az OTP Bank rendszereiben és kizárólag papírmentesen igényelhető. A folyamatban előálló dokumentumok megtekintése és aláírása is a Magyar Telekom boltjaiban működő MobilSign elektronikus aláíró rendszeren lehetséges.

A Telekom Hitelkártya önállóan az OTP Bank fiókhálózatában nem igényelhető.

7.1. Adatbiztonság

Az egyes hardver és szoftver komponensek együttesen fizikai védelemmel rendelkeznek, a hozzáféréseket beléptető, jogosultságkezelő, tűzfal és egyéb védelmi eszközök védik szoftveresen. A külső fenyegetés ellen a Bank lokális adattitkosítást, adatátvitel-, adat szintű titkosítást, valamint csatorna titkosítást is alkalmaz, kiegészítve az OTP Bank teljes infrastruktúrájára értelmezett, valamennyi védelmi eszközzel, mint a tűzfalak, hálózati monitoring eszközök. Az OTP Bank és a Magyar Telekom közötti adatkapcsolat titkosított.

7.2. Az ügyfél-átvilágítás szabályai

Minden ügyfelet a Magyar Telekom Nyrt. ügyintézője személyesen azonosít be a szükséges személyazonosításra szolgáló okmányok alapján. A Magyar Telekom a hitelkártya igénylési folyamatban az OTP Bank függő ügynökeként jár el. Az ügyfél OTP Bank általi beazonosítása a természetes azonosító adatok titkosított adatkapcsolaton keresztüli átadását követően történik.

7.3 Rendszerből előálló dokumentumok változtathatatlansága

Az aláíró rendszerben keletkező dokumentumok változtathatatlanságát a rendszer zártsága biztosítja. Az aláírási folyamat lépései biztosítják a dokumentumok hitelességét (a folyamat megfelelő pontjain időbélyegek, szervezeti tanúsítványok és titkosított aláírás beágyazások történnek), mely biztonsági lépéseket követően a dokumentumok a Bank zárt és auditált archiváló rendszerében tárolódnak.

7.4 Adatok tárolása, mentése, visszakereshetősége

Rendszeresen mentett, zárt adatbázisban kerülnek eltárolásra az adatok, melyekhez csak a szigorú belső szabályzatok szerinti nyilvántartott jogosultsággal rendelkező személyek férhetnek hozzá. A rendszerek kizárólag a működéséhez feltétlenül szükséges adatokat tárolják.

7.5 Visszaélések elleni védelem

A Telekom Hitelkártya igénylési folyamatot kiszolgáló OTP Bank által működtetett rendszerekben a visszaélések elleni védelem a rendszer zártsága és a Bank felhasználó- és jogosultságkezelési rendszere által biztosított. Az egyes rendszerekben végzett tevékenységek naplózásra kerülnek, a főbb naplóesemények a Bank biztonsági napló rendszerébe automatikusan töltődnek és elemzésre kerülnek. A rendszer eszközök fizikai védelmét kártyás beléptetőrendszer, riasztó és kamerával megfigyelt helyiségek biztosítják.

7.6 Rendszeres ellenőrzések, tesztelések, auditok

A Telekom Hitelkártya igénylési folyamatot kiszolgáló OTP Bank által biztosított rendszerek rendszeres felülvizsgálatra kötelezettek, amely magában foglalja a teljes biztonsági dokumentáció és biztonsági tesztelések évenkénti frissítését is. A rendszeren végzett fejlesztések tesztelése a Bank belső működési szabályzata által biztosított. A Telekom Hitelkártya folyamatot kiszolgáló OTP Bank által üzemeltetett rendszerek esetében a tervezett új kódok élesítését megelőzően kötelező annak teljeskörű tesztelése a mindenkori teljes funkcionalitás tekintetében.

7.7 Verzióváltások esetén alkalmazott intézkedések, karbantartás

A Telekom Hitelkártya folyamatot kiszolgáló OTP Bank által üzemeltetett rendszerek esetében ütemezetten történnek verzióváltások, minden esetben az értékesítési időszakon kívüli időpontban. A verzióváltásokat megelőzően, mind az új mind pedig a meglévő funkcionalitás teljes körűen tesztelésre kerül. A tesztek tartalma és eredménye pontosan dokumentált. A verzióváltás minden esetben csak sikeres tesztelést követően történhet meg.