K&H Bank Zrt.

1095 Budapest, Lechner Ödön fasor 9.
telefon: (06 1) 328 9000
fax: (06 1) 328 9696
Budapest 1851
www.kh.hu • bank@kh.hu

A K&H Bank Zrt.

Bizalmi Szolgáltatási Szabályzata elektronikus aláírás elhelyezéséhez

KH-BSZ-NMEA

Hatálybalépés dátuma: 2019. november 5.

Dokumentum verzió: v6

A módosulások sárga színnel kerülnek megjelenítésre.

Változáskövetés

Verzió	Dátum	A változás leírása	Készítette	Ellenőrizte	Jóváhagyta
v1	2018.08.24.	eredeti v1 változat	László István Somogyi Tamás Mezősi Attila Pávlicz György dr. Horváth Anna	László István Somogyi Tamás Mezősi Attila Pávlicz György dr. Horváth Anna	László István Somogyi Tamás Mezősi Attila Pávlicz György dr. Horváth Anna
v2	2018.09. 25.	módosítás az NMHH észrevételei alapján	dr. Horváth Anna	László István Mezősi Attila dr. Horváth Anna	László István Mezősi Attila dr. Horváth Anna
v3	2018.11. 13.	módosítás az NMHH észrevételei alapján	dr. Horváth Anna	László István Mezősi Attila dr. Horváth Anna	László István Mezősi Attila dr. Horváth Anna
v4	2018.11. 21.	pontosítás a nyújtott szolgáltatás tekintetében	dr. Horváth Anna	dr. Kosdi-Kovács Zoltán	dr. Kosdi-Kovács Zoltán
v5	2018.11. 23.	pontosítás a datagram tartalma tekintetében	dr. Horváth Anna	dr. Kosdi-Kovács Zoltán	dr. Kosdi-Kovács Zoltán
v6	2019.10.18.	Szolgáltató aláírói tanúsítványcseréjével kapcsolatos módosítás átvezetése	dr. Horváth Anna	dr. Kosdi-Kovács Zoltán	dr. Kosdi-Kovács Zoltán

Tartalomjegyzék

1. Bevezetés

1.1 Áttekintés

Jelen dokumentum a K&H Bank Zrt. (továbbiakban: „**Szolgáltató**”) Bizalmi Szolgáltatási Szabályzata (a továbbiakban: „Szolgáltatási Szabályzat” vagy „Szabályzat”), amely a Szolgáltatónak az eIDAS 3. cikk 16. a) pontja szerinti következő nem minősített bizalmi szolgáltatására vonatkozik: **elektronikus aláírás elhelyezése** (a továbbiakban hivatkozva mint a „**Szolgáltatás**”). A jelen Szabályzat szerinti elektronikus aláírás az eIDAS 26. cikkében meghatározott fokozott biztonságú elektronikus aláírás.

A K&H Bank Zrt. bizonyos ügyletek tekintetében lehetővé teszi az ügyfelei számára a szerződéskötés online felületen történő kezdeményezését, és a vonatkozó szerződések online megkötését.

Az ügyfelek a Szolgáltató rendszerébe integrált, speciálisan erre a célra kialakított informatikai szolgáltatás igénybe vételével köthetik meg a szerződéseket a jelen Szabályzatban meghatározott módon.

Felhívjuk a figyelmet arra, hogy a Szolgáltató által nyújtott pénzügyi szolgáltatások felügyelete nem tartozik a Nemzeti Média és Hírközlési Hatóság hatáskörébe, azok felügyelete tekintetében a Magyar Nemzeti Bank rendelkezik hatáskörrel.

1.2 Dokumentum neve és azonosítása

Jelen Szolgáltatási Szabályzat teljes neve: **K&H Bank Zrt. Bizalmi Szolgáltatási Szabályzata elektronikus aláírás elhelyezéséhez.**

A Szolgáltatási Szabályzat objektum azonosítója és verziószáma a címlapon található.

A Szolgáltatási Szabályzat hatályba lépését és hatályának megszűnését a 9.2. fejezet tartalmazza.

Jelen Szabályzat eleget tesz az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (továbbiakban: E-ügyintézési tv.), a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU Rendeletben, a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről szóló 24/2016. (VI.30.) BM rendeletben foglaltaknak, és egyéb jogszabályok előírásainak, valamint megfelel a bizalmi szolgáltatások általános szabályait meghatározó „ETSI EN 319 401 v2.2.1” szabványnak.

1.3 Tanúsítványok alkalmazhatósága

A Szolgáltató az ügyféllel való kapcsolata során nem bocsát ki tanúsítványokat az általa nyújtott bizalmi Szolgáltatás nyújtása céljából. A jelen Szabályzatban hivatkozott fokozott biztonságú elektronikus aláírást az ügyfél kizárólag a Szolgáltatóval történő online szerződéskötés során használja fel.

A Szolgáltató a szerződéskötési folyamat során, az általa történő aláíráshoz, minősített elektronikus bélyegző tanúsítványt használ, amely biztosítja, hogy a Szolgáltató aláírása a későbbiekben ne legyen módosítható. Ez a minősített elektronikus bélyegző tanúsítvány a 6.2 és a 6.3.4 fejezetekben foglaltak szerint kerül felhasználásra a Szolgáltató által. A Szolgáltató által használt, minősített elektronikus bélyegző tanúsítványt a MicroSec Zrt. tanúsítja, és az ottani személyes regisztráció alkalmával került kibocsátásra. Ez a tanúsítvány a Szolgáltató, mint jogi személy részére lett kibocsátva. A MicroSec Zrt. időbélyeg-szolgáltatóként is működik, és minősített időbélyegeket biztosít az ügyféllel való kapcsolat során létrejött dokumentumokhoz. Ez lehetővé teszi annak igazolását, hogy egy adott időpontban minden szükséges dokumentum rendelkezésre állt.

1.4 Szabályzat adminisztráció

1.4.1 Szabályzat karbantartása

A Szolgáltató jelen Szolgáltatási Szabályzat karbantartását a belső szabályzatai szerint vizsgálja felül.

1.4.2 Szolgáltató

cégnév:	K&H Bank Zrt.
cégjegyzékszám:	01-10-041043
székhely:	1095 Budapest, Lechner Ödön fasor 9.
telefon:	(06 1) 328 9000
fax:	(06 1) 328 9696
internetes cím:	www.kh.hu • bank@kh.hu https://www.kh.hu/bizalmi-szolgaltatas
adatvédelem	https://www.kh.hu/adatvedelem

A Szolgáltatót a bizalmi szolgáltatási ügyfelei az alábbi elérhetőségeken érhetik el:

személyesen	bankfiókokban - a bankfiókok mindenkori listája az alábbi linken érhető el: https://www.kh.hu/terkepes-kereso
telefonon	(06 1/20/30/70) 335 3355-ös telefonszámon
faxon	(06 1) 328 9696
postai úton	Budapest Pf. 1851
elektronikus úton	bank@kh.hu

1.4.3 Szolgáltatási Szabályzat felülvizsgálata

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend, illetve a Szolgáltatási Szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek alapján megfelelően módosítja azokat.

1.4.4 Szolgáltatási Szabályzat jóváhagyása

A Szolgáltatási Szabályzat felülvizsgálata, és az elvégzett módosítások jóváhagyása a Szolgáltató belső eljárási szabályai szerint történik.

A jóváhagyás előtt a Szolgáltató megvizsgálja a Szolgáltatási Szabályzat bizalmi szolgáltatási rendnek való megfelelését.

A Szolgáltatási Szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

A hatályba lépés napját a dokumentum címlapja tartalmazza.

A Szolgáltatási Szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és közzétételre Szolgáltató internetes honlapján.
Az új verzió kötelező érvényű valamennyi bizalmi szolgáltatási ügyfélre.

1.5 Bizalmi szolgáltatás és felügyelete

A Szolgáltató az alábbi bizalmi szolgáltatást nyújthatja a bizalmi szolgáltatási ügyfelei (továbbiakban: ügyfél) részére, jelen Szabályzat keretein belül:
Az eIDAS rendelet 3. cikk 16. a) pontja szerinti elektronikus aláírás elhelyezése.

A Szolgáltató által elhelyezett elektronikus aláírás fokozott biztonságú elektronikus aláírásnak minősül, amelynek az eIDAS 26. cikke alapján az alábbi követelményeknek kell megfelelnie:
a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Az eIDAS 25. cikke alapján az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

A Szolgáltató felügyeleti szerve a Nemzeti Média- és Hírközlési Hatóság (továbbiakban: „Bizalmi Felügyelet”).

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott Szolgáltatás felügyeletét, ellenőrzi a Szolgáltatás jogszabályi megfelelőségét. Többek között, figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a bizalmi szolgáltatók által a szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket, továbbá jogerős és végrehajtható határozatában elrendelheti a bizalmi szolgáltatások keretében kibocsátott tanúsítványok felfüggesztését vagy visszavonását. Felhívjuk a figyelmet arra, hogy a Szolgáltató által nyújtott pénzügyi szolgáltatások felügyelete nem tartozik a Bizalmi felügyelet hatáskörébe, azok felügyelete tekintetében a Magyar Nemzeti Bank rendelkezik hatáskörrel.

A Szolgáltató a Szolgáltatást 2018.08.24-én jelentette be a Bizalmi felügyeletnek, mint nem minősített bizalmi szolgáltató.

A Bizalmi felügyelet nyilvántartásainak elérhetősége: http://webpub-ext.nmhh.hu/esign2016/

1.6 Rövidítések, definíciók hivatkozások

Jelen Szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásra vonatkozó jogszabályokban (1.6.2. pont) szereplő meghatározásokkal.

1.6.1 Rövidítések, definíciók

Fogalom	Leírás
Aláírt DOC1	DOC 1, amelyet a Szolgáltató a saját minősített elektronikus aláírásával valamint időbélyegzővel látott el (végleges ajánlat)
Aláírt DOC2	DOC2, amelyet a Szolgáltató a saját minősített elektronikus aláírásával valamint időbélyegzővel látott el
ASiC	(Associated Signature Containers), az elektronikus aláírás és az aláírt tartalmak összekapcsolására létrehozott szabványos fájlformátum
datagram	személyadatokat és más információkat tartalmazó adatblokk
datagram 1	az online felületen történő szerződéskötési folyamat során képzett datagram, amely a következőket tartalmazza: személynév; születési idő; lakcím; okmányszám; telefonszám; e-mail cím; Email kód; SMS kód; IP cím; időbélyeg valamint az érintett szerződésre vonatkozó szerződésszám, hitelösszeg, lejárat és a THM
datagram 2	az online felületen történő szerződéskötési folyamat során képzett datagram, amely a datagram 1-ben szereplő adatokat továbbá a MicroTRX kódot tartalmazza
DOC1	a Szolgáltató által az egyedi ügylet során elkészített (egyediesített) és véglegesített szerződéstervezet
DOC2	az aláírási folyamat elindítását követően a DOC 1 adatai alapján automatikusan képzett új dokumentum, amely tartalmát tekintve mindenben megegyezik a DOC1-gyel, kivéve, hogy a létrehozásakor már azonnal és automatikusan tartalmazza a MicroTRX kódot is.
DOC3	a szerződés mellékletét képező dokumentum, amely a HSH2-t tartalmazza
elektronikus aláírás létrehozásához használt adat	olyan egyedi adat, amelyet az aláíró elektronikus aláírás létrehozásához használ. A jelen Szabályzat vonatkozásában a MicroTRX kódot jelenti

eIDAS	910/2014/EU rendelet közismert megnevezése
E-mail kód	A Szolgáltató által az ügyfél email címére megküldött véletlenszerűen generált, egyedi (azaz tranzakciónként eltérő) öt számjegyű, betűt vagy speciális karaktert nem tartalmazó kód
E-szignó Automata	a Microsec Zrt terméke (https://e-szigno.hu/uzleti-megoldasok/e-szigno-automata.html)
hash függvény	kriptográfiai függvény, amellyel bármilyen hosszúságú adatot adott hosszúságú bitsorozatra képez le, az eredményből az eredeti adatsorozat nem állítható vissza; ld. SHA-256
SHA-256	ld. FIPS 180-4 (March 2012) szabvány
HSH1	a Szolgáltató rendszere által az Aláírt DOC1 és a datagram 1 alapján, készített SHA-256 hash
HSH2	a Szolgáltató rendszere által az Aláírt DOC1, Aláírt DOC2, HSH1 és a datagram 2 alapján, készített SHA-256 hash
HSM	(Hardware Security Module) fejlett kriptográfiai, biztonsági és kulcs menedzsment funkciókkal rendelkező dedikált hardver biztonsági eszköz
MicroTRX	Az az 1 forintos átutalás (mikrotranzakció), amely folyamán az ügyfél megkapja az 'MicroTRX kódját'. A tranzakció az ügyfél által az szerződés kötési folyamat során megadott folyósítási számlaszámra érkezik.
MicroTRX kód	az ügyfél számára véletlenszerűen generált, egyedi (azaz ügyfelenként és tranzakciónként eltérő), egyszer használatos 8 karakterrel leírható véletlen érték, amely kizárólag számjegyekből állhat, és amely a P2P aláírás során kerül felhasználásra, azt elindítva
MNB rendelet	a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól szóló 19/2017. (VII. 19.) MNB rendelet
online felület	Az ügyfél számára kiajánlott, a speciálisan egy-egy banki termékhez kapcsolódó online szerződéskötési folyamat céljára kialakított informatikai szolgáltatás, amely segítségével az ügyfél a Szolgáltató által meghatározott ügyletek tekintetében szerződéskötést kezdeményezhet és

	teljesen online módon megkötheti az azokhoz kapcsolódó szerződéseket.
OID	objektum azonosító kód az International Telecommunications Union (ITU) és az ISO/IEC által meghatározott rendszerben
P2P	peer-to-peer
PAdES-T	(PDF Advanced Electronic Signatures) PDF dokumentumok aláírásának típusa; ld. ISO 32000-1
PDF	(Portable document format) Adobe Systems, Inc. dokumentum-formátum szabványa
peer-to-peer	Kapcsolódási mód, amely alkalmazható fokozott biztonságú elektronikus aláírás létrehozásához; közvetlen, személyközi aláírás; megbízható harmadik féltől független aláírási mód
Pmt.	a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény
Publikus Kulcsú Infrastruktúra	A publikus (vagy nyilvános) kulcsú infrastruktúra kriptográfiai kulcsmenedzsmentből, tanúsítvány menedzsmentből, hitelesítés és időbélyegzős szolgáltatásokból, kriptográfiai műveleteket és különböző szabványos adatkezelést végző rendszerekből és szabályozási eszközökből tevődik össze. Publikus Kulcsú Infrastruktúra jelentős mértékben szabványos eszközökkel és megoldásokkal működik.
SMS kód	A Szolgáltató által az ügyfél telefonszámára megküldött véletlenszerűen generált, egyedi (azaz tranzakciónként eltérő) öt számjegyű, betűt vagy speciális karaktert nem tartalmazó kód

1.6.2 Jogszabályi hivatkozások

- 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: **eIDAS**)
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: **E-ügyintézési tv**.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: **Ptk.**)
- 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről (továbbiakban: **BM rendelet**)

- 137/2016 (VI. 13.) Korm. rendelet az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz

1.6.3 Szabványok és műszaki-technikai specifikációk

A Szolgáltató által nyújtott Szolgáltatás megfelel a jelen 1.6.3 fejezetben felsorolt szabványoknak. Ezek a szabványok a következők:

ETSI SR 019 050 V1.1.1 (2015-06)	Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures (Az elektronikus aláírásokat alkalmazó, regisztrált elektronikus kézbesítési szolgáltatásokra vonatkozó szabványok racionalizált keretrendszere)
ETSI EN 319 401 v2.2.1	General Policy Requirements for Trust Service Providers (A bizalmi szolgáltatók szabályzataira vonatkozó általános előírások)
ETSI TR 103 304 V1.1.1 (2016-07)	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services (Személyes azonosítást lehetővé tevő információk védelme mobilos és felhőszolgáltatások esetében)
ETSI TR 119 000 V1.2.1 (2016-04)	Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview (Az aláírások szabványosításának keretrendszere: áttekintés)
ISO 27001 A.6.2.	External parties (Külső felek)
ISO 27001 A.10.2.	Third party service delivery management (Harmadik fél szolgáltatások kezelése)

1.6.4 A Szolgáltató egyéb szabályozó eszközei

- Üzletszabályzat
- Adatvédelmi tájékoztató
- Elektronikus azonosítású szolgáltatások általános szerződési feltételei
- Szerződés

2. Közzététel és tároló

2.1 Hitelesítéssel kapcsolatos információk közzététele

A Szolgáltató a jelen Szabályzat szerinti Szolgáltatást kizárólag releváns üzleti folyamatai során nyújtja, az érintett fokozott biztonságú elektronikus aláírás pedig kizárólag az adott folyamatban és annak céljára kerül alkalmazásra.

Egyéb célú felhasználásra nincs lehetőség, a Szolgáltató az ügyféllel való kapcsolata során nem bocsát ki tanúsítványt. Következésképp a Szolgáltató nem tesz közzé tanúsítványokkal kapcsolatos információt.

A Szolgáltató az általa nyújtott Szolgáltatással kapcsolatos információt, valamint a bizalmi szolgáltatások igénybevételével összefüggő általános információt a vonatkozó weblapján (https://www.kh.hu/bizalmi-szolgaltatas) teszi közzé, míg az egyéb közérdekű szolgáltatói információ a kh.hu weboldalon kerül közzétételre.

2.2 A tárolókhoz való hozzáférés ellenőrzése

A Szolgáltató megfelelő technikai és eljárásbeli biztonsági intézkedésekkel gondoskodik az információkhoz való jogosulatlan hozzáférés, illetve azok megváltoztatása, sérülése és megsemmisülése elleni védelemről.

3. A személyazonosság ellenőrzésének folyamata

Ahogyan azt a jelen Szabályzat 1.3 pontjában is kifejtettük, a Szolgáltató nem bocsájt ki tanúsítványt. A jelen fejezetben szereplő folyamatleírás célja, hogy bemutassa, hogy az ügyfél miként kerül azonosításra a Szolgáltató által, hogy a folyamat során azonosított ügyfél adatait annak aláírásához rendelhesse, ebből kifolyólag nem hivatkozik olyan szabványokra és nem ír le olyan folyamatokat, amelyek tanúsítvány kibocsátása esetén elengedhetetlenek lennének.

3.1 Személyazonosság ellenőrzése

3.1.1 Az azonosítási folyamat

Az azonosítás első lépéseként az ügyfél az 'online felületen' megad néhány személyes adatot (vezetéknév, keresztnév, születési idő), és megerősítteti elérhetőségeit (SMS, e-mail). Ezt követően a valós idejű ügyfél-átvilágítás folyamatát a Szolgáltató – a Pmt. végrehajtására kiadott MNB rendelet alapján – kép-és hangfelvétellel rögzíti, amelyen az ügyfél a Szolgáltató egy telecenter-es munkavállalójával fog valós időben video chat-en keresztül beszélgetni. A videó azonosításra szolgáló alkalmazás a hatályos jogszabályi előírásoknak megfelelően került kiválasztásra és auditálásra.

Ezen valós idejű ügyfél-átvilágítás során a bemutatkozást követően egyeztetésre kerülnek a korábban megadott személyes adatok, továbbá az ügyfél mobiltelefonjának/telefonszámának és e-mail címének újbóli validálására is sor kerül. A Szolgáltató az ügyfél által az online felületen megadott telefonszámra és e-mail címre egy-egy véletlenszerűen generált kódot küld, melyet az ügyfél a kódok rendelkezésre bocsátását követően a felület meghatározott mezőjébe beírja. A Szolgáltató ellenőrzi a kódok helyességét. A fenti azonosítás azt a célt szolgálja, hogy a Szolgáltató meggyőződhessen arról, hogy valódi személlyel került kapcsolatba, illetve, hogy a Szolgáltató rendelkezésére álljanak azok a létező csatornák, amelyeken keresztül szükség szerint fel tudja az ügyféllel venni a kapcsolatot.

Ezt követően a Szolgáltató az ügyfél arcképéről, valamint a kártyaformátumú személyazonosító igazolványáról (személyi igazolvány, lakcímkártya), és azok biztonsági elemeiről (pl. hologram) is felvételeket készít. A Szolgáltató a kártyaformátumú személyazonosító igazolvány adatait – azok érvényességének, valamint az adatok egyezőségének ellenőrzése céljából – összeveti a GIRO Zrt.-nél, a GIRinfO szolgáltatás keretében kezelt adatokkal.

Az azonosítás további lépése, hogy a Szolgáltató az ügyfél által korábban az online felületen megadott bankszámlaszámára egy, a 3.1.2. pontban meghatározott kódot küld, így ellenőrizve a felületen megadott bankszámlaszám valódiságát.

3.1.2 Az elhelyezendő elektronikus aláírás létrehozásával kapcsolatos adatok kizárólagos kontrollja és bizalmas mivolta

A kizárólagos kontroll és a bizalmasság védelmének magas fokát az alábbiak biztosítják:

- A MicroTRX kód nem látható a bejövő tranzakciók bankszámlára való beérkezését követően kiküldött egyszerű SMS értesítésekben,
- Az érintett bankszámla felett rendelkezésre jogosult e minőségében nem élhet vissza a MicroTRX kóddal, mivel a rendelkezésre jogosult nem menne át a 3.1.1 fejezetben leírt azonosító ellenőrzéseken és a bankszámla feletti tulajdonjog ellenőrzésén.
- A MicroTRX kódhoz a megfelelő internet bankok és azok szolgáltatásain keresztül lehetséges hozzáférni, vagyis elengedhetetlen az azokba történő belépéshez szükséges erős hitelesítés.
- A Szolgáltató a belsőleg tárolt MicroTRX kódok jogosulatlan hozzáférés elleni védelméhez a jelenleg rendelkezésre álló minden ésszerű technológiát és folyamatmegoldást felhasznál.

4. Az elektronikus aláírás létrejöttének és elhelyezésének folyamata

4.1 Az elektronikus aláírás létrejöttének és elhelyezésének folyamata

A szerződéskötést (és az aláírást) megelőző ügyfél-azonosítási folyamat leírása

A folyamat elindítása: A folyamat első lépéseként az ügyfél személyi számítógép, tablet vagy mobiltelefon segítségével egy internetes böngészőn keresztül megnyitja a Szolgáltató online felületét és ezt követően a Szolgáltató az ügyfél vonatkozó hozzájárulása birtokában, ellenőrzi az ügyfél földrajzi lokációját, IP cím alapján.

Személyes adatok valamint egyéb szükséges ügyfél-adatok megadása: Az ügyfél megadja az online felület által kért személyes adatait, továbbá a mobiltelefon számát és email címét, valamint azt a magyarországi bankszámla számot, amelynek az ügyfél-azonosítás és az aláírás kapcsán lesz jelentősége az alábbiak szerint. Az online rendszeren keresztül történő szerződés megkötésére és így az elektronikus aláírás elkészítésére kizárólag azok az ügyfelek jogosultak, akik rendelkeznek a Szolgáltató által meghatározott, magyar banknál vezetett bankszámlával és e bankszámla vonatkozásában internetbank hozzáféréssel.

Az ügyfél és az általa használt kommunikációs csatornák ellenőrzése: A Szolgáltató egy-egy - véletlenszerűen generált, egyedi (azaz tranzakciónként eltérő) öt számjegyű, betűt vagy speciális karaktert nem tartalmazó, - kódot küld az ügyfélnek a megadott telefonszámra illetve email címre (a továbbiakban: „**SMS-kód**” és „**Email-kód**”). Mindkét kód titkosított módon, ún. pszeudorandom generátorral kerül előállításra. A kódok limitált ideig érvényesek, és az ügyfélnek maximum három lehetősége van a kódok online felületen történő helyes bevitelére, akként, hogy a vonatkozó mezőbe beírja a kapott két egyedi kódot. A beírt kódok helyességét a Szolgáltató ellenőrzi. Ez az azonosítás alapvetően arra szolgál, hogy a Szolgáltató meggyőződhessen arról, hogy valódi személlyel került kapcsolatba, illetve, hogy szükség esetén rendelkezésre álljanak azok a kommunikációs csatornák, amelyeken keresztül az ügyféllel fel tudja venni a kapcsolatot.

Az ügyfél személyazonosságának ellenőrzése: A folyamat egy további lépéseként megtörténik az ügyfél személyazonosságának ellenőrzése, amely minden esetben a Pmt. valamint a végrehajtására kiadott MNB rendelet rendelkezéseivel összhangban történik előzetesen auditált elektronikus hírközlő eszköz útján, amely a gyakorlatban egy élő, video-csatornán történő azonosítást jelent. A video-azonosítás egyik lépéseként az ügyfél köteles az ügyintézőnek bemutatni személyazonosító igazolványát valamint a lakcímkártyáját. A Szolgáltató IT rendszerei ellenőrzik az igazolvány és lakcímkártya számát, továbbá a kártya érvényességének valamint az adatok egyezőségének ellenőrzése céljából hatósági adatszolgáltatótól, a GIRO Zrt. GIRinfO szolgáltatásának igénybe vételével, lekérik a szükséges ügyféladatokat.

A szerződéskötési folyamat leírása a végső ajánlatig:

Az elektronikus aláírás létrehozásához használt adat: A video-azonosítással egyidejűleg a Szolgáltató, - szükség szerint közvetítő igénybe vételével, - kis (1 Ft) összegű átutalást küld az ügyfél által megadott bankszámlaszámra (ez az ún. „**MicroTRX**").

A Szolgáltató az átutalás közleményében elküldi az ügyfél részére a harmadik azonosító kódot („**MicroTRX kód**") amely az ügyfél elektronikus aláírásának létrehozásához használt adat.

A MicroTRX kód generálása, az ügyfél részére történő rendelkezésre bocsátása, valamint használata teljes mértékben az eIDAS 26. cikkében foglalt követelményekkel összhangban történik. A Szolgáltató e körben felhívja az ügyfelek figyelmét a következőkre:

- MicroTRX kódhoz az ügyfél minden esetben (azaz akkor is, ha SMS értesítést kap az átutalásról) kizárólag a meglévő internetbankjába belépve – a belépéshez szükséges azonosítást követően - tud hozzáférni, ugyanis az alkalmazott technikai megoldásnak köszönhetően az SMS-ben küldött szöveg nem fogja tartalmazni a MicroTRX kódot: a kód az átutalási közlemény utolsó nyolc számjegye. Az átutalási közlemény 57 karakterből áll, és a netbanki felületre bejelentkezve a teljes átutalási közlemény olvasható. Ugyanakkor, bár az SMS értesítés tartalmazhatja az átutalási közlemény egy részét, az SMS hosszának limitáltsága és a „feladó" névhosszúsága miatt az MicroTRX kód nem látszik az SMS-ben;
- az azonosítási és szerződéskötési folyamat során használt kódok (azaz az SMS kód, az Email kód és a MicroTRX kód) mindegyike automatikusan kerül generálásra, naplózásra és megküldésre az ügyfél részére. Az érintett rendszerelemekhez történő hozzáférés korlátozott, naplózott, és az esetleges hozzáférés biztonságos csatornán keresztül történik. A kódok több rendszeren futnak keresztül és e rendszerek mindegyikéhez egyik munkatársnak sincs egyidejű azonnali hozzáférése. A rendszer kialakítása miatt a fenti háromféle kód kombinációja minden esetben egyedi. Az elektronikus aláírásokat létrehozó alkalmazást (Signature Creation Application) az online felület működteti.

Az eljáró ügyfél további ellenőrzése: A Szolgáltató az ügyfél által megadott adatok és a saját adatbázisai, illetve – szükség szerint – az ügyfél által a banki rendszerbe feltöltött bankszámla-kivonat alapján automatikusan ellenőrzi, hogy a bankszámla számlatulajdonosa azonos-e az eljáró ügyféllel. A Szolgáltató kizárólag olyan ügyféllel köt szerződést, aki a személyazonosítási eljáráson átesett és a Szolgáltató által ügyfélként befogadása megtörtént.

A szerződéstervezet (DOC1) elkészítése: A jogszabályok által megkövetelt tájékoztatás megtörténtét és a szerződés megkötéséhez szükséges egyéb követelmények teljesülését követően a Szolgáltató elkészíti az adott ügyre vonatkozó szerződés tervezetét, amely már tartalmazza az ügyfél és az ügylet pontos adatait is („**DOC1**"). A folyamat során a rendszer a megadott adatok alapján a vonatkozó szerződés-mintát felhasználva automatikusan generálja az egyedi szerződést.

A végleges ajánlat (Aláírt DOC1) elkészítése és az ügyfél rendelkezésére bocsátása: Szolgáltató a DOC1-et minősített elektronikus bélyegző tanúsítvánnyal (PAdES-T) és időbélyegzővel látja el, létrehozva így a végleges ajánlatot („**Aláírt DOC1**"). A Szolgáltató az ügyfél rendelkezésére bocsátja az Aláírt DOC1-et (a jogszabályok által megkövetelt esetleges további dokumentumokkal együtt).

Az aláírási folyamat részletes leírása a végleges ajánlat elfogadásától:

Az ügyfél a végleges ajánlat, azaz Aláírt DOC1, birtokában eldöntheti, - a választásának megfelelő gombra történő kattintással, - hogy meg kívánja-e kötni a Szolgáltatóval a szerződést, vagy sem.

Amennyiben az ügyfél meg kívánja kötni a szerződést, úgy a szerződést az ügyfélnek alá kell írnia a következők szerint: az ügyfél a megjelölt helyre beírja a MictroTRX keretében kapott MicroTRX kódot (azaz felhasználja azt az elektronikus aláírása létrehozásához), majd a szerződéskötési szándékát megerősítendő a megfelelő gombra kattint (azaz kezdeményezi a szerződés aláírását). A Szolgáltató automatikus rendszerei ellenőrzik az elküldött és a beírt kódok egyezőségét.

Ezt követően a Szolgáltató rendszere SHA-256 algoritmussal egy hash-t készít, amely alapja az Aláírt DOC1, valamint az ügyfélre és az adott ügyletre vonatkozó datagram 1 (ez a hash a „**HSH1**").

Az aláírási folyamat fentiek szerinti elindítását követően a Szolgáltató rendszere az (Aláírt) DOC1 adatai alapján automatikusan létrehoz egy új dokumentumot („**DOC2**"), amely tartalmát tekintve mindenben megegyezik a DOC1-gyel, kivéve, hogy a létrehozásakor már azonnal és automatikusan tartalmazza a MicroTRX kódot is.

A DOC2-t létrehozó rendszer minden releváns mozzanata naplózott (Nagios rendszer által monitorozott) továbbá riasztás-védelemmel ellátott. Az automatizmuson túlmenően többek között ezek a magas színvonalú biztonsági elemek gondoskodnak arról, hogy a DOC1 és a DOC2 tartalma, - az aláíráskor a dokumentumhoz rendelt aláírási adatokat leszámítva, - megegyezik, és a későbbiekben bármely esetleges változás nyomon követhető és azonosítható. A dokumentumok tartalmi egyezőségéről az ügyfél szabad szemmel is meggyőződhet.

A DOC2-t a Szolgáltató rendszere a létrehozását követően azonnal minősített elektronikus bélyegző tanúsítvánnyal és időbélyegzővel látja el. Ez egyrészt az ügyfél által aláírt példány Szolgáltató általi aláírását jelenti, másrészt biztonságosan „lezárja" a mindkét fél által aláírt dokumentumot („**Aláírt DOC2**"). A teljes folyamat automatizált, zárt és a Szolgáltató IT rendszereiben naplózott. Ebből következően az online folyamat során elkészített és mindkét fél által aláírt szerződés technikai szempontú módosítására nincs lehetőség.

Ezzel párhuzamosan a Szolgáltató rendszere SHA 256 algoritmussal egy második hash-t is készít, amely tartalmazza az Aláírt DOC1-et, az Aláírt DOC2-t, HSH1-et, valamint az ügyfélre és az adott ügyletre vonatkozó datagram 2-t (ez a hash a „**HSH2**").

További intézkedések az aláírás megtörténtét követően:

A Szolgáltató az aláírási folyamatot követően, kizárólag információs céllal elkészít egy további dokumentumot, amely olvasható formában tartalmazza a HSH2-t („**DOC 3**").

A Szolgáltató a saját minősített elektronikus bélyegző tanúsítványával (PAdES-T) és időbélyeggel látja el a DOC 3-at, majd az ügyfél rendelkezésére bocsájtja.

A DOC 3 dokumentum szolgál bizonyítékul az ügyfél számára az aláírás megtörténtéről, mert ebből a dokumentumból visszafejthető az aláírási folyamat minden lépése.

Minden adat egy, az ISO27001-nek és a K&H/KBC biztonsági előírásainak megfelelő ISMS és ITIL folyamatok szerint irányított és működő, biztonságos adatközpontban kerül tárolásra.

5. Fizikai, eljárási és személyzeti óvintézkedések

Ez a fejezet az alkalmazott megoldások, biztonsági naplózási eljárások és adatarchiválás tekintetében alkalmazott fizikai és személyzeti óvintézkedéseket írja le.

5.1 Fizikai óvintézkedések

5.1.1 K&H adatközpont

A KBC Csoport magyarországi adatközpontjai dedikáltan erre a célra tervezett épületekben kerültek kialakításra. Az adatközpont kielégíti a TIER minősítési rendszerben elérhető 3. fokozat által támasztott követelményeket.

Az adatközpont fizikai biztonságáról többek között a fizikai hozzáférés korlátozása gondoskodik. Az adatközpontokban folyamatosan biztonsági személyzet teljesít szolgálatot, biztosítva többek között az előre definiált beléptetési protokollok maradéktalan betartatását, emellett rendszeresen járőrözik az épületekben. Az állandó személyzeten kívül mindenki más csak kísérővel tartózkodhat az épületekben.

Az adatközpont területén CCTV rendszer működik, melynek segítségével az események utólagos rekonstruálására is lehetőség nyílik.

Az épületekben biztonsági zónák kerültek kialakításra a különösen érzékeny területek védelmének fokozása érdekében (sms-ben biztosított egyszeri jelszó szükséges a belépésez).

Az adathordozók selejtezésére vonatkozó előírást a CEDC-ÜZEM-01 Adatközpont üzemeltetési szabályzat 7. fejezete tartalmazza, amely külön foglalkozik a különböző típusú adathordozókkal, illetve a folyamathoz szükséges részletes dokumentációs követelményeket is meghatározza.

Az adathordozók tárolására vonatkozó előírást a CEDC-ÜZEM-01 Adatközpont üzemeltetési szabályzat 7.2.1 fejezete tartalmazza, melynek értelmében az adathordozókat megsemmisítésig erre a célra dedikált, zárt páncélszekrényben kell tárolni.

Mindkét adatközpont dedikált helyiséggel rendelkezik a szalagos mentőrendszer számára. A rendszeres mentések és az archív szalagok is ezekben a rendszerekben kerülnek tárolásra, így biztosítva fizikailag elkülönítetten őrzött, duplikált mentési példányokat.

A fentieken túlmenően az adatközpont természetesen rendelkezik a szervertermek környezeti tényezőinek folyamatos ellenőrzéséhez és fenntartásához szükséges berendezésekkel, felszerelésekkel is, úgy, mint hőmérséklet és páratartalom figyelés, 2N+1-es redundanciával rendelkező klímaberendezés.

Nedvesség érzékelők és emelt padló biztosítja a beázás és elárasztás észlelését és kezelését, illetve az IT helyiségekben sem a mennyezet, sem a padló, sem a falak mentén nem haladnak vízvezetékek.

Gázzal működő tűzoltó berendezés gondoskodik a tűzvédelemről, illetve 2N+1-es redundanciával rendelkező szünetmentes tápegységek és dízelgenerátor biztosítsa a folyamatos áramellátást.

A rendkívüli üzemhelyzetek, katasztrófák kezelésére mindkét adatközpont rendelkezik kiürítési, illetve részletes katasztrófa elhárítási tervvel. A katasztrófa elhárítás terv teljes körű, részletesen dokumentált tesztelésére évente kétszer kerül sor, mely szimulálja az egyik

adatközpont részleges vagy teljes kiesését. A feltárt hiányosságok, problémák legkésőbb a következő tesztig megoldásra kerülnek.

5.1.2 O2 CZ felhőszolgáltató központ

Az online felület (a valós idejű ügyfél-átvilágításra használt szoftver kivételével) a „Nagano Park" (K Červenému dvoru 25/3156 Prága 3, Csehország) 3. fokozatú adatközpontban kerül üzemeltetésre. A csehországi O2 3. fokozatú hitelesítést kapott tervezési dokumentumokra az Uptime Institute Professional Services, LLC-től.
Az online felület környezetről naponta biztonsági mentés készül.
Az adatközpont a fizikai biztonságról a fizikai hozzáférés korlátozásával gondoskodik. A csatlakoztatott erőforrások mindegyike rendelkezik vírusvédelemmel.

5.2 Személyzeti szabályzatok

5.2.1 Bizalmi munkakörök

Szolgáltató az alábbi bizalmi munkaköröket azonosította, melyektől a Szolgáltatás biztonsága függ:
a) a Szolgáltató informatikai rendszeréért általánosan felelős vezető;
b) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;
c) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;

d) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;
e) független rendszervizsgáló: a Szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a Szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy;
f) regisztrációs felelős: az elektronikus aláírások előállításának, kibocsátásának, felfüggesztésének és visszavonásának jóváhagyásáért, az életciklus menedzsment tevékenységek szabályszerű végzéséért felelős személy;

A bizalmi munkakörökhöz tartozó feladatkörök és felelősségek leírását a Szolgáltató belső szabályzata határozza meg.
A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval.
Valamennyi bizalmi munkakört betöltő személy rendelkezik helyettessel.
A bizalmi munkaköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A bizalmi munkaköröket tartalmazó nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a vonatkozó jogszabályok alapján a Bizalmi Felügyeletnek bejelenti.

5.2.2 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy
a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;
b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, a regisztrációs felelős, és a rendszeradminisztrátor feladatait.

5.2.3 Képzettségre vonatkozó rendelkezések

Szolgáltató kellő számú, a Szolgáltatás nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező munkavállalókat alkalmaz.

Szolgáltató garantálja, hogy bizalmi munkakört csak olyan személyek töltenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

Szolgáltató figyelmet fordít arra, hogy a kollégák folyamatosan a megfelelő tudással rendelkezzenek, ennek érdekében rendszeres időközönként továbbképzést vagy ismétlő jellegű képzést biztosít.

Szolgáltató a nagyobb jelentőségű változtatások esetén ismételt, vagy az adott változtatásra vonatkozó képzést tart az érintett kollégák számára. Azaz a Szolgáltató biztonságpolitikájának változtatása, a szoftver vagy hardver jelentős változása (upgrade), vagy a kulcs kezelésének és biztonsági kezelési óvintézkedéseinek változása esetén, valamennyi kolléga, az őt érintő mélységben továbbképzésben részesül, továbbá megkapja a szükséges dokumentációkat. Kisebb jelentőségű változások esetén a kollégák a várható változásról, annak bekövetkezte előtt írásos tájékoztatást kapnak.

Szolgáltató legalább évente egyszer továbbképzést biztosít az újonnan ismertté vált jogszabályokról, sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a kollégák saját szakterületét érintően.

Szolgáltató folyamatosan biztosítja a munkavállalók részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.
Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

- egyéni munkaköri leírást;
- valamennyi releváns szabályzatot, vonatkozó nyilvános és belső dokumentációt;
- továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.2.4 Követelmények és korlátozások a K&H adatközpontban

A KBC Csoport magyarországi adatközpontjai dedikáltan erre a célra tervezett épületekben kerültek kialakításra. Az adatközpont kielégíti a TIER minősítési rendszerben elérhető 3. fokozat által támasztott követelményeket. Az adatközpont fizikai biztonságáról többek között a fizikai hozzáférés korlátozása gondoskodik. Az adatközpontokban folyamatosan biztonsági személyzet teljesít szolgálatot, biztosítva többek között az előre definiált beléptetési protokollok maradéktalan betartatását, emellett rendszeresen járőrözik az épületekben. Az

állandó személyzeten kívül mindenki más csak kísérővel tartózkodhat az épületekben. Az adatközpont területén CCTV rendszer működik, melynek segítségével az események utólagos rekonstruálására is lehetőség nyílik. Az épületekben biztonsági zónák kerültek kialakításra a különösen érzékeny területek védelmének fokozására.

A fentieken túlmenően az adatközpont természetesen rendelkezik a szervertermek környezeti tényezőinek folyamatos ellenőrzéséhez és fenntartásához szükséges berendezésekkel, felszerelésekkel is, úgy, mint hőmérséklet és páratartalom figyelés, klímaberendezés, emelt padló, tűzoltó-berendezés, szünetmentes tápegységek, dízelgenerátor.

5.2.5 Követelmények és korlátozások az O2 CZ felhőszolgáltató központban

Az O2 adatközpont több adatközpontból áll, melyek összekapcsolt gerinchálózatot alkotnak. Az O2 CZ társaság minden, az Uptime Intézetnek a 3. fokozatú specifikációkban (tervezési dokumentumok hitelesítési fokozatai) foglalt hitelesítési követelményei értelmében az adatközpontok működtetésére vonatkozó feltételnek megfelel (DC Chodov, DC Nagano, DC Hradec Králové).
Alkalmazott működési folyamatok – DRP, ISMS és ITIL folyamatok.

5.3 Biztonsági naplózási folyamatok

5.3.1 Ellenőrzési naplózási események

Az informatikai és kommunikációs rendszerek naplózzák a működésük során bekövetkező fontosabb eseményeket, valamint a felhasználói tevékenységeket, de jelszavak és érzékeny személyes adatok nem kerülnek naplózásra.

5.3.2 Naplófájlok elemzése

Monitorozó rendszer elemzi a naplófájlokat az informatikai és kommunikációs rendszerek állapotának ellenőrzése és a Szolgáltatás folyamatos biztosítása érdekében. Ezen túlmenően a Szolgáltatás nyújtásában fellépő rendellenes esemény vagy tevékenység feltárása érdekében, potenciális incidens észlelésekor, továbbá rendellenes esemény vagy tevékenység megelőzése érdekében a naplófájlok elemzésre kerülhetnek.

5.3.3 Naplófájlok tárolásának ideje

A naplófájlokat a naplógyűjtő komponens 10 évig őrzi meg.

5.3.4 Naplók központi gyűjtése

A naplófájlok a szerverről időszakonként átmásolásra kerülnek a központi gyűjtőre.

5.3.5 Naplófájlok védelme

A naplók védelme az alkalmazásokéval megegyező módon történik – a szerverekhez való hozzáférés a felhasználói szerepkörön alapul.
A központi naplógyűjtő el van különítve a többi szervertől.

5.3.6 Naplófájlok biztonsági mentése

A biztonsági mentésre minden nap sor kerül. A biztonsági mentések 14 napig érhetők el, majd ennek az időszaknak a végén törlésre kerülnek. A biztonsági mentések teljes körűen tartalmazzák az adatokat – a szerveren található egyes fájlok deltáiról (különbségeiről) is biztonsági mentés készül. A biztonsági mentéseket az adatközpont működtetője (O2) törli – automatikus beállítás.

A naplófájlok a későbbiekben átmásolásra kerülnek a naplószerverre.

6. Technikai biztonsági kontrollok

A technikai biztonsági kontrollok a jelen fejezetben bemutatott elektronikus aláírásokhoz kapcsolódnak.

6.1 Az elektronikus aláírások létrejötte – adatok generálása

6.1.1 Az elektronikus aláírások létrejötte, az elektronikus aláírás elemei és az adatok eljuttatása az aláíróhoz

A MicroTRX kód (elektronikus aláírás-létrehozó adat) mikrotranzakción keresztül megküldésre kerül az aláíró részére a mikrotranzakcióhoz kapcsolódó közlemény rovatban, utolsó 8 karaktere formájában. A mikrotranzakció csak az ügyfél által a kérelemben megadott számlára kerül megküldésre.

Az ügyfélnek a folyamat végén meg kell adnia a MicroTRX kódot a szerződés aláírásához.
A MicroTRX kód minden szerződéskötés (és így minden ügyfél, valamint minden pénzügyi tranzakció) esetében egyedi, és kizárólag az internetbankba való bejelentkezést követően hozzáférhető (a részleteket lásd a 3.1.2 fejezetben).

Az elektronikus aláírás az alábbi elemekből tevődik össze:

- *HSH 1*, amelynek bemeneti adatai az Aláírt DOC1 és a datagram 1;
- *datagram 1* amely a fenti 1.6.1. pontban, a datagram 1 definíciójában meghatározott adatokat tartalmazza;
- *HSH 2*, amelynek bemeneti adatai az Aláírt DOC1, Aláírt DOC2, HSH1 és a datagram 2;
- *datagram 2* amely a fenti 1.6.1. pontban, a datagram 2 definíciójában meghatározott adatokat tartalmazza.

6.1.2 Az elektronikus aláírások létrejötte – adatméret

A MicroTRX kód 8 karakterből áll (melyek kizárólag számok lehetnek, speciális vagy regionális karakterek nem), így kombinációk milliárdjait teszi lehetővé.
A MicroTRX kódot egy titkosítással biztosított pszeudorandom generátor hozza létre véletlenszerű módon.

6.1.3 Az elektronikus aláírások létrejötte – adatok generálása és minőségellenőrzés

Az ügyfélnek három próbálkozása van, hogy megadja a helyes kódot, és így létrehozza az elektronikus aláírás. Az ügyfél által beírt kódot a rendszer összehasonlítja az ügyfélnek megküldött MicroTRX kóddal. A szerződéskötési és aláírási folyamat csak akkor folytatódik, ha a két kód megegyezik. Három sikertelen kísérlet után a szerződéskötési folyamat törlésre kerül, és ilyen esetben nem jön létre aláírás.

6.1.4 Az elektronikus aláírások létrejötte – az adatok felhasználásának céljai

Az ügyfélnek a folyamat végén meg kell adnia a MicroTRX kódot a szerződés aláírásához.

Az ügyfél a kódnak az űrlapon való megadásával és az „aláírás” gomb megnyomásával kinyilvánítja az irányú akaratát, hogy szeretné megkötni a szerződést a rendelkezésére bocsátott dokumentumnak (.pdf fájl) megfelelően.

.

Az elektronikus aláírás létrehozásához kapcsolódó adatok felhasználásra kerülnek az ügyfél tényleges elektronikus aláírásának létrehozásához.

6.2 Az elektronikus aláírások létrejötte – adatvédelem és a kriptográfiai modul vezérlő kontrolljai

Az elektronikus aláírás létrehozásához kapcsolódó adatok vagy a rendszeren belül kerülnek tárolásra, vagy egy biztonságos csatornán keresztül megküldésre kerülnek az ügyfél részére. A szerződéses dokumentumokat és tartalmukat a Szolgáltató szabvány PAdES minősített elektronikus bélyegző tanúsítványa és időbélyeg védi a változtatásoktól.

6.2.1 A kriptográfiai modulra vonatkozó szabványok és kontrollok

A véletlenszám-generátorokat java.security osztályú SecureRandom funkció biztosítja rejtjelezés útján.
A dokumentumok lezárását a Szolgáltató szabvány PAdES bélyegzője és időbélyege biztosítja.

6.2.2 Az egyazon elektronikus aláírás létrehozásához kapcsolódó adatok ismételt felhasználásának megakadályozására alkalmazott módszer

A MicroTRX kód teljesen egyedi. Amikor a véletlenszám-generátor egy korábban már használt kombinációt generál, mielőtt a rendszer megküldené az ügyfélnek, újraszámításra kerül, amíg egy korábban még nem használt nyolc számjegyű kód nem kerül legenerálásra.
A több milliárd lehetséges kombinációra és a kibocsátandó elektronikus aláírások várható mennyiségére tekintettel feltételezhető, hogy legalább 10 évig fenntartható a kódok egyedisége.

6.3 Az elektronikus aláírások létrehozása és kontrolljai

Az ügyfél elektronikus aláírása egy, az online szerződéskötési folyamat során generált lenyomat, amely tartalmazza a 6.1.1. pont szerinti elemeket, így az aláírt elektronikus adatokat, az aláírót azonosító datagram-struktúrát (datagram) és az elektronikus aláírás az ügyfél általi megadásának körülményeit.

6.3.1 Hash az elektronikus aláíráshoz

Az aláírt elektronikus adatok (digitális pdf dokumentum) és az aláírás létrehozásához kapcsolódó adatok csomagja (időbélyeg, valamint az ügyfél és a szerződéskötési folyamat azonosítója és paraméterei) alapján egy SHA-256 ellenőrző összeg készül. Ez az ellenőrző összeg megcáfolhatatlanul, egyedileg igazolja a dokumentum és az adatok sértetlenségét.

6.3.2 Adatcsomagok felhasználása a tördeléshez

Az adatcsomagok (datagram) biztonságos módon kerülnek létrehozásra a rendszerben az aláírási folyamat során.

Az adatcsomagok a fenti 1.6.1. pontban, a datagram 1 illetve a datagram 2 definíciójában meghatározott adatokat tartalmazzák. Ezen az adatok, az 1.6.1. pont vonatkozó meghatározása szerinti tartalommal, kiterjednek az ügyfél személyes és kapcsolattartási adataira, a körülményekre vonatkozó metaadatokra és az ügylettel illetve szerződéssel kapcsolatos adatokra.

6.3.3 A kapcsolódó aláírt dokumentumok és hash-ek

Az alkalmazott hash értékek biztosítják a dokumentumok, adatok utólagos módosítása elleni védelmet, így azok változatlanságát is igazolják.

6.3.4 Az elektronikus aláírás módosítását megakadályozó óvintézkedések

A hash-ek és az adatcsomag a csak olvasható ellenőrzési naplókban, valamint a Szolgáltató dokumentumkezelő rendszerének csak olvasható attribútumai között kerülnek tárolásra.
Az ügyfél rendelkezésére bocsátott dokumentumok integritását a pdf dokumentum PAdES bélyegzője és időbélyege biztosítja.

Mivel a hash-ek az aláírt elektronikus adatokra jellemzőek:

- a .pdf fájlok bármiféle későbbi megváltoztatása azt eredményezné, hogy az adott dokumentumhoz kapcsolódó, tárolt hash fájl nem egyezne meg a rendelkezésre bocsátott dokumentumból képzettel
- a hash fájl bármiféle későbbi megváltoztatása azt eredményezné, hogy a rendelkezésre bocsátott .pdf fájl alapján képzett nem egyezne meg magával a hash-sel az SHA-256 ellenőrző összeg újraszámításakor

6.4 Archiválás és tárolás

Amennyiben az ügyfél végig viszi az online felület által biztosított szerződéskötés teljes folyamatát, akkor az alábbi dokumentumok kerülnek lementésre az ügyfél eszközére:

1. Szerződéstervezet – DOC1
2. Szerződés (a K&H Bank Zrt. által aláírt verziója) – Aláírt DOC1
3. Szerződés (a K&H Bank Zrt. és az ügyfél által is aláírt verziója) – Aláírt DOC2
4. Szerződés melléklet – DOC3

A jogszabályi követelményeknek megfelelően az online szerződéskötési folyamat során keletkező dokumentumok a Szolgáltató dokumentumkezelő rendszerébe megfelelően kategorizáltan lementésre kerülnek. Az adott dokumentumkategóriák alapján a dokumentumok a megfelelő banki eljárások alapján kerülnek archiválásra, illetve a jogszabályok által meghatározott tárolási idő elteltével azok fizikailag is törlésre kerülnek.

A Szolgáltató a jelen Szabályzat szerinti Szolgáltatással kapcsolatban keletkezett vagy megszerzett adatokat a jogszabályokban - különösen a pénzmosási, adatvédelmi és könyvelési jogszabályokban - előírt kötelező megőrzési idő elteltével törli.

Tekintettel arra, hogy a Szolgáltató nem nyújt minősített bizalmi szolgáltatást, illetve, hogy a jelen Szabályzat szerinti szolgáltatás keretében nem kerül tanúsítvány kibocsátásra, az E-ügyintézési tv. 84. § szerinti 10 éves megőrzési idő nem általánosan, csak a Szabályzat 5.3. pontban körülírt napló-komponensek esetén alkalmazandó.

Mivel a dokumentumok újbóli elérésére az online felületen nincs lehetőség, az ügyfélnek az adott szerződésre irányadó jogszabályok által meghatározott időn belül van lehetőségük a Szolgáltatótól ezen dokumentumok elektronikus, és/vagy papír alapú pótlására, amennyiben ez szükséges.

6.5 Hálózatbiztonsági óvintézkedések

Az ügyfél a szerződéskötés kezdeményezését célzó információszerzés és az esetleges szerződéskötés lebonyolításának érdekében használja a Szolgáltató online szerződéskötési felületét (https://ekolcson.kh.hu).

A Szolgáltató gondoskodik arról, hogy a Szolgáltatást nyújtó informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerül sor. A Szolgáltató egyszerre több védelmi vonalat is használ:

- napi operatív működés folyamataiba épített kontrollok;
- adott rendszerességgel a szervezeti szinten működtetett kontrollok, ellenőrzések;
- független értékelés és belső ellenőrzés nyújt bizonyosságot az előző kettő védelmi vonal megfelelő működéséről.

A fokozott biztonságú elektronikus aláíráshoz tartozó érzékeny adatok bizalmasságát és sértetlenségét a Szolgáltató nem biztonságos hálózaton történő átvitel során is megfelelően védi.

A hálózatbiztonságot megvalósított biztonsági funkciók az alábbiak:

- biztonságos kommunikáció (a Szolgáltatást biztosító szerverek és felhasználó közötti, valamint a Szolgáltatást nyújtó rendszer komponensei közti kommunikáció bizalmasságának, sértetlenségének és hitelességének biztosítása. A Transport Layer Security titkosítási protokoll az Interneten keresztüli kommunikációhoz biztosít védelmet. Az adatközpontok közötti kommunikáció védelméről VPN csatorna gondoskodik. A Szolgáltatást nyújtó webszerver a felhasználó böngészőjének adott válaszok fejlécébe olyan információt tesz, amely jelzi a böngészőnek, hogy Szolgáltatás lapjaihoz a fejlécben megadott ideig mindig biztonságos csatornán kell fordulni. Az biztonságos csatornákhoz alkalmazott titkosító csomagok kizárólag erős titkosítás használatát engedélyezik.

- hálózati és alkalmazás szintű tűzfalas védelem: csomagszűrő tűzfalak és proxyk alkalmazásával csak a szolgáltatáshoz szükséges szolgáltatás-csatornák vannak nyitva a rendszerkomponensek, a felhasználók és az üzemeltetési szereplők számára.

A Szolgáltató biztosítja az általános informatikai biztonságot még akkor is, ha a Szolgáltatás egyes funkciót más egység valósítja meg. A Szolgáltató ún. mélységi védelmi stratégiát alkalmaz, mely azt jelenti, hogy az informatikai biztonság területén a védelem réteges felépítésű, azaz többrétegű védelem. A többrétegű védelem nem csak megakadályozza a Szolgáltatás illetéktelen használatát, hanem észleli az illegális tevékenységet, így lehetőséget a megfelelő eseti kezelésre is.

A Szolgáltató rendelkezik az informatikai és kommunikációs technológiai rendszereire vonatkozó, a 42/2015 (III.12.) Korm. rendelet 5/B. § elvárásainak teljesítésére vonatkozó zártsági tanúsítással.

A Szolgáltató általános informatikai és kommunikációs biztonsági szintjének megtartását illetve emelését biztosító belső folyamatokat rendszeresen ellenőrzi a belső ellenőrzés, egy a Szolgáltatótól független audit, valamint a Magyar Nemzeti Bank is.

7. Megfelelőség vizsgálat és egyéb értékelések

A Szolgáltató a jelen Szabályzat által érintett bizalmi Szolgáltatást az irányadó jogszabályok valamint a jelen Szabályzat 1.6.3. pontjában megjelölt szabványok és műszaki-technikai specifikációk alapján végzi.

A Szolgáltató külső és belső vizsgálatokat és ellenőrzéseket végez, illetve végeztet annak érdekében, hogy a Szolgáltatásával kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

Tekintettel arra, hogy a Szolgáltató bank, a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény (Hpt.) 154.§ (1) bekezdése értelmében közvetlenül a felügyeleti jogkörrel rendelkező vezető testület irányítása alatt álló belső ellenőrzési szervezeti egységet működtet. A Hpt. 154. § (12) cikke bekezdése értelmében a belső ellenőrzési funkció szervezetét, hatáskörét, feladatait és eljárásrendjét évente felülvizsgálandó belső ellenőrzési szabályzatban hivatalosan rögzíti.

A Szolgáltatónak a Szolgáltatásra vonatkozó szabályzatát a Bizalmi Felügyelet is megvizsgálja a nyilvántartásba vételi eljárása során, valamint az érintett szabályzat módosításakor, és megfelelőség esetén közzé teszi a kötelezően benyújtandó szabályzatot. A Bizalmi Felügyelet rendszeres időközönként (legalább évente) átfogó helyszíni ellenőrzés keretében ellenőrizheti Szolgáltató tevékenységét.

7.1 Vizsgálatok gyakorisága és körülményei

A belső ellenőrzési szervezeti egység az egyes banki tevékenységek és folyamatok kockázata alapján éves audit tervet állít össze. A belső ellenőrzés a különböző tevékenységeket és folyamatokat évente újraértékeli és minősíti, valamint belső szabályozásban rögzítetten a kockázattal megfelelően arányos időközönként azok teljes átfogó auditját elvégzi.

7.2 Auditor azonosítása és képesítése

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával. A belső ellenőrök igazoltan rendelkeznek feladatkörüknek megfelelő szakértelemmel és tapasztalattal, továbbképzésük a belső szabályzatban rögzített kereteknek megfelelően folyamatos.

A külső megfelelőségértékeléseket olyan természetes vagy jogi személyek (vagy ezek csoportja) végzi, aki a megfelelőség-értékelés elvégzéséhez megfelelő felhatalmazással rendelkezik, képes a Szolgáltató által végzett Szolgáltatásra irányadó szabványok vonatkozásában az audit elvégzésére (ideértve azt is, hogy rendelkezik a szükséges akkreditációval), és megfelel a jogszabályok és a jelen Szabályzat által támasztott függetlenségi követelményeknek.

7.3 Auditor függetlensége

A külső megfelelőségértékeléseket végző szervezet, annak munkatársai, valamint a külső rendszervizsgáló (’külső auditor’) teljes mértékben függetlenek Szolgáltatótól, így a külső auditor független többek közt a Szolgáltató tulajdonosi körétől, vezetőségétől és üzemeltetésétől illetve díjazása nem függ az értékelés során végzett tevékenységének végkimenetelétől.

A belső ellenőrzés a Hpt. 154. § (1) bekezdésének megfelelően az ellenőrzött területektől függetlenül, a Felügyelő Bizottság és a külső Igazgatósági tagokból álló Risk and Compliance Bizottság szakmai irányítása alatt végzi tevékenységét. A függetlenség megtartása érdekében az ellenőrzött területek vezetői a belső ellenőrzésnek nem adhatnak instrukciókat a vizsgálat módszere és terjedelme vonatkozásában.

7.4 Audit során vizsgált területek

Szolgáltató bizalmi Szolgáltatására vonatkozó megfelelőségértékelése során az alábbi területek vizsgálata és ellenőrzése történik meg:

- a hatályos, vonatkozó jogszabályoknak illetve műszaki szabványoknak való megfelelés;
- Bizalmi Szolgáltatási Rendnek és jelen Szolgáltatási Szabályzatnak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- az irányadó fizikai, személyi és IT biztonsági feltételek megfelelősége;
- az adatvédelmi szabályok betartása.

Külső megfelelőségértékelés esetén a megfelelőségértékelőnek az adott értékelési rendszer által meghatározott követelmények és kritériumok teljesülése kerül értékelésre.

A fentieken túlmenően a Hpt. 154. § (2) bekezdésének megfelelően a belső ellenőrzési rendszer működtetésének célja, hogy

a) a hitelintézet jogszabályoknak megfelelő működését elősegítse,

b) a hitelintézet belső szabályzataiban foglalt előírások betartását ellenőrizze,

c) a jogszabályoktól és a belső szabályzatokban foglaltaktól való eltéréseket feltárja, továbbá javaslatot tudjon megfogalmazni a feltárt hiányosságok kijavítására,

d) a döntéshozatalhoz szükséges pénzügyi és egyéb információk biztosíthatóak legyenek,

e) a hitelintézet, valamint ügyfeleinek és a tulajdonosoknak az érdekei védve legyenek, valamint

f) a hitelintézetre vonatkozó belső szabályzatokban foglalt előírások betartását, és azok tartalmi elégségességét ellenőrizze.

A belső ellenőrzési rendszer működési keretein belül a belső ellenőrzési szervezeti egység a törvényesség, a biztonság, az áttekinthetőség szempontjából vizsgálja a pénzügyi intézmény

- belső szabályzatnak megfelelő működését,
- pénzügyi szolgáltatási, illetve kiegészítő pénzügyi szolgáltatási tevékenységeit,
- mindazt, amit jogszabály a feladatkörébe utal.

7.5 Hiányosságok esetén végrehajtandó tevékenységek

A külső és belső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére a Szolgáltató intézkedési tervet készít, a hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A fentiekkel összhangban a belső ellenőrzés a Szolgáltató vezetése számára rendszeres visszacsatolást nyújt, hogy a vizsgált terület működése összhangban van-e a kitűzött üzleti célokkal, a jogszabályokkal, a belső utasításokkal, valamint annak hiányában a legjobb gyakorlattal. A vizsgálatok során a belső ellenőrzés az azonosított eltéréseket feltárja és javaslatokat tesz a hiányosságok kiküszöbölésére, a kockázatok csökkentésére a tevékenységért felelős terület vezetőjének. A belső ellenőrzés ellenőrzi és jelenti, hogy a vizsgálatok során definiált intézkedési tervek megfelelő módon és időben végrehajtásra kerültek-e.

7.6 Eredmény kommunikációja

A belső ellenőrzés minden vizsgálatot írásban dokumentál és bizalmasan kezel minden, az ellenőrzés során tudomására jutott adatot és információt. Az elkészített jelentéseket időben, a bizalmas információk terjesztésére vonatkozó szabályok figyelembe vételével megküldi az érintettek részére. Az audit megfelelő felhatalmazás nélkül a K&H Csoporton kívüli személyek számára nem küld információt, kivéve, ha azt jogi vagy szakmai kötelezettségek miatt kell megtenni. A Szolgáltató nem köteles az esetleg feltárt konkrét hiányosságot nyilvánosságra hozni.

8. Egyéb üzleti és jogi kérdések

8.1 Biztosítási fedezet

A Szolgáltató rendelkezik olyan felelősségbiztosítással, amely kiterjed a Szolgáltató által nyújtott bizalmi Szolgáltatással összefüggésben okozott alábbi károkra és költségekre:

a) a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,

b) a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,

c) az E-ügyintézési tv. 88. §-ában foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az E-ügyintézési tv. 89. §-a szerinti költségekre, és

d) az eIDAS Rendelet 17. cikk (4) bekezdés e) pontja alapján a bizalmi felügyelet által felkért megfelelőség értékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.

A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft.

8.2 Üzleti információk bizalmas kezelése

A Szolgáltató – az alábbi kivétellel – minden adatot és információt bizalmasan kezel.

Nem minősül bizalmasan kezelendő információnak:

- a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;
- az olyan adatok, melyek nyilvános adatforrásból elérhetők.

A Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított munkavállalói, esetlegesen megbízottjai számára teszi lehetővé. A bizalmas információk védelmét az érintett munkavállalók megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

8.3 Személyes adatok védelme

A Szolgáltató rendelkezik mind banki szintű adatvédelmi tájékoztatóval mely nyilvános dokumentum, és elérhető a Szolgáltató internetes honlapján. Ezen dokumentum magába foglalja a Szolgáltató által kezelt személyes adatok körét, az adatkezelés célját továbbá az érintettet megillető jogokat. A vonatkozó adatvédelmi tájékoztatók és szabályzatok a jelen szabályzat által lefedett témakörökben is alkalmazandóak.

Az adatkezelésre, adatvédelemre vonatkozó dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó adatvédelmi jogszabályokkal.

A Szolgáltató - mint adatkezelő - szerepel a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

8.4 Felelősség

A Szolgáltató felel a bizalmi szolgáltatási rendben és jelen Szolgáltatási Szabályzatban megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatás nyújtásához kapcsolódó egyes feladatokat kiszervezett tevékenység keretében harmadik személy végez.

A Szolgáltató Üzletszabályzata, így különösen annak felelősségre vonatkozó rendelkezései a Szolgáltatás vonatkozásában is alkalmazandó.

8.5 Díjak

Tekintettel arra, hogy a Szolgáltató a jelen Szolgáltatási Szabályzat szerinti bizalmi Szolgáltatás igénybevételét önmagában nem, csak bizonyos ügyletek tekintetében teszi lehetővé az ügyfelei számára, a bizalmi Szolgáltatás díja az ezen ügyletekre vonatkozó díjak részét képezi.

9. Módosítások

9.1 A Szolgáltatási Szabályzat módosítása

A Szolgáltatási Szabályzat módosítása az 1.4.3 és 1.4.4 fejezetekben leírt szabályok szerint történik. A Szolgáltatási Szabályzat módosulását a verziószám megfelelő változása jelzi.

A Szolgáltatási Szabályzat módosítása esetén a Szolgáltató a módosulás hatályba lépését megelőző 15 nappal közzéteszi internetes honlapján a módosult Szolgáltatási Szabályzatot oly módon, hogy az ügyfél számára megállapíthatóak legyenek a módosult rendelkezések.

9.2 Hatályosság és megszűnés

9.2.1 Hatályosság

Időbeli hatály

A Szolgáltatási Szabályzat egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik, és határozatlan időre szól. Az időbeli hatály megszűnik a Szolgáltatási Szabályzat újabb verziójának hatályba lépésével vagy amennyiben a Szolgáltató jövőre nézve beszünteti a jelen Szabályzat szerinti bizalmi Szolgáltatás nyújtását.

Tárgyi hatály

A jelen Szolgáltatási Szabályzat tárgyi hatálya kiterjed a 1.1. pontban körülírt Szolgáltatás nyújtására és igénybe vételére.

Személyi hatály

A Szolgáltatási Szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az ügyfélre, aki az online szerződéskötési felületen keresztül online módon kezdeményez szerződéskötést és köt szerződést a Szolgáltatóval a Szolgáltató által meghatározott ügyletek tekintetében.

9.2.2 Megszűnés

A Szolgáltatási Szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

A jelen Szolgáltatási Szabályzat szerinti szolgáltatási tevékenység megszűnése esetén

- szerződés megkötésének online módon történő kezdeményezésére és a szerződés elektronikus aláírással való ellátására nincs mód,
- a korábban megkötött szerződések a vonatkozó jogszabályok értelmében érvényesek,
- az ügyfélnek a Szolgáltató telephelyein (bankfiókban) van lehetősége a korábban megkötött szerződések papír alapú formátumban való kikérésére.

Amennyiben a Szolgáltató a jelen Szolgáltatási Szabályzat tárgyát képező szolgáltatási tevékenységével fel kíván hagyni, erről a döntéséről legkésőbb a tevékenység

megszüntetésekor értesíti az ügyfeleket és a Bizalmi Felügyeletet az E-ügyintézési törvény 88. § (1) bekezdésének megfelelően. Amennyiben a Szolgáltató ellen megszüntetési eljárás indult, a Szolgáltató haladéktalanul tájékoztatja a Bizalmi felügyeletet az E-ügyintézési törvény 89. § (4) bekezdésének megfelelően.

A Szolgáltató a jelen Szolgáltatási Szabályzat tárgyát képező szolgáltatási tevékenység beszüntetésekor teljekörű biztonsági mentést készít az informatikai rendszereiben foglalt, a jelen Szolgáltatási Szabályzat tárgyát képező szolgáltatási tevékenységgel összefüggő adatairól. A Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. A Szolgáltató biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek a BM rendelet 7. §-ának megfelelően.

Abban az esetben, ha a Szolgáltató a jelen Szolgáltatási Szabályzat tárgyát képező bizalmi szolgáltatási tevékenység nyújtását megszünteti,

- de a jelen Szabályzatban foglalt bizalmi szolgáltatási tevékenység nyújtásának megszüntetése után más bizalmi szolgáltatás nyújtását továbbra is folytatja: a Szolgáltató gondoskodik a jelen Szabályzat hatálya alá tartozó, megszüntetni kívánt bizalmi szolgáltatással összefüggő, a nyilvánosság számára elérhető nyilvántartásainak folyamatos elérhetőségéről, az E-ügyintézési törvény 88. § (2) bekezdésében foglaltaknak megfelelően;
- és a továbbiakban nem kíván bizalmi szolgáltatást nyújtani: a szolgáltatás megszüntetéséről az ügyfelek és a Bizalmi Felügyelet részére megküldött értesítésben megjelöli azt a bizalmi szolgáltatót, amely biztosítja a jelen szolgáltatási szabályzat hatálya alá tartozó, megszüntetni kívánt bizalmi szolgáltatással összefüggő, a nyilvánosság számára elérhető nyilvántartásaihoz való hozzáférést. Ebben az esetben a Szolgáltató gondoskodik a hozzáférési kötelezettség alá eső nyilvántartási adatok átvevő bizalmi szolgáltatónk történő átadásáról az E-ügyintézési törvény 88.§ (3) és (6) bekezdésének megfelelően.

Tekintettel arra, hogy a Szolgáltató nem bocsájt ki sem minősített, sem pedig nem minősített tanúsítványt (a fenti, 1.3 pontban kifejtettek szerint), ezért a kifejezetten a tanúsítványokhoz kapcsolódó, az E-ügyintézési törvény 88.§ és 89. §-ban előírt értesítési, adatátadási és egyéb kötelezettségek a Szolgáltatóra nem alkalmazandók.

9.3 Vitás ügyek rendezése

9.3.1 Általános szabályok

A Szolgáltató és ügyfelei a Szolgáltatással összefüggő vitáikat mindenkor megkísérlik békés úton – peren kívül – tárgyalások útján rendezni.

Az ügyfél a jelen Szabályzatban meghatározott Szolgáltatással összefüggő panasz vagy jogvita esetén az Ügyfél békéltető testülethez vagy az illetékes bírósághoz fordulhat.

9.3.2 Panaszkezelés

Az ügyfél jogosult panaszát szóban vagy írásban előterjeszteni.

Szóbeli panasz előterjeszthető az Szolgáltató bankfiókjaiban személyesen vagy meghatalmazott útján nyitvatartási időben, illetve telefonon a Szolgáltató telefonos ügyfélszolgálatain a következő telefonszámon: 06-(1/20/30/70)-335-3355-ös telefonszámon.

Írásbeli panasz a következő módokon terjeszthető elő:

a) Személyesen vagy más által átadott irat útján a Szolgáltató bármely bankfiókjában az ügyintézőhöz, fiókvezetőhöz nyújtható be, illetve a bankfiókban található formanyomtatvány kitöltésével tehető.

b) Postai úton bármelyik bankfióknak vagy a Szolgáltató központjának (K&H Bank 1851 Budapest) címezve.

c) Telefaxon a Szolgáltató központjának címezve, a Szolgáltató központi telefax számára 06-1-328-9696 küldhető.

Az írásbeli panasz benyújtásához formanyomtatványokat biztosít a Szolgáltató, amely a Szolgáltató honlapján (www.kh.hu) elérhető.

Az ügyfél eljárhat meghatalmazott útján is. Az ehhez szükséges meghatalmazás formanyomtatványa a Szolgáltató honlapján (https://www.kh.hu/panaszkezeles) elérhető.

A panaszkezelés részletes szabályai a Szolgáltató Panaszkezelési Szabályzatában kerültek meghatározásra, mely a Szolgáltató honlapján (https://www.kh.hu/panaszkezeles) elérhető.

9.3.3 Békéltető Testület

Felek jogosultak viták rendezése céljából békéltető testülethez fordulni.

A békéltető testület elérhetőségei:	
Név	Budapesti Békéltető Testület

Cím:	1016 Budapest, Krisztina krt. 99. III. em. 310.
Postai cím:	1253 Budapest, Pf.: 10.
Telefonszám:	06 (1) 488 21 31
Email cím:	bekelteto.testulet@bkik.hu
Internetes cím:	http://bekeltet.hu/

9.4 Jogi szabályozás

A Szolgáltató tevékenységét a mindenkor hatályos magyar és egyes Uniós jogszabályoknak megfelelően végzi. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

A legfontosabb jogszabályok:

- Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 470/2017 (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről
- 2013. évi V. törvény a Polgári Törvénykönyvről
- 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról
- 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

9.5 Jogszabályoknak való megfelelés

A Szolgáltató a saját mindenkori szabályzatainak megfelelően nyújtja Szolgáltatását, megfelelve a mindenkori magyar és Uniós jogszabályokban foglalt előírásoknak.

9.6 Vis maior

A "vis major" a Szolgáltató érdekkörén kívül álló olyan, előre nem látható eseményt jelent, amely a Szolgáltatással összefüggésben következik be, a Szolgáltatás ésszerű teljesítését akadályozza, a Szolgáltató ellenőrzésén kívülálló, általa elháríthatatlan. "Vis major" esetében a Szolgáltató haladéktalanul tájékoztatja ügyfeleit a vis maiorral összefüggő késedelem okairól.