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 Rend
elektronikus aláírás elhelyezéséhez

KH-BR-NMEA

Hatálybalépés dátuma: 2019. november 5.

Dokumentum verzió: v.6

A módosult részek sárga színnel kerülnek megjelölésre.

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

1.1 Áttekintés 6
1.2 Dokumentum neve és azonosítása 6
1.3 Tanúsítványok alkalmazhatósága 6
1.4 Szabályzat adminisztráció 7
1.4.1 Szabályzat karbantartása 7
1.4.2 Szolgáltató 7
1.4.3 Szolgáltatási Szabályzat felülvizsgálata 7
1.4.4 Szolgáltatási Szabályzat jóváhagyása 7
1.5 Bizalmi szolgáltatás és felügyelete 8
1.6 Rövidítések, hivatkozások 9
1.6.1 Rövidítések 9
1.6.2 Jogszabályi hivatkozások 11
1.6.3 Szabványok és műszaki-technikai specifikációk 12
1.6.4 A Szolgáltató egyéb szabályozó eszközei 12
2.1 Hitelesítéssel kapcsolatos információk közzététele 13
2.2 A tárolókhoz való hozzáférés ellenőrzése 13
3.1 Személyazonosság ellenőrzése 14
3.1.1 Az azonosítási folyamat 14
3.1.2 Az elektronikus aláírás létrehozásával kapcsolatos adatok kizárólagos kontrollja és bizalmas mivolta 14
4.1 Az elektronikus aláírás létrejöttének és elhelyezésének folyamata 15
5.1 Fizikai óvintézkedések 19
5.1.1 K&H adatközpont 19
5.1.2 O2 CZ felhőszolgáltató központ 19
5.2 Személyzeti szabályzatok 19
5.2.1 Bizalmi munkakörök 19
5.2.2 Egymást kizáró munkakörök 19
5.2.3 Képzettségre vonatkozó rendelkezések 19
5.2.4 Követelmények és korlátozások a K&H adatközpontban 20
5.2.5 Követelmények és korlátozások az O2 CZ felhőszolgáltató központban 20
5.3 Biztonsági naplózási folyamatok 20
5.3.1 Ellenőrzési naplózási események 20
5.3.2 Naplófájlok elemzése 20

5.3.3 Naplófájlok tárolásának ideje 20
5.3.4 Naplók központi gyűjtése 20
5.3.5 Naplófájlok védelme 20
5.3.6 Naplófájlok biztonsági mentése 21
6.1 Az elektronikus aláírások létrejötte – adatok generálása 22
6.1.1 Az elektronikus aláírások létrejötte, az elektronikus aláírás elemei, adatok eljuttatása az aláíróhoz 22
6.1.2 Az elektronikus aláírások létrejötte – adatméret 22
6.1.3 Az elektronikus aláírások létrejötte – adatok generálása és minőségellenőrzés 22
6.1.4 Az elektronikus aláírások létrehozása – az adatok felhasználásának céljai 22
6.2 Az elektronikus aláírások létrejötte – adatvédelem és a kriptográfiai modul vezérlő kontrolljai 23
6.2.1 A kriptográfiai modulra vonatkozó szabványok és kontrollok 23
6.2.2 Az egyazon elektronikus aláírás létrehozásához kapcsolódó adatok ismételt felhasználásának megakadályozására alkalmazott módszer 23
6.3 Az elektronikus aláírások létrehozása és kontrolljai 23
6.3.1 Hash az elektronikus aláíráshoz 23
6.3.2 Adatcsomagok felhasználása a tördeléshez 23
6.3.3 A kapcsolódó aláírt dokumentumok és hash-ek 23
6.3.4 Az elektronikus aláírás módosítását megakadályozó óvintézkedések 24
6.4 Archiválás és tárolás 24
6.5 Hálózatbiztonsági óvintézkedések 24
7.1 Vizsgálatok gyakorisága és körülményei 26
7.2 Auditor azonosítása és képesítése 26
7.3 Auditor függetlensége 27
7.4 Audit során vizsgált területek 27
7.5 Hiányosságok esetén végrehajtandó tevékenységek 27
7.6 Eredmény kommunikációja 28
8.1 Biztosítási fedezet 29
8.2 Üzleti információk bizalmas kezelése 29
8.3 Személyes adatok védelme 29
8.4 Felelősség 29
8.5 Díjak 29
9.1 A Szolgáltatási Rend módosítása 30
9.2 Hatályosság és megszűnés 30

9.2.1 Hatályosság 30
9.2.2 Megszűnés 30
9.3 Vitás ügyek rendezése 31
9.4 Jogi szabályozás 31
9.5 Jogszabályoknak való megfelelés 31
9.6 Vis maior 31

1. Bevezetés

1.1 Áttekintés

Jelen dokumentum a K&H Bank Zrt. (továbbiakban: „Szolgáltató") Bizalmi Szolgáltatási Rendje (a továbbiakban: „Szolgáltatási Rend" vagy „Rend"), 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 Rend 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 Bank rendszerébe integrált, speciálisan erre a célra kialakított informatikai szolgáltatás igénybe vételével köthetik meg a szerződéseket.

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 Rend teljes neve: **K&H Bank Zrt. Bizalmi Szolgáltatási Rend elektronikus aláírás elhelyezéséhez**.

A Szolgáltatási Rend objektum azonosítója és verziószáma a címlapon található.

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

Jelen Rend 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 Rendben 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 szolgáltatási Rend 6.2 és 6.3.4 fejezeteiben 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, 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 Szolgáltatónak a bizalmi szolgáltatási szabályzat karbantartását a belső szabályzatai szerint felül kell vizsgálnia**.**

1.4.2 Szolgáltató

Az Ügyfélkapcsolati Iroda elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

1.4.3 Szolgáltatási Szabályzat felülvizsgálata

A Szolgáltatónak legalább évente egyszer meg kell vizsgálnia a Szolgáltatási Rend, illetve a bizalmi szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek alapján megfelelően módosítani azokat.

1.4.4 Szolgáltatási Szabályzat jóváhagyása

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

A jóváhagyás előtt a Szolgáltatónak meg kell vizsgálnia a szolgáltatási szabályzat 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 Rend új verziójának mindig új verziószámmal kell nyilvánosságra és közzétételre kerülnie a 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, a jelen Rend 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.

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, hivatkozások

Jelen Rendben használt fogalmak értelmezése megegyezik a Szolgáltatásra vonatkozó jogszabályokban szereplő meghatározásokkal.

1.6.1 Rövidítések

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 Rend 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	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
- 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 Szolgáltatónak a jelen Rend szerinti Szolgáltatást kizárólag a releváns üzleti folyamatai során nyújthatja, az érintett fokozott biztonságú elektronikus aláírást 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) köteles közzétenni, míg az egyéb közérdekű szolgáltatói információkat a kh.hu weboldalon köteles közzétenni.

2.2 A tárolókhoz való hozzáférés ellenőrzése

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

3. A személyazonosság ellenőrzésének folyamata

Ahogyan azt a jelen Szolgáltatási Rend 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

A Szolgáltatónak a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényben („Pmt.") meghatározott ügyfél-átvilágítási kötelezettségének teljesítése érdekében azonosítania kell az ügyfelet a Pmt. szerinti auditált elektronikus hírközlő eszköz útján. A Szolgáltatónak a szolgáltatási szabályzatban részletesen ismertetnie kell a valós idejű ügyfél-átvilágítás egyes lépéseit illetve a további validációs célt szolgáló ellenőrzéseket.

3.1.2 Az 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 Szolgáltatónak a belsőleg tárolt MicroTRX kódok jogosulatlan hozzáférés elleni védelméhez a jelenleg rendelkezésre álló minden ésszerű technológiát és folyamatmegoldást fel kell használnia.

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

A Szolgáltató a szerződéskötést megelőzően köteles elvégezni a szolgáltatást használni szándékozó ügyfelek azonosítását. A Szolgáltató az ügyfél azonosítási folyamat lefolytatásához valamint az elektronikus aláírás ügyfelek általi létrehozásának és a Szolgáltató általi elhelyezésének biztosítása céljából köteles egy erre alkalmas online felületet működtetni. Az online felület ügyfelek általi használatának módjáról, a Szolgáltató a szolgáltatási szabályzatban köteles rendelkezni. A Szolgáltató az ügyfél vonatkozó hozzájárulása birtokában, köteles ellenőrizni az ügyfél földrajzi lokációját, IP cím alapján.

A Szolgáltató a szolgáltatási szabályzatban köteles rendelkezni arról, hogy mely ügyfelek jogosultak az online rendszeren keresztül történő szerződés megkötésére és így az elektronikus aláírás elkészítésére.

Az ügyfél és az általa használt kommunikációs csatornák ellenőrzése: A Szolgáltató a szolgáltatási szabályzatban köteles rendelkezni arról, hogy miként ellenőrzi az ügyfél által használt kommunikációs csatornákat. A Szolgáltató köteles egy-egy - véletlenszerűen generált, egyedi (azaz tranzakciónként eltérő) öt számjegyű, betűt vagy speciális karaktert nem tartalmazó, - kódot küldeni az ügyfélnek, az ügyfél által megadott telefonszámra illetve email címre (a továbbiakban: „SMS-kód” és „Email-kód”). Mindkét kódot titkosított módon, ún. pszeudorandom generátorral kell előállítani. 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 Szolgáltatónak kell ellenőriznie.

Az ügyfél személyazonosságának ellenőrzése: A Szolgáltató köteles a szolgáltatási szabályzatban rendelkezni az ügyfélazonosítás egyes lépéseiről, az ügyfélazonosítás módjáról. Az ügyfélazonosítást a Szolgáltató minden esetben a Pmt. valamint a végrehajtására kiadott MNB rendelet rendelkezéseivel összhangban köteles elvégezni, előzetesen auditált elektronikus hírközlő eszköz útján, amelynek a gyakorlatban egy élő, video-csatornán történő azonosítást kell jelentenie. A video-azonosítás egyik lépéseként az ügyfél köteles az ügyintézőnek bemutatni személyazonosító igazolványát valamint a lakcímkártyáját. A Szolgáltató IT rendszereinek ellenőrizniük kell az igazolvány és lakcímkártya számát, továbbá a Szolgáltató IT rendszereinek a kártya érvényességének valamint az adatok egyezőségének ellenőrzése céljából hatósági adatszolgáltatótól, a GIRO Zrt. GIRinfO szolgáltatásának igénybe vételével, le kell kérniük a szükséges ügyféladatokat**.**

A szerződéskötési folyamat leírása a végső ajánlatig:

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

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

A MicroTRX kód generálásának, az ügyfél részére történő rendelkezésre bocsátásának, valamint használatának teljes mértékben az eIDAS 26. cikkében foglalt követelményekkel összhangban kell történnie. A Szolgáltató e körben köteles felhívni 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 köteles automatikusan ellenőrizni, hogy a bankszámla számlatulajdonosa azonos-e az eljáró ügyféllel. A Szolgáltató kizárólag olyan ügyféllel köthet szerződést, aki a személyazonosítási eljáráson átesett és a Szolgáltató által ügyfélkénti befogadása megtörtént.

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

A végleges ajánlat (Aláírt DOC1) elkészítése és az ügyfél rendelkezésére bocsátása: Szolgáltató köteles a DOC1-et minősített elektronikus bélyegző tanúsítvánnyal (PAdES-T) és időbélyegzővel ellátnia, létrehozva így a végleges ajánlatot („**Aláírt DOC1**"). A Szolgáltatónak az ügyfél rendelkezésére kell bocsátania 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 rendszereinek ellenőrizniük kell az elküldött és a beírt kódok egyezőségét.

Ezt követően a Szolgáltató rendszerének SHA-256 algoritmussal egy hash-t kell készítenie, 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 rendszerének az (Aláírt) DOC1 adatai alapján automatikusan létre kell hoznia egy új dokumentumot („**DOC2**"), amely tartalmát tekintve mindenben meg kell, hogy egyezzen a DOC1-gyel, kivéve, hogy a létrehozásakor már azonnal és automatikusan tartalmaznia kell a MicroTRX kódot is.

DOC1 és a DOC2 tartalma, - az aláíráskor a dokumentumhoz rendelt aláírási adatokat leszámítva, - meg kell, hogy egyezzen, és annak a későbbiekben bármely esetleges változásának nyomon követhetőnek és azonosíthatónak kell lennie. A Szolgáltató a szolgáltatási szabályzatban köteles rendelkeznie arról, hogy milyen módon biztosítja DOC1 és a DOC2 tartalmának egyezőségét, valamint az esetleges változások nyomon követhetőségét és azonosíthatóságát.

DOC2-t a Szolgáltató rendszerének a létrehozását követően azonnal minősített elektronikus bélyegző tanúsítvánnyal és időbélyegzővel kell ellátnia. Ez egyrészt az ügyfél által aláírt példány Szolgáltató általi aláírását jelenti, másrészt biztonságosan „lezárja" a mindkét fél által aláírt dokumentumot („**Aláírt DOC2**"). A teljes folyamatnak automatizáltnak, zártnak és a Szolgáltató IT rendszereiben naplózottnak kell lennie. Ebből következően az online folyamat során elkészített és mindkét fél által aláírt szerződés technikai szempontú módosítására nem lehet lehetőség.

Ezzel párhuzamosan a Szolgáltató rendszerének SHA 256 algoritmussal egy második hash-t is kell készítenie, amelynek tartalmaznia kell 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 el kell elkészítenie egy további dokumentumot, amely olvasható formában tartalmazza a HSH2-t („**DOC 3**”).

A Szolgáltató köteles minősített elektronikus bélyegző tanúsítvánnyal (PAdES-T) és időbélyeggel ellátni a DOC 3-at, majd azt az ügyfél rendelkezésére bocsátani.

A Szolgáltatónak a szolgáltatási szabályzatban rendelkeznie kell arról, hogy a DOC3 milyen módon szolgál bizonyítékul az ügyfél számára az aláírás megtörténtéről.

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

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 területén működő biztonsági rendszerek illetve az alkalmazott egyéb fizikai óvintézkedések részletes leírását a szolgáltatási szabályzat tartalmazza.

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 Szolgáltatónak be kell tartania a szolgáltatási szabályzatban leírt intézkedéseket az adatok védelme és a fizikai biztonság fenntartása érdekében.

5.2 Személyzeti szabályzatok

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatás biztonsága függ. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. A bizalmi munkakört betöltő személyekre vonatkozó részletes szabályokat a Szolgáltató szolgáltatási szabályzatának kell meghatároznia.

5.2.2 Egymást kizáró munkakörök

Szolgáltatónak biztosítania kell, 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

A Szolgáltató köteles kellő számú, a szolgáltatás nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező munkavállalókat alkalmazni.

A Szolgáltató köteles garantálni, 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.

A Szolgáltatónál bizalmi munkakört betöltő személyek képzettségére, szakmai továbbképzésére vonatkozó részletes szabályokat a szolgáltatási szabályzatban határozza meg.

5.2.4 Követelmények és korlátozások a K&H adatközpontban

A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell az alkalmazott biztonsági előírásokat, kitérve a beléptetési protokollra, a biztonsági zónákra illetve a berendezések minőségére.

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, 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. A Szolgáltatónak az egyes naplókra vonatkozó részletes szabályokat a szolgáltatási szabályzatban kell meghatároznia.

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 naplófájloknak a szerverről időszakonként átmásolásra kell kerülniük 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 Szolgáltatónak el kell végeznie a szükséges biztonsági mentéseket továbbá be kell tartania a tárolásra vonatkozó kritériumokat a szolgáltatási szabályzatban meghatározott módon.

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, 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 az ügyfél által a kérelemben megadott számlára.

Az ügyfélnek a folyamat végén meg kell adnia a MicroTRX kódot a szerződés aláírásához (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), amelyet egy titkosítással biztosított, pszeudorandom generátor hoz 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 aláírást. 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 létrehozása – az adatok felhasználásának céljai

Az ügyfélnek a folyamat végén meg kell adnia a MicroTRX kódot a szerződés aláírásához (a részleteket lásd a 3.1.2 fejezetben).

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 Szolgáltatónak ismertetnie kell a szolgáltatási szabályzatban a MicroTRX kód generálására és egyediségére vonatkozó technikai részleteket.

6.3 Az elektronikus aláírások létrehozása és kontrolljai

Az ügyfél elektronikus aláírása egy az online szerződéskötési folyamat során generált lenyomat, amely tartalmazza 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 sérthetetlenségét.

6.3.2 Adatcsomagok felhasználása a tördeléshez

Az adatcsomagok (datagram) biztonságos módon kerülnek létrehozásra a rendszerben az aláírási folyamat során. A Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia az adatcsomagok tartalmát.

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. A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a hash-ek tulajdonságait.

6.4 Archiválás és tárolás

A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a lementett dokumentumokat valamint a mentés technikai részleteit, abban az esetben, ha az ügyfél végig viszi a szerződéskötés teljes folyamatát.

A jogszabályi követelményeknek megfelelően az online szerződéskötési folyamat során keletkező dokumentumokat a Szolgáltató köteles dokumentum kezelő rendszerébe megfelelően kategorizáltan lementeni. A Szolgáltató köteles az adott dokumentumkategóriák alapján a dokumentumokat a megfelelő banki eljárások alapján kerülnek archiválni, illetve a jogszabályok által meghatározott tárolási idő elteltével azokat fizikailag is törölni.

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

Tekintettel arra, hogy a Szolgáltató nem nyújt minősített bizalmi szolgáltatást, illetve, hogy a jelen Szolgáltatási Rend szerinti Szolgáltatás keretében nem kerül sor tanúsítvány kibocsátásra, az E-ügyintézési tv. 84. § szerinti 10 éves megőrzési időt nem általánosan, csak a jelen Szolgáltatási Rend és a szolgáltatási szabályzat 5.3. pontjában körülírt napló-komponensek esetén köteles alkalmazni.

6.5 Hálózatbiztonsági óvintézkedések

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

A Szolgáltatónak gondoskodnia kell arról, hogy a Szolgáltatást nyújtó informatikai rendszerében megfelelő hálózatbiztonsági ellenőrzésekre kerüljön 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 Szolgáltatónak a szolgáltatási szabályzatban részletesen ismertetnie kell a hálózatbiztonságot megvalósító biztonsági funkciókat.

7. Megfelelőség vizsgálat és egyéb értékelések

A Szolgáltató a jelen Szolgáltatási Rend által érintett bizalmi Szolgáltatást az irányadó jogszabályok valamint a jelen Szolgáltatási Rend és a szolgáltatási szabályzat 1.6.3. pontjában megjelölt szabványok és műszaki-technikai specifikációk alapján köteles végezni.

A Szolgáltató köteles külső és belső vizsgálatokat és ellenőrzéseket végezni, illetve elvégeztetni 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 a közvetlenül a felügyeleti jogkörrel rendelkező vezető testület irányítása alatt álló belső ellenőrzési szervezeti egységet kell működtetnie. A Hpt. 154. § (12) cikke bekezdése értelmében a belső ellenőrzési funkció szervezetét, hatáskörét, feladatait és eljárásrendjét évente felülvizsgálandó belső ellenőrzési szabályzatban hivatalosan köteles rögzíteni.

7.1 Vizsgálatok gyakorisága és körülményei

A belső ellenőrzési szervezeti egységnek az egyes banki tevékenységek és folyamatok kockázata alapján éves audit tervet kell összeállítania. 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**.**

A Szolgáltató vizsgálatának gyakorisága és körülményei meg kell, hogy feleljenek a hatályos jogszabályi előírásoknak.

7.2 Auditor azonosítása és képesítése

A Szolgáltató köteles a tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket végeztetni, a szolgáltatási szabályzat 7.2 pontjában meghatározottak szerint. A belső ellenőröknek igazoltan rendelkezniük kell feladatkörüknek megfelelő szakértelemmel és tapasztalattal, továbbképzésük a belső szabályzatban rögzített kereteknek megfelelően folyamatos.

A külső megfelelőségértékeléseket olyan természetes vagy jogi személyeknek (vagy ezek csoportjának) kell elvégezni, akik a megfelelőségértékelés elvégzéséhez megfelelő felhatalmazással rendelkeznek, képesek a Szolgáltató által végzett Szolgáltatásra irányadó szabványok vonatkozásában az audit elvégzésére (ideértve azt is, hogy rendelkezik a szükséges akkreditációval), és megfelelnek a jogszabályok és a szolgáltatási szabályzat által támasztott függetlenségi követelményeknek.

7.3 Auditor függetlensége

A külső megfelelőségértékeléseket olyan értékelő végezheti, aki vagy amely a Szolgáltató tulajdonosi körétől, vezetőségétől, üzemeltetésétől független.

A belső ellenőrzésnek 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 kell végeznie 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 területeket kell vizsgálnia és ellenőriznie:

- a hatályos, vonatkozó jogszabályoknak illetve műszaki szabványoknak való megfelelés;
- Bizalmi Szolgáltatási Rendnek és a 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 teljesülését kell értékelnie.

A fentieken túlmenően, a Szolgáltatónak a szolgáltatási szabályzatban részleteznie kell a Hpt. 154. § (2) bekezdésének megfelelően a belső ellenőrzési rendszer működtetésének célját és feltételeit.

7.5 Hiányosságok esetén végrehajtandó tevékenységek

A külső és belső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére a Szolgáltatónak intézkedési tervet kell készítenie, a hiányosságokat késlekedés nélkül orvosolnia kell, valamint dokumentálnia és ellenőriznie kell az intézkedéseket.

A fentiekkel összhangban a belső ellenőrzésnek a Szolgáltató vezetése számára rendszeres visszacsatolást kell nyújtani, 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 ellenőrzésnek az azonosított eltéréseket fel kell tárnia és javaslatokat kell tennie a hiányosságok kiküszöbölésére, a kockázatok csökkentésére a tevékenységért felelős terület vezetőjének. A belső ellenőrzésnek ellenőriznie és jelentenie kell, hogy a vizsgálatok során definiált intézkedési tervek megfelelő módon és időben végrehajtásra kerültek-e.

7.6 Eredmény kommunikációja

A belső ellenőrzésnek minden vizsgálatot írásban kell dokumentálnia és bizalmasan kell kezelnie minden, az ellenőrzés során tudomására jutott adatot és információt. Az elkészített jelentéseket időben, a bizalmas információk terjesztésére vonatkozó szabályok figyelembe vételével meg kell küldenie 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.

8. Egyéb üzleti és jogi kérdések

8.1 Biztosítási fedezet

A Szolgáltatónak rendelkeznie kell olyan felelősségbiztosítással, amely kiterjed a Szolgáltató által nyújtott bizalmi Szolgáltatással összefüggésben okozott károkra és költségekre. A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a károkat továbbá meg kell adnia a felelősségvállalási értéket.

8.2 Üzleti információk bizalmas kezelése

A Szolgáltatónak a szolgáltatási szabályzatban meg kell határoznia azokat az információkat, amelyek nem minősülnek bizalmasan kezelendőnek. Ezek kivételével minden adatot és információt bizalmasan kell kezelnie.

8.3 Személyes adatok védelme

A Szolgáltató rendelkezik 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 rend által lefedett témakörökben is alkalmazandóak.

Az adatkezelésre, adatvédelemre vonatkozó dokumentumoknak összhang kell lenniük a nemzetközi és hazai vonatkozó adatvédelmi jogszabályokkal.

A Szolgáltatónak - mint adatkezelőnek, szerepelnie kell a Nemzeti Adatvédelmi és Információszabadság Hivatal Adatvédelmi Nyilvántartásában.

8.4 Felelősség

A Szolgáltatónak felelnie kell a bizalmi szolgáltatási szabályzatban és jelen Szolgáltatási Rendben 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

A Szolgáltatónak a szolgáltatási szabályzatban kell rendelkeznie a bizalmi Szolgáltatás díjáról.

9. Módosítások

9.1 A Szolgáltatási Rend módosítása

A Szolgáltatási Rend módosítására az 1.4.3. és 1.4.4 fejezetekben leírtak megfelelően alkalmazandók. A Szolgáltatási Rend módosulását a verziószám megfelelő változása jelzi.

A Szolgáltatási Rend módosítása esetén a Szolgáltatónak a módosulás hatályba lépését megelőző 15 nappal közzé kell tennie internetes honlapján a módosult Szolgáltatási Rendet oly módon, hogy az ügyfél számára megállapíthatóak legyenek a módosult rendelkezések.

9.2 Hatályosság és megszűnés

9.2.1 Hatályosság

Időbeli hatály

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

Tárgyi hatály

A jelen Szolgáltatási Rend tárgyi hatálya az 1.1. pontban körülírt Szolgáltatás nyújtására és igénybe vételére terjed ki.

Személyi hatály

A Szolgáltatási Rend személyi hatálya kiterjed Szolgáltatónak a szolgáltatások 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.

A Szolgáltatónak meg kell adnia a szolgáltatási szabályzatban a szolgáltatási szabályzat időbeli, tárgyi és személyi hatályára vonatkozó részletes kritériumokat.

9.2.2 Megszűnés

A Szolgáltatási Rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek. A Szolgáltató szolgáltatási szabályzata tartalmazza a tevékenység megszűnése esetén alkalmazandó eljárásrendre vonatkozó szabályokat. A szolgáltatási tevékenység megszűnése esetén a Szolgáltatónak teljes körűen eleget kell tennie a mindenkor hatályos jogszabályokban foglalt kötelezettségeinek. A Szolgáltató köteles a szolgáltatási szabályzatban rendelkezni arról, hogy a szolgáltatási tevékenység megszűnésével összefüggésben a mindenkor hatályos jogszabályokban foglaltaknak eleget tesz.

9.3 Vitás ügyek rendezése

A Szolgáltatónak és ügyfeleinek a Szolgáltatással összefüggő vitáikat mindenkor meg kell kísérelni békés úton – peren kívül – tárgyalások útján rendezni.

Bizalmi szolgáltatással összefüggő panasz vagy jogvita esetén az ügyfél békéltető testülethez vagy bírósághoz fordulhat.

Felek jogosultak viták rendezése céljából békéltető testülethez fordulni, melynek részleteit a szolgáltatási szabályzat tartalmazza.

9.4 Jogi szabályozás

A Szolgáltatónak tevékenységét a mindenkor hatályos magyar és egyes Uniós jogszabályoknak megfelelően kell végeznie. A Szolgáltató szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők. A legfontosabb jogszabályokat a szolgáltatási szabályzatban kell ismertetni.

9.5 Jogszabályoknak való megfelelés

A Szolgáltatónak a saját mindenkori szabályzatainak megfelelően kell nyújtania a 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 Szolgáltatónak haladéktalanul tájékoztatnia kell ügyfeleit a vis maiorral összefüggő késedelem okairól.