A FaceKom Kft.
Bizalmi Szolgáltatási Szabályzata
elektronikus aláírás elhelyezéséhez

Verzió	v20240901
Információvédelmi besorolás	Publikus
Kiadás dátuma	2024.09.01
Ellenőrizte	Erdélyi Gábor biztonsági tisztviselő Csordás Sándor informatikai rendszerért általánosan felelős vezető
Jóváhagyta	Gyenese Péter ügyvezető Dr. Csege Gyula ügyvezető
Jóváhagyók aláírása	Elektronikusan aláírta: Gyenese Péter Elektronikusan aláírta: Dr. Csege Gyula
Hatályos mellékletek	
Kapcsolódó dokumentumok	
-	

Dokumentumtörténet

Verzió	Készítette	Dátum	Típus	Megjegyzés
v0	Tóth Gábor	2019.01.31	Első verzió	
v.1	Tóth Gábor	2019.10.24	Felülvizsgálat	
v2	Tóth Gábor	2019.11.11	Felülvizsgálat	
v2.1	Tóth Gábor	2021.11.22	Felülvizsgálat	Az elektronikus úton kötött szerződések esetén az ügyfél aláírásának helyén megjelenő szöveg az ügyfél nevére módosul.
v.3	Tóth Gábor, Kiss Szilárd	2022.04.26	Felülvizsgálat	Cégnév változás miatti módosítások átvezetése
v3.1	Tóth Gábor, Kiss Szilárd	2022.10.24	Felülvizsgálat	FaceKom Kft. új székhelyének átvezetése, Békéltető testület adatváltozásainak átvezetése
v20240901	Nagy Zoltán, Dr Nagy András	2024.09.01.	Felülvizsgálat	Jogszabály változások átvezetése

Tartalomjegyzék

Tartalomjegyzék

1. Bevezetés ... 6
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 ... 7
1.6 Rövidítések, definíciók hivatkozások ... 8
1.6.1 Rövidítések, definíciók ... 8
1.6.2 Jogszabályi hivatkozások ... 9
1.6.3 Szabványok és műszaki-technikai specifikációk ... 10
1.6.4 A Szolgáltató egyéb szabályozó eszközei ... 10
2. Közzététel és tároló ... 10
2.1 Hitelesítéssel kapcsolatos információk közzététele ... 10
2.2 A tárolókhoz való hozzáférés ellenőrzése ... 11
3. A személyazonosság ellenőrzésének folyamata ... 11
3.1 Személyazonosság ellenőrzése ... 11
3.1.1 Az azonosítási folyamat ... 11
4. Az elektronikus aláírás létrejöttének és elhelyezésének folyamata ... 11
4.1 A Szolgáltató és Partner kapcsolata ... 11
4.2. Szolgáltató és az Ügyfél kapcsolata ... 12
4.3. Személyazonosság ellenőrzése ... 12
4.4. Elektronikus aláírás létrejöttének és elhelyezésének folyamata ... 12
4.5. Ügyfél oldali aláírás ... 13
4.5.1. Az aláírási folyamat során alkalmazott időbélyegekről ... 13
4.5.2. Első fázis: M1 - Első üzenet lépései ... 13
4.5.3. Második fázis: Kétfaktoros autentikáció lépései ... 14
4.5.4. Harmadik fázis: M2 - Második üzenet ... 15

4.5.5. Negyedik fázis - Aláírás ellenőrzése ... 17
4.5.6. Ötödik fázis - Szolgáltató általi véglegesítés ... 17
4.6. eIDAS megfelelés ... 18
5.1 Fizikai óvintézkedések ... 19
5.1.1 FaceKom adatközpont ... 19
5.2 Személyzeti szabályzatok ... 19
5.2.1 Bizalmi munkakörök ... 19
5.2.2 Egymást kizáró munkakörök ... 20
5.2.3 Képzettségre vonatkozó rendelkezések ... 20
5.3 Biztonsági naplózási folyamatok ... 21
5.3.1 Ellenőrzési naplózási események ... 21
5.3.2 Naplófájlok elemzése ... 21
5.3.3 Naplófájlok tárolásának ideje ... 21
5.3.4 Naplók központi gyűjtése ... 21
5.3.5 Naplófájlok védelme ... 21
5.3.6 Naplófájlok biztonsági mentése ... 21
6. Technikai biztonsági kontrollok ... 21
6.1 Az elektronikus aláírások létrejötte – adatok generálása ... 21
6.1.1 Archiválás és tárolás ... 21
6.4 Archiválás és tárolás ... 21
6.5 Hálózatbiztonsági óvintézkedések ... 22
7. Megfelelőség vizsgálat és egyéb értékelések ... 22
8. Egyéb üzleti és jogi kérdések ... 23
8.1 Biztosítási fedezet ... 23
8.2 Üzleti információk bizalmas kezelése ... 23
8.3 Személyes adatok védelme ... 23
8.4 Felelősség ... 24
8.5 Díjak ... 24
9. Módosítások ... 24
9.1 A Szolgáltatási Szabályzat módosítása ... 24
9.2 Hatályosság és megszűnés ... 24
9.2.1 Hatályosság Időbeli hatály ... 24
9.2.2 Megszűnés ... 24
9.3 Vitás ügyek rendezése ... 25
9.3.1 Általános szabályok ... 26
9.3.2 Panaszkezelés ... 26

9.3.3 Békéltető Testület 26
9.4 Jogi szabályozás 26
9.5 Jogszabályoknak való megfelelés 27
9.6 Vis maior 27

1. Bevezetés

1.1 Áttekintés

Jelen dokumentum a FaceKom Kft. (továbbiakban: „Szolgáltató”) Bizalmi Szolgáltatási Szabályzata (a továbbiakban: „Szolgáltatási Szabályzat” vagy „Szabályzat”), amely a Szolgáltatónak az eIDAS2 1 . cikk 3. d) 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.

Partner alatt értjük a szolgáltatóval szerződésben álló pénzügyi vállalkozást, pénzforgalmi intézményt, elektronikuspénz-kibocsátó intézményt, aki az Ügyfelei számára felkínálja a Szolgáltatást.

A Szolgáltató a Szolgáltatást az Ügyfele részére csak és kizárólag olyan dokumentumokhoz nyújtja, amelyet a Partnere Ügyfele részére felkínált aláírásra.

Az Ügyfelek a Partner rendszerébe integrált, speciálisan erre a célra kialakított informatikai szolgáltatás igénybe vételével köthetik meg a szerződéseiket.

A pénzügyi szolgáltatásokra vonatkozóan a Szolgáltató felelősséggel nem tartozik.

1.2 Dokumentum neve és azonosítása

Jelen Szolgáltatási Szabályzat teljes neve: FaceKom Kft. 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 2023. évi CIII. törvény - a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáptv.) , 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 (továbbiakban: eIDAS), AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1183 RENDELETE (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról (továbbiakban: eIDAS2) 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.

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:	FaceKom Kft.
Cégjegyzékszám:	01-09-962028
Székhely:	1052 Budapest, Deák Ferenc tér 3.
Internetes cím:	https://bizalmiszolgaltatas.facekom.net
Adatvédelem:	https://bizalmiszolgaltatas.facekom.net

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, a jelen Rend keretein belül:
Az eIDAS2 rendelet 1. cikk 3. d) 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 Partner által nyújtott pénzügyi szolgáltatások felügyelete nem tartozik a Bizalmi Felügyelet hatáskörébe, azok felügyelete tekintetében a Magyar Nemzeti Bank rendelkezik hatáskörrel, továbbá a pénzügyi szolgáltatások nem tartoznak a Szolgáltató hatáskörébe, azokra vonatkozóan a Szolgáltató a felelősségét kizárja.

Szolgáltató a Szolgáltatást 2019.01.31-én jelentette be a Bizalmi Felügyeletnek, mint nem minősített bizalmi szolgáltató.
A Bizalmi Felügyelet 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 Dokumentum	az a Dokumentum, amelyen az Ügyfél elektronikus aláírása elhelyezésre került.
Aláírási Folyamat	Az Ügyfél, az Applikáció és a Szolgáltató között létrejövő titkosított kommunikáció összessége, amely az elektronikus aláírás elhelyezéséhez szükséges.
Aláírási Csomag	Az Ügyfél általi elektronikus aláírási folyamatot reprezentáló adatcsomag amely tartalmazza az aláírási folyamat összes releváns lépésének egyértelműen megfeleltethető, az Alkalmazás és a Szolgáltató között zajlott, a teljes aláírási folyamatra kiterjedő kommunikációt és köztes adatállományt, többek között a Felkínált Dokumentumot, az Aláírt Dokumentumot, az aláírási folyamat közben időbélyegeket úgy, hogy ezek alapján az elektronikus aláírás létrejöttének és elhelyezésének a folyamata, a Dokumentumok tartalmi egyezősége egyértelműen és hitelt érdemlően ellenőrizhető.

Applikáció	az aláírás létrejöttének és elhelyezésének idejére az Ügyfél birtokában lévő informatikai eszközön futtatott alkalmazás (akár mobiltelefon alkalmazás akár böngészős weboldal formájában)
Dokumentum	PDF formátumú fájl vagy fájlok összessége.
Partner	a szolgáltatóval szerződésben álló pénzügyi vállalkozás, pénzforgalmi intézmény, elektronikuspénz-kibocsátó intézmény, aki az Ügyfelek számára felkínálja a Szolgáltatást.
Ügyfél	az a természetes személy, aki igénybe veszi a Szolgáltatást
Szolgáltatás	eIDAS szerinti fokozott biztonságú elektronikus aláírás elhelyezése
Szolgáltató	FaceKom Kft. mint nem minősített bizalmi szolgáltató
eIDAS	910/2014/EU rendelet
eIDAS	Az Európai Parlament és a Tanács (EU) 2024/1183 rendelete
pAdES-T	(PDF Advanced Electronic Signatures) PDF dokumentumok aláírásának típusa; ld. ISO 32000-1
PDF	(Portable document format) Adobe Systems, Inc. dokumentum-formátum szabványa

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)
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1183 RENDELETE (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáptv.) 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)
- 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

- 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről
- 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

- Adatvédelmi tájékoztató
- Elektronikus azonosítású szolgáltatások általános szerződési feltételei

2. Közzététel és tároló

2.1 Hitelesítéssel kapcsolatos információk közzététele

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 https://bizalmiszolgaltatas.facekom.net című weblapján (továbbiakban: Szolgáltatás honlapja) teszi közzé.

A Szolgáltató weboldalának folyamatos működése és rendelkezésre állása biztosítja, hogy az ügyfelek részére a Szolgáltató nyilvános szabályzatai folyamatosan hozzáférhetőek legyenek. A Szolgáltató nyilvános szabályzatait saját minősített bélyegzőjével és külső, regisztrált, minősített bizalmi szolgáltatótól származó időbélyegzővel látja el, így biztosítva annak teljeskörűségét és sértetlenségét.

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 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

A Partner a saját rendszerében végrehajtja a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvényben („Pmt.”) meghatározott ügyfél-átvilágítási intézkedéseket az általa üzemeltetett - általában FaceKom VideoChat típusú - auditált elektronikus hírközlő eszközzel. Amennyiben az ügyfél-átvilágítási intézkedés sikeres volt, úgy a Partner a Szolgáltató informatikai integrációján keresztül, biztonságos csatornán a Szolgáltató informatikai rendszerébe átadásra kerülnek a következő információk:

- Ügyfél személyazonosság igazolására használt hatósági igazolványban foglalt adatai, az igazolvány érvényességi ideje és száma,
- Az ügyfél-átvilágítás adatai és az ügyfél-átvilágítás eredménye,
- Ügyfél azonosítására használt adata (felhasználóneve) a Partner informatikai rendszerében,
- Ügyfél második faktoros azonosításra használt az ügyfél-átvilágítás alatt validált csatornájának azonosítója (telefonszám).

4. Az elektronikus aláírás létrejöttének és elhelyezésének folyamata

4.1 A Szolgáltató és Partner kapcsolata

A Szolgáltató az Ügyfél személyazonosságának ellenőrzésére a Partner, mint harmadik fél által végzett 29/20 24. MNB rendeletnek megfelelő, pozitív eredménnyel zárult ügyfél-átvilágítását fogadja el és veszi át. Melynek része a személyazonosító okmányok Pmt. szerinti ellenőrzése, illetve az abban foglalt adatok rögzítése és adatigénylésre jogosult nyilvántartás alapján való ellenőrzése.

A Partner által elvárt, hogy feleljen meg a következő rendeleteknek, jogszabályoknak:

- 42/2015. (III.12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
  29/2024. (VI. 24.) MNB rendelet a Magyar Nemzeti Bank által felügyelt szolgáltatók által alkalmazott auditált elektronikus hírközlő eszköz és működtetésének, belső szabályozása minimumkövetelményeinek, auditálása módjának, valamint az ilyen eszköz útján végzett elektronikus ügyfél-átvilágítás végrehajtásának részletszabályairól

4.2. Szolgáltató és az Ügyfél kapcsolata

A Szolgáltatás igénybevételéhez az Ügyfélnek a Szolgáltató rendszerébe történő belépését követően - a bizalmi szolgáltatás megkezdését megelőzően - a visszakereshetőség biztosításával el kell fogadnia a következőket:

- Az aktuális Általános Szerződési Feltételeket
- Az aktuális Adatkezelési Tájékoztatót
- Az aktuális Bizalmi Szolgáltatási Rend-et.

Ezen nyilatkozatok megtételével az Ügyfél a Szolgáltatóval szolgáltatási szerződést köt bizalmi szolgáltatás nyújtására. A Szolgáltató bizalmi szolgáltatást képviseletet ellátó személynek nem nyújt.

4.3. Személyazonosság ellenőrzése

A Partner a saját rendszerében elvégzi a MNB szerinti ügyfél-átvilágítást. Sikeres azonosítás esetén az informatikai integráción keresztül, biztonságos csatornán a Szolgáltató informatikai rendszerébe átadásra kerülnek a következő információk:

- Ügyfél személyazonosság igazolására használt hatósági igazolványban foglalt adatai, az igazolvány érvényességi ideje és száma,
- Az ügyfél-átvilágítás adatai és az ügyfél-átvilágítás eredménye,
- Ügyfél azonosítására használt adata (felhasználóneve) a Partner informatikai rendszerében,
- Ügyfél második faktoros azonosításra használt az ügyfél-átvilágítás alatt validált csatornájának azonosítója (telefonszám).

A Szolgáltatást nem igénybevevő Ügyfelek fenti adatai a jogszabályban meghatározott időtartamot követően törlésre kerülnek.

4.4. Elektronikus aláírás létrejöttének és elhelyezésének folyamata

A Partner az Ügyfélnek aláírásra kínált Dokumentum előállítása után az informatikai integráción keresztül a következő adatot juttatja el biztonságos csatornán a Szolgáltatóhoz:

- Ügyfél azonosítója
- Ügyfél általi aláírásra kínált Dokumentum
- Az aláírásra kínált Dokumentum aláírásának legkésőbbi időpontja

Ez után a Partner értesíti az Ügyfelét az elektronikus aláírási lehetőségről.
Ekkor az Ügyfél a Szolgáltató informatikai rendszerébe történő kétfaktoros authentikáció után megtekinti a számára aláírásra kínált Dokumentumot.

Az Ügyfél a Felkínált Dokumentum megismerése után fejezheti ki szándékát a Szolgáltatás igénybevételére (a Dokumentumon történő elektronikus aláírása elhelyezésére), amellyel az alábbi folyamat indul el.

Az Ügyfélnek ezen rendszerben lehetősége van az aláírás visszautasítására is.

4.5. Ügyfél oldali aláírás

Az aláírás és annak menete egy összetett, több lépéses folyamat, ami az Ügyfél Applikációja és a Szolgáltató szervere között zajlik. Az aláírási folyamat során az Ügyfélnek csak egyszer szükséges interaktálni az applikációval, minden további, a következőkben ismertetett részfolyamat automatikus, emberi beavatkozás nélkül történik.
A teljes folyamat automatizált, zárt és a Szolgáltató rendszereiben naplózott és riasztás-védelemmel ellátott. Ebből következően a Partner által elkészített Dokumentum módosítására nincs lehetőség.

Az aláírási folyamat három fázisból áll:

1. **M1**: Első, aláírással kapcsolatos üzenetküldés az Applikáció és a Szolgáltató szervere között
2. Kétfaktoros autentikáció
3. **M2**: Második, aláírással kapcsolatos üzenetküldés az Applikáció és a Szolgáltató szervere között

Az aláírási folyamat csak akkor kezdhető meg, ha az Ügyfél végigolvasta (kötelezően végig görgette) a Felkínált Dokumentumot. Ezután aktiválódik az “Aláírás gomb”, aminek megnyomásával elkezdődik az aláírási folyamat.

4.5.1. Az aláírási folyamat során alkalmazott időbélyegekről

Az Applikáció által használt időbélyegek minden esetben az alábbiak szerint készülnek.
Az időbélyeg minden esetben egy minősített időbélyegző szolgáltatótól származik. Először az applikáció a Szolgáltató szerveréhez titkosított HTTPS csatornán keresztül intéz kérést, amire válaszként a Szolgáltató szervere egy minősített időbélyeg szolgáltatótól származó időbélyeget továbbít az Applikációnak válaszként.
Az időbélyegzés folyamata során az időbélyegzett adat nem hagyja el az ügyfél Applikációját, az nem kerül elküldésre - csak és kizárólag az időbélyegzett adat hash értéke, amiből nem lehetséges visszafejteni vagy újrageneránlni az eredeti adatot. Se a Szolgáltató szervere, se az időbélyeg szolgáltató így nem szerez tudomást az időbélyegzett adatról.
A hash érték garantálja, hogy az időbélyegzett adat az időbélyegzés idejében létezett.

4.5.2. Első fázis: M1 - Első üzenet lépései

Aszimmetrikus kulcspár generálás

Az Ügyfél Applikációja egy RSA-2048 algoritmusnak megfelelő “publikus” és “privát” kulcspárt generál, amit csakis memóriában tárol. Ez a kulcspár csak és kizárólag az aktuális aláírás erejéig létezik az

Applikációban. Mind sikeres, mind sikertelen aláírás után a kulcspár az applikáció számára újbóli felhasználásra alkalmatlanná válik, mivel nem tárolja azt tartós adathordozón.
A kulcsokról bizonyítható egymáshoz tartozásuk, azonban egyikből a másik számításának időigénye a jelenlegi számítási kapacitásokat alapul véve évtizedekben mérhető. Annak esélye, hogy egy korábban generált kulcspár újra véletlenszerűen legenerálásra kerül, az $1:10^{100}$ képest is elhanyagolható. Az aszimmetrikus kulcspár sajátsága továbbá, hogy az egyik kulccsal előállított kódolt üzenet csak a másik kulccsal dekódolható.

Üzenet előállítása

Az applikáció előállítja a következő JSON struktúrát (**JSON1**):

[[“publicKey”,“<Base64>”],["username”,“<String>”]]

ami tartalmazza a generált publikus kulcsot base64 kódolással, valamint az Ügyfél felhasználónevét.

Ezután az Applikáció:

1. kiszámolja a **JSON1** struktúra SHA256 szerinti hash értékét (*TEMP_HASH1*)
2. és a generált privát kulccsal kriptografikusan aláírja a hash-t (**SIGN1**)
3. majd kiszámolja **SIGN1** SHA256 szerinti hash értékét (*TEMP_HASH2*)
4. és *TEMP_HASH2*-t időbélyeggel látja el (**TS1**)

Rövid folyamat ábra szerint:
JSON1 -> *TEMP_HASH1* -> **SIGN1** -> *TEMP_HASH2* -> **TS1**

M1 elküldése

Az applikáció HTTPS titkosított csatornán keresztül elküldi az **M1** üzenet részeként a **JSON1** struktúrát, az első időbélyeget (**TS1**), valamint **SIGN1** értéket.

4.5.3. Második fázis: Kétfaktoros autentikáció lépései

Verifikációs token

A Szolgáltató oldali szerver fogadva az M1 üzenetet, generál egy verifikációs kódot (**TOKEN**), amit SMS-ben kiküld az Ügyfél előzőleg a Partner által ellenőrzött telefonszámára.
A token egy, az ügyfélhez köthető véletlenszerűen és egyedileg generált 8 karakter hosszú alfanumerikus adat, ami a kibocsátás után a Szolgáltató által meghatározott rövid időablak bezártáig elfogadható (10 perc). Az időkorlát lejárta után a Szolgáltató szervere nem fogadja el a kódot, az nem használható két-faktoros autentikációra többet, így az aláírási folyamat is megszakad.

Kétfaktoros autentikáció

Az Ügyfél az Applikáción keresztül kétfaktoros autentikációs képernyőn megadja a következő autentikációs adatokat:

- Az Ügyfél Partner rendszerében használt felhasználóneve
- Az Ügyfél Partner rendszerében használt jelszava
- Az SMS-ben kapott verifikációs kód (**TOKEN**)

Az applikáció HTTPS titkosított csatornán elküldi az autentikációs adatokat a Szolgáltató szerverének ellenőrzésre. A Szolgáltató ellenőrzi TOKEN az adott ügylethez való megfelelését, valamint a Partner rendszerében biztonságos csatornán keresztül ellenőrzi a felhasználónév és jelszó egymáshoz tartozását és a felhasználói fiók érvényességét. Esetleges elgépelés esetén az Ügyfélnek lehetősége van újra próbálkozni a TOKEN lejárati idejéig. Sikeres ellenőrzés után az Applikáció folytatja az aláírási folyamatot.

4.5.4. Harmadik fázis: M2 - Második üzenet

Ügyfél aláírás előállítása

Az applikáció előállítja az ügyfél aláírásának törzsét alkotó JSON struktúrát (**JSON2**):

```
[
  [“publicKey”, <Base64>],
  [“privateKey”, <Base64>],
  [“offers”, <listOfOfferHashes>],
  [“username”, <String>],
  [“smsToken”, <TOKEN>],
  [“deviceInfo”, <deviceInfo>],
  [“photo”, <Base64>]
]
```

ami tartalmazza a következőket:

- generált publikus és privát kulcspárt base64 kódolással
- az ajánlat részét képező dokumentumok SHA256 algoritmusnak megfelelő hash értékeit
- az Ügyfél felhasználónevét
- a kétfaktoros autentikáció során begépelt verifikációs tokent
- az aláíró eszköz és Applikáció adatai (IMEI, MAC, telefonszám, App ID, opcionálisan geolokáció)
- az Ügyfélről a készülék kamerájával készített fénykép, amennyiben ez az opció elérhető és az ügyfél engedélyezte a kamerahasználatot (opcionális)

Az dokumentumok hash értékének JSON struktúrája egy lista, amiben az elemek további két-elemű listák, amiben az egyes dokumentumok azonosítója és a hozzájuk tartozó SHA256 hash értékek szerepelnek.

Példa egy listOfOfferHashes ahol két dokumentum szerepel:

```
[
  [“1”, <hash>],
  [“2”, <hash>]
]
```

Ezután az Applikáció:

1. kiszámolja a **JSON2** struktúra SHA256 szerinti hash értékét (*TEMP_HASH3*)
2. a hash-t időbélyeggel látja el (**TS2**)

Az applikáció összeállítja az ügyfél aláírását reprezentáló JSON struktúrát (**JSON3**):

```
[
  [“publicKey”, <Base64>],
  [“privateKey”, <Base64>],
  [“offers”, <listOfOfferHashes>],
  [“username”, <String>],
  [“smsToken”, <TOKEN>],
  [“deviceInfo”, <deviceInfo>],
  [“timestamp”, <TS2 Base64>]
]
```

ami tartalmazza az aláírás törzsét és annak időbélyegét base64 kódolással.

Ezután az Applikáció:

1. kiszámolja a **JSON3** struktúra SHA256 algoritmusnak megfelelő hash értéket (**HASH1**).
2. előállítja a következő JSON struktúrát (**JSON4**):

```
[
  [“customerSignatureHash”, <HASH1>],
  [“customerSignature”, <JSON3>]
]
```

ami tartalmazza az ügyfél aláírását reprezentáló JSON struktúrát, valamint annak hash értékét.

Ezután az applikáció:

1. kiszámolja **JSON4** SHA256 szerinti hash értékét (*TEMP_HASH4*)
2. és a generált publikus kulccsal kriptografikusan aláírja *TEMP_HASH4*-et (**SIGN2**)
3. majd kiszámolja **SIGN2** SHA256 szerinti hash értékét (*TEMP_HASH5*)
4. majd *TEMP_HASH5*-t időbélyeggel látja el (**TS3**)

Rövid folyamat ábra szerint:

JSON2 -> *TEMP_HASH3* -> **TS2**
JSON3 -> **HASH1**
JSON4 -> *TEMP_HASH4* -> **SIGN2** -> *TEMP_HASH5* -> **TS3**

M2 elküldése

Az Applikáció HTTPS csatornán keresztül elküldi az **M2** üzenet részeként a **JSON4** struktúrát, a harmadik időbélyeget (**TS3**), valamint **SIGN2** értéket.

Az **M2** üzenet szervernek küldésével a kulcspár a szerver oldal számára is ismertté válik. A jövőben ezért az adott kulcspár semmilyen más célra, beleértve más Dokumentum aláírását, nem használható. Az újbóli felhasználás kizárását az rendszer felépítése, az általa megvalósított automatizmusok garantálják.
Az Ügyfélnek az Applikáción keresztül nincs direkt hozzáférése a kulcspárhoz, azokat nem éri el, továbbá az implementált aláírási folyamat biztosítja minden Dokumentumhoz az új kulcspár létrejöttét.

4.5.5. Negyedik fázis - Aláírás ellenőrzése

Az Ügyfél aláírásának ellenőrzéséhez a Szolgáltató a következő pontokat vizsgálja:

1. Az Applikáció által küldött adatok hiánytalan meglévősége és formai megfelelősége a folyamat szerint.
2. Publikus kulcsok egyezése **M1** és **M2**-ben, ami garantálja, hogy a folyamatban ugyanazt a kulcspárt használták.
3. Publikus és privát kulcs egymáshoz tartozásának vizsgálata.
4. **SIGN1** és **SIGN2** ellenőrzése az **M1**-ben található publikus kulccsal, ami garantálja, a kulcspár ügyfélhez tartozását.
5. **M1** és **M2**-ben kapott felhasználónevek egyezése a Partner által tárolt felhasználónévvel.
6. Az ajánlat részét képező Dokumentum hash értékeinek ellenőrzése
7. A kétfaktoros azonosítás során használt SMS token (**TOKEN**) egyezése a Szolgáltató által kibocsátott tokennel.
8. Ügyfél-aláírás hash (**HASH1**) ellenőrzése.
9. **M1** és **M2** ellenőrzése a privát kulcs birtokában, azok újragenerálásával.
10. Időbélyegek sorrendiségének ellenőrzése:
    a. Az időbélyegekben dátuma szerint: **TS1** < **TS2** < **TS3**, ami garantálja, hogy a privát kulcs nem volt a Szolgáltató birtokában az aláírás pillanatában
    b. **TS3** – **TS1** < 10 perc, ami garantálja, hogy az aláírási folyamat maximum 10 perc alatt végbement

4.5.6. Ötödik fázis - Szolgáltató általi véglegesítés

1. A Szolgáltató a Felkínált Dokumentum alapján - azt változatlanul felhasználva - létrehozza az Aláírt Dokumentumot, amit a Szolgáltató számára a saját nevére előzőleg kiállított, érvényes, minősített elektronikus bélyegző tanúsítvánnyal bélyegez és minősített időbélyeggel látja el (PAdES-T), amely aláírásnál a vizuális reprezentáció részeként feltüntetve az ügyfél nevét, felhasználónevét, az aláírás pontos időpontját, valamint a JSON aláírás hash értékét (HASH1).

2. Ezt követően a Szolgáltató az Applikáción keresztül:
    a. Felajánlja letöltésre az Aláírt Dokumentumot és ennek letöltését naplózza.
    b. Letölti az Ügyfél eszközére az Aláírási Csomagot. Így a folyamat összes lépése és azok ellenőrzése az Ügyfél számára is elvégezhető.

Ezzel a lépéssel véget ért az elektronikus aláírás létrejöttének és elhelyezésének folyamata.

A Dokumentumon az Ügyfél elektronikus aláírását egy hash reprezentálja, ennek a Dokumentumra helyezésénél a technológiai megoldás, hogy a Szolgáltató elektronikus bélyegzőjének vizuális reprezentációjaként kerül fel az információ. Ennek előnye, hogy ha a PDF formátumú Dokumentum előzőleg tartalmazott PAdES szabványú elektronikus aláírást, akkor az az Ügyfél aláírása után is érvényes marad.

4.6. eIDAS megfelelés

Az eIDAS rendelet (EU 910/2014) 26. cikk követelményei az ügyfél fokozott biztonságú elektronikus aláírásával szemben:

Kizárólag az aláíróhoz köthető

A Partner az ügyfél-átvilágítás során meggyőződik az Ügyfél személyazonosságáról. Az ekkor kialakított két külön faktor egyenként és kizárólag az aláíróhoz köthető.

Alkalmas az aláíró azonosítására

Az Aláírási Csomag tartalmazza az ügyfél az ügyfélhez egyedileg köthető felhasználónevét és a kétfaktoros authentikáció adatait.

Olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;

Az aláírás létrehozásához használt adat csak az Ügyfél rendelkezésére álló eszközön futó Alkalmazás számára ismert az aláírás pillanatában. Az adat egy véletlenszerűen generált publikus és privát kulcspár (RSA 2048).

Az aláírás során használt minősített időbélyegek sorrendisége alapján kijelenthető, hogy ez az adat a Szolgáltató rendelkezésére csak az aláírás elkészülte után, ellenőrzési célból vált ismertté.

A kulcspár ismételt felhasználására nincs lehetőség, minden aláírási folyamathoz új kulcspár kerül létrehozásra, amit az Applikációba épített automatizmusok biztosítanak.

A Szolgáltató számára ismert publikus kulcsból a privát kulcs nem számítható a jelenkori számítási kapacitásokat alapul véve.

Olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Az Ügyfél aláírását reprezentáló hash az Aláírási Csomagból előállítható, az aláírás ideje a minősített időbélyegzők adataiból származtatható. Az Aláírt Dokumentum legkisebb változtatása is eltérő hash értéket eredményez annak újraszámításakor.

Az Aláírt Dokumentumon a Szolgáltató által elhelyezett minősített elektronikus bélyegző biztosítja a Dokumentum eredetének és sértetlenségének bizonyosságát.

Az Aláírt Dokumentumon a Szolgáltató által elhelyezett minősített időbélyeg biztosítja az általa feltüntetett dátum és időpont pontosságát, valamint az adott dátumhoz és időponthoz kapcsolt adatok sértetlenségét.

5.1 Fizikai óvintézkedések

5.1.1 FaceKom adatközpont

A FaceKom Kft. adatközpontja a T-Systems Cloud & Data Center adatközpontjában került kialakításra (1087 Budapest, Asztalos Sándor út 13). 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 T-Systems szolgáltatási szabályzat tartalmazza.

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.

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 (SZMSZ) határozza meg. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. Valamennyi bizalmi munkakört betöltő személy rendelkezik helyettessel. A bizalmi munkaköröket betöltő személyekről a Szolgáltató nyilvántartást vezet.

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, és szakmai gyakorlattal igazolni tudja.

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

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 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.

5.3 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 az adott rendszerről folyamatosan szinkronizálásra kerülnek egy központi loggyüjtő és elemző rendszerbe.

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 automatikusan törlésre kerülnek.

A naplófájlok állandó szinkronizálás alatt állnak egy 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 Archiválás és tárolás

6.4 Archiválás és tárolás

Amennyiben az Ügyfél az Applikáción keresztül igénybe veszi a Szolgáltatást akkor az Ügyfél Applikációt futtató informatikai eszközére az Aláírási Csomag kerül letöltésre.

A jogszabályi követelményeknek megfelelően az elektronikus aláírási folyamat során keletkező Dokumentumot a Szolgáltató köteles megőrizni és a megfelelő belső eljárásrendek alapján 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 Szolgáltatás igénybevételéhez használja Szolgáltató Applikációját.
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 nyújthat bizonyosságot az előző kettő védelmi vonal megfelelő működéséről.

A Szolgáltató az Applikáción keresztül biztosítja az Ügyfél részére a teljes kommunikációt érintő zártságot, bizalmasságot és sértetlenséget.

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 biztonságos csatornáknál alkalmazott titkosító algoritmusok 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. 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 általános informatikai és kommunikációs biztonsági szintjének megtartását, illetve emelését biztosító belső folyamatokat időközönként ellenőrizheti egy a Szolgáltatótól független audit.

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 végezhet, illetve végeztethet annak érdekében, hogy a Szolgáltatásával kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szakmai követelményeknek.

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 átfogó helyszíni ellenőrzés keretében ellenőrizheti Szolgáltató tevékenységét.

Szolgáltató bizalmi Szolgáltatására vonatkozó megfelelőség értékelése során az alábbi területeket vizsgálhatja és ellenőrizheti:

- 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.

Az ellenőrzések, szakértői elemzések által feltárt hiányosságokat, hibás késlekedés nélkül orvosolnia kell, valamint dokumentálnia és ellenőriznie kell a megtett intézkedéseket.

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) a Dáptv. 92. §-ában foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, a Dáptv. 93. §-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 legalább 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 adatkezelési 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

adatkezelési 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 Szolgáltatónak - mint adatkezelőnek, szerepelnie kell 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 Általános Szerződési Feltétele, így különösen annak felelősségre vonatkozó rendelkezései a Szolgáltatás vonatkozásában is alkalmazandó.

8.5 Díjak

Az Ügyfél részére jelen Szolgáltatási Szabályzat szerinti Szolgáltatás igénybevételére vonatkozóan díjat nem számít fel a Szolgáltató.

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 lépés napján közzé kell tennie internetes honlapján a módosult Szolgáltatási Szabályzatot.

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 igénybevételére.

Személyi hatály

A Szolgáltatási Szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az Ügyfélre.

9.2.2 Megszűnés

A Szolgáltatási Szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

A jelen Szolgáltatási Szabályzat szerinti szolgáltatási tevékenység megszűnése esetén:

- Az Ügyfélnek nincs lehetősége igénybe venni a Szolgáltatást,

- a korábban elhelyezett elektronikus aláírások a vonatkozó jogszabályok értelmében érvényesek,
- az Ügyfélnek a Szolgáltató telephelyén személyes azonosítást követően van lehetősége a korábban igénybevett Szolgáltatáshoz tartozó Aláírási Csomagok elektronikus formában történő átvételére.

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 a Dáp törvény 92. § megfelelően. Amennyiben a Szolgáltató ellen megszüntetési eljárás indult, a Szolgáltató haladéktalanul tájékoztatja a Bizalmi Felügyeletet a Dáp törvény 93. § megfelelően.

A Szolgáltató a jelen Szolgáltatási Szabályzat tárgyát képező szolgáltatási tevékenység beszüntetésekor teljeskörű 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 24/2016 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, a Dáp törvény 92. § 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 szolgáltatónak történő átadásáról a Dáp törvény 93. § 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, a Dáp törvény 92.§ és 93. §-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 írásban előterjeszteni.

Írásbeli panasz a következő módokon terjeszthető elő:

- online módon az ugyfelszolgalat@techteamer.com elérhetőségen,

A panaszkezelés részletes szabályai a Szolgáltató Panaszkezelési Szabályzatában kerültek meghatározásra, amely a https://bizalmiszolgaltatas.facekom.net weboldalon elérhető.

9.3.3 Békéltető Testület

Felek jogosultak viták rendezése céljából békéltető testülethez fordulni.

A Budapesti Békéltető Testület székhelye:

1016 Budapest, Krisztina krt. 99. I . em. 111.

Levelezési cím: 1253 Budapest, Pf.: 10.

E-mail cím: bekelteto.testulet@bkik.hu

Weboldal: www.bekeltet.hu

Telefon: 06 (1) 488 21 31

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;
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2024/1183 RENDELETE (2024. április 11.) a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
- 2023. évi CIII. törvény a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól (továbbiakban: Dáptv.)
- 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;
- 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.