A MikroCredit Zrt.
Bizalmi Szolgáltatási Rend
elektronikus aláírás elhelyezéséhez

Szabályzat száma	P13
Verzió	v1
Hatálybalépés dátuma	2019.06.29.

Változáskövetés

Verzió	**Hatálybalépés dátuma**	**Változás oka**
v0	2019.03.25.	Létrehozás
v1	2019.06.29.	Nem valós idejű ügyfélátvilágítás bevezetése

Tartalomjegyzék

1. Bevezetés

1.1 Áttekintés

Jelen dokumentum a MikroCredit 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 Szolgáltató a Szolgáltatást az Ügyfele részére csak és kizárólag olyan dokumentumokhoz nyújtja, amelyet az Ügyfele részére felkínált aláírásra.

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

Az ügyfelek a Szolgáltató rendszerébe integrált, speciálisan erre a célra kialakított informatikai szolgáltatás igénybevételével 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: **MikroCredit 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., Eütv), 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 nem bocsát ki tanúsítványokat az általa nyújtott bizalmi szolgáltatás keretei között. A jelen Rendben 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 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 bizalmi szolgáltatásaival kapcsolatos internetes honlapján, a https://www.minikolcson.hu címen.
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 2019.03.25-én jelentette be a Bizalmi Felügyeletnek, mint nem minősített bizalmi szolgáltató.
A Bizalmi Felügyelet 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 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.
Ügyfél	az a természetes személy, aki igénybe veszi a Szolgáltatást
Szolgáltatás	eIDAS szerinti fokozott biztonságú elektronikus aláírás elhelyezése
Szolgáltató	MikroCredit Zrt. mint nem minősített bizalmi szolgáltató
eIDAS	910/2014/EU rendelet
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)
- 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
- 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
- 45/2018. (XII. 17.) 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;
- 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról.

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
- Bizalmi Szolgáltatási Szabályzat
- Bizalmi Szolgáltatási Rend

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://www.minikolcson.hu című weblapján 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- és nem valós idejű ügyfél-átvilágítás egyes lépéseit, illetve a további validációs célt szolgáló ellenőrzéseket.

4. Az elektronikus aláírás létrejöttének és elhelyezésének folyamata

4.1. Az elektronikus aláírás létrejöttének és elhelyezésének folyamata

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 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, útlevelét vagy kártyaformátumú vezetői engedélyét, valamint a lakcímkártyáját. A Szolgáltató IT rendszereinek ellenőrizniük kell az igazolvány és lakcímkártya számát, továbbá a Szolgáltató IT rendszereinek a személyazonosító igazolvány érvényességének, valamint az adatok egyezőségének ellenőrzése céljából

hatósági adatszolgáltatótól, a GIRO Zrt. szolgáltatásának igénybevételével, le kell kérniük a szükséges ügyféladatokat.

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 többek között el kell fogadnia a következőket:

- Az Elektronikus Azonosítású Szolgáltatások Általános Szerződési Feltételei
- Az Adatvédelmi Tájékoztatót
- A 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 Szolgáltató a saját rendszerében elvégzi a Pmt. szerinti ügyfél-átvilágítást.

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

4.4. Elektronikus aláírás létrejöttének és elhelyezésének folyamata

A Szolgáltató az Ügyfélnek aláírásra kínált Dokumentumról elektronikus formában (email, illetve push üzenet) értesíti az ügyfelet.
Ekkor az Ügyfél a Szolgáltató informatikai rendszerébe történő 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, amely 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 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 authentikáció
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 újragenerálni 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 authentikáció lépései

Verifikációs token

A Szolgáltató oldali szerver fogadva az M1 üzenetet, generál egy verifikációs kódot (**TOKEN**), amit SMS-ben kiküld az Ügyfél 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 authentikációra többet, így az aláírási folyamat is megszakad.

Kétfaktoros authentikáció

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

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

Az applikáció HTTPS titkosított csatornán elküldi az authentikációs adatokat a Szolgáltató szerverének ellenőrzésre. A Szolgáltató ellenőrzi TOKEN az adott ügylethez való megfelelését és 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
- az kétfaktoros authentikáció 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, amelyben 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 felhasználónévvel.
6. Az ajánlat részét képező Dokumentum hash értékeinek ellenőrzése
7. Az 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 JSON aláírás hash értékét (**HASH1**), és az ügyfél felhasználónevét.
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.

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 Szolgáltató 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 az 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. 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 MikroCredit adatközpont

A MikroCredit Zrt. adatközpontja az Invitech Kozma utcai, backup adatközpontja pedig az Invitech Ilka utcai Data Centerében került kialakításra (1108 Budapest Kozma utca 2 és 1143 Budapest Ilka utca 31). 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 az Invitech szolgáltatási szabályzat tartalmazza.

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 az adatközpontban

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

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 rendszer 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 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. Archiválás és tárolás

A Szolgáltatónak a szolgáltatási szabályzatban ismertetnie kell a mentett dokumentumokat, valamint a mentés technikai részleteit.

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.

6.2 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 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 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.

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 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 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. A NAIH nyilvántartási szám igénylése folyamatban van.

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

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 igénybevételére terjed ki.

Személyi hatály

A Szolgáltatási Rend személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az Ügyfélre.
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 teljeskörűen 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 maior" 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 maior" esetében a Szolgáltatónak haladéktalanul tájékoztatnia kell Ügyfeleit a vis maiorral összefüggő késedelem okairól.