Minősített tanúsítványok elektronikus aláírás szolgáltatáshoz

Digical Működési Szabályzat Nemzetközi Leányvállalat Igazgatóság

(CIB Bank Zrt.-re irányadó változat)

Terjesztés:	NYILVÁNOS								
Dokumentumkód:	CIB	-	SCD	-	04	-	2020	-	02
	Vállalat		*Szolgáltatás*		*Kód*		*Év*		*Verzió*

A DIGICAL MŰKÖDÉSI SZABÁLYZAT VERZIÓI

Verzió	Kiadás dátuma	A változtatás leírása
01	2020.04.03.	Első verzió (ISP-SCD-014-2019 v03 alapján)
02	2020.06.17.	Második verzió (ISP-SCD-04-2020 v05 alapján)

TARTALOMJEGYZÉK

1. ÁLTALÁNOS INFORMÁCIÓK

1.1 Áttekintés

A jelen (az alábbiakban meghatározott jelentéssel bíró) „Távoli Digitális Aláírási Működési Szabályzat" célja, hogy az Intesa Sanpaolo S.p.A. által – a 82/2005. számú olasz törvényerejű rendelettel (Digitális Igazgatási Szabályzat) és későbbi módosításaival, valamint az irányadó nemzeti és európai jogszabályokkal és szabályozásokkal összhangban – (az alábbiakban meghatározott) Nemzetközi leánybankok (az alábbiakban meghatározott) Ügyfeleinek nyújtott, elektronikus aláírási szolgáltatási célú minősített tanúsítványok szabályozása, amely szolgáltatásokat többcsatornás szolgáltatásokkal kapcsolatban nyújt (úgymint az Ügyfelek távoli csatornákon keresztüli hozzáférése a Nemzetközi leánybankok által nyújtott szolgáltatásokhoz).
Ez a Távoli Digitális Aláírási Működési Szabályzat a digitális aláírás DPCM 22/02/2013-ban szereplő jogi keretének implementálására szolgáló műszaki szabályokra is hivatkozik. Ha bármelyik jogszabály megváltozna, a Távoli Digitális Aláírási Működési Szabályzatot ennek megfelelően kell módosítani.

1.2 Definíciók és értelmezés

A jelen Távoli Digitális Aláírási Működési Szabályzatban nagybetűvel használt kifejezések jelentése az alábbi:

- „**Bank**": Az Intesa Sanpaolo Csoport bármely Nemzetközi leánybankja.
- „**Kérelmező"** (**Applicant)**: az az Ügyfél, aki magánszemélyek részére szóló elektronikus aláíráshoz minősített tanúsítvány kibocsátását kéri; a Kérelmező a Birtokossal (Holder) azonos személy;
- „**Fiók**" (**Branch)**: az a hely, ahol a megrendelő és a Bank közötti üzletet bonyolítják, ez magába foglalja az adott Nemzetközi Leánybank valamennyi helyszínét, irodáját és helyiségét.
  - „**Hitelesítésszolgáltató" (Certification Authority)**: az a bizalmi szolgáltató, amely jogosult elektronikus aláírási célú minősített tanúsítványok kibocsátására olyan eljárással, amely megfelel a nemzetközi szabványoknak, valamint az európai és nemzeti jogszabályoknak és szabályozásoknak. A jelen Távoli Digitális Aláírási Működési Szabályzat értelmezésében a Hitelesítésszolgáltató az Intesa Sanpaolo S.p.A.
  - „**Hitelesítésszolgáltatási szerződés":** A Hitelesítésszolgáltató és az Ügyfél között megkötött, Szolgáltatási szerződés hitelesítésszolgáltatás nyújtásához című szerződés.
- „**Ügyfél" (User)**: az a magánszemély, valamely Nemzetközi leánybankkal a hitelesítés szolgáltatási szerződés (aláírója (jelen esetben a Kérelmezővel és a Birtokossal azonos személy);
  - „**Digital Acquisition**": a digitális ügyfélszerződési folyamat elvégzésére szolgáló csatorna, amelyen keresztül a banki ügyintéző videoazonosítást végez az ügyfél által biztosított azonosító okmány alapján;
  - **Távoli Digitális Aláírási (RDS) Működési Kézikönyv" (Remote Digital Signature (RDS) Operating Manual)**: a jelen dokumentum a későbbi módosításokkal és kiegészítésekkel;
  - **„Nemzetközi leánybankok„ (International Subsidiary Banks)**: az Intesa Sanpaolo Csoporthoz tartozó bármely nemzetközi leánybank;
- „**Birtokos" (Holder):** az az Ügyfél, akinek a minősített elektronikus aláírási tanúsítványt kibocsátották; a birtokos jogosult e tanúsítvány használatára elektronikus dokumentumok digitális aláírására, egyben biztosítva a szóban forgó elektronikus dokumentumok eredetének hitelességét és tartalmának sértetlenségét, a Nemzetközi leánybankok Hitelesítésszolgáltatási Szerződésében előírt korlátozásoknak megfelelően;
- „**Intesa Sanpaolo**": Intesa Sanpaolo Részvénytársaság, az elektronikus aláírásokat szolgáló minősített tanúsítványok szolgáltatója;
- „**OTP eszköz" (OTP device)**: a csak egy tranzakcióra érvényes jelszót közvetlenül a digitális aláírási művelet előtt generálja a Hitelesítésszolgáltató és bocsátja a Birtokos rendelkezésére. Ha a használt csatorna a digitális ügyfélszerző csatorna vagy Fiók, az egyszeri kódot (angolul one time password, azaz OTP) SMS útján kapja meg az Ügyfél. Távoli digitális banki szolgáltatás esetén az egyszeri kódot (angolul one time password, azaz OTP) a TOKEN generálja;
  - „**Regisztrációs szervezet" (Registration Authority)**: Az a szervezet, amelynek főként az alábbiak a feladatai (i) azonosítja a Kérelmezőt , biztosítva az azonosságuk pontosságát, (ii) megadja a Kérelmezők számára a minősített aláírási tanúsítvánnyal kapcsolatos szükséges tájékoztatást, és a használatukra vonatkozó korlátozásokról is tájékoztatja őket, (iii) szerződést köt a Kérelmezőkkel az Intesa Sanpaolo nevében és érdekében, (iv) továbbítja az Intesa Sanpaolo részére a tanúsítványok visszavonására és felfüggesztésére vonatkozó kérelmeket. A jelen Távoli Digitális Aláírási Működési Szabályzat értelmezésében a Regisztrációs szervezet az Intesa Sanpaolo S.p.A. bármelyik azon Nemzetközi leánybankja, aki a minősített aláírási tanúsítvány tárgyában megállapodást kötött az Intesa Sanpaolo S.p.A.-val. Jelen esetben ez a CIB Bank Zrt.
  - „**TOKEN**": Biztonságos autentikációs rendszer, amely az erős ügyfélhitelesítést (Strong Customer Authentication, lásd a 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelet 4-9. cikkét) biztosítja; PIN ellenőrzést követően OTP (egyszeri jelszó) létrehozására használják.
  - „**Magánkulcs**": Az aszimmetrikus kulcspár titokban tartott összetevőjét jelenti, amelyet a

Hitelesítésszolgáltató egy megfelelő aláíró eszközön tárol biztonságos módon.

- „**Nyilvános kulcs**”: Az aszimmetrikus kulcspár azon nyilvános összetevőjét jelenti, amellyel az elektronikus aláírás hitelesítése elvégzésre kerül.

1.3 Hivatkozott jogszabályi rendelkezések

[Dlgs 82/2005]	A 2007. március 7-én kelt, 82. sz. jogszabály, közzé téve a 2005. május 16-i keltű 112. sz. Hivatalos Közlöny, - 93. sz. rendes mellékletében: „Digitális Közigazgatási Szabályzat”, melyet frissített a 2017. december 13-i 217. sz. olasz törvényerejű rendelet, közzé téve az olasz 9. sz. Hivatalos Közlönyben, 2018. január 9.
[DPCM]	Az olasz Miniszterelnök 2013. febr. 22-i Rendelete – A továbbfejlesztett minősített és digitális elektronikus aláírások létrehozásának, alkalmazásának és hitelesítésének technikai szabályai, a következő cikkek szerint: 20 (3), 24 (4), 28 (3), 32 (3) b. pont, 35 (2), 36 (2), és 71.
[CNIPA/CR/48]	A 2005. szept. 6-i CNIPA/CR/ 48 sz. Körlevél (közzé téve 2005. szept. 13., a 213 sz. Hivatalos Közlönyben), a tanúsítvány szolgáltatók nyilvános listájában bejegyzés kérelmének benyújtási eljárása a 445. sz. Elnöki Rendelet 28. cikk (1) bek. szerint. Kelte 2000. dec. 28.
[Del 45/2009]	Az Olasz 2009. máj. 21-i 45. sz. Határozat – Elektronikus dokumentumok elismerésének és hitelesítésének szabályai.
EU Regulation 910/2014 - eIDAS	Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről.
(EU) 2016/679 rendelete – GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

1.4 Szabvány hivatkozások

[LDAP2] Zeilenga, „Lightweight Directory Access Protocol version 2”, Internet RFC 3494, March 2003. (Egyszerűsített címtár hozzáférési protokoll, 2. verzió)

[PKCS7] B. Kaliski, „PKCS#7: Cryptographic Message Syntax Version 1.5”, Internet RFC 2315, March 1998. (Kriptográfiás üzenet szintaktika, 1.5 verzió”

[PKCS10] B. Kaliski, „PKCS#10: Certification Request Syntax - Version 1.7”, Internet RFC 2986, November

2000.
(Tanúsítványkérés szintaktika – 1.7 verzió)

[SHA1] ISO/IEC 10118-3-2018, „Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions”, 2018.
(Információtechnika – Biztonsági technikák – Hash funkciók – 3. rész: Dedikált Hash funkciók)

[SHA-256] ISO/IEC 10118-3:2018, „Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions”, March 2004.
(Információtechnika – Biztonsági technikák – Hash funkciók – 3. rész: Dedikált Hash funkciók)

[X500] ISO/IEC 9594-1: 2008, ISO/IEC 9594-2:2008 „Information technology — Open Systems Interconnection — The Directory: Overview of concepts, models and services”.
(Információtechnológia – Nyílt rendszerek összekapcsolása – A címtár: koncepciók, modellek és szolgáltatások áttekintése)

[X509] ISO/IEC 9594-8: 2005 „Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks”.
(Információtechnológia – Nyílt rendszerek összekapcsolása – A címtár: Nyilvános kulcs és attribútum-tanúsítás alapjai)

[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu.
(Internet X.509 Nyilvános kulcsú infrastruktúra tanúsítási politika és tanúsítási megoldások kerete)

[RFC 3778] The application PDF Taft, Pravetz, Zilles, Masinter, May 2004.
(A PDF alkalmazása)

1.5 Rövidítések

A jelen Távoli Digitális Aláírási Működési Szabályzatban használatos egyes kifejezéseket az alábbiak szerint kell rövidíteni:

AgID	A Digitális Olaszország Ügynöksége	The Agency for Digital Italy
CRL	Tanúsítvány visszavonási lista	Certificate Revocation List
CPS	Tanúsítvány megvalósítási nyilatkozat	Certificate Practice Statement
DBMS	Adatbázis kezelő rendszer	Database Management System
DN	Megkülönböztető név	Distinguished Name
DNS	Domén név rendszer	Domain Name System
DPR	Elnöki Rendelet	Presidential Decree
HSM	Hardver Biztonsági Modul	Hardware Security Module
HTTP	HyperText transzfer protokoll	HyperText Transfer Protocol
ITSEC	Információtechnológia biztonságértékelési kritériumai	Information Technology Security Evaluation Criteria
LDAP	Egyszerűsített címtár hozzáférési protokoll	Lightweight Directory Access Protocol
NEI	„Galileo Ferraris” Nemzeti Elektrotechnikai Intézet (olaszul: „Istituto Elettrotecnico Nazionale”)	National Electrotechnical Institute „Galileo Ferraris” (in Italian „Istituto Elettrotecnico Nazionale”)
OTP	Egyszer használatos jelszó	One Time Password
PDF	Hordozható dokumentumformátum	Portable Document Format
PIN	Személyi azonosító szám	Personal Identification Number
PKCS	Nyilvános kulcsú kriptográfiás szabvány	Public Key Cryptography Standard

RFC	Felhívás észrevételezésre	Request For Comments
RDS	Távoli Digitális Aláírás	Remote Digital Signature
RSA	Rivest-Shamir-Adleman algoritmus	Rivest-Shamir-Adleman
SHA-1	Biztonságos Hash funkció 1	Secure Hash Function 1
SHA-2	Biztonságos Hash funkció 2	Secure Hash Function 2
SSL	Protokoll réteg	Secure Sockets Layer
URL	Egységes erőforrás-hely	Uniform Resource Locator

2 BEVEZETÉS

A digitális aláírás aszimmetrikus kulcsokra támaszkodik, egy nyilvános és egy magánkulcsra, melyek biztosítják a digitálisan aláírt elektronikus dokumentumok eredetének hitelességét és tartalmuk sértetlenségét egy vagy több fogadó fél számára, akik viszont ellenőrizni tudják a vonatkozó érvényességet.

A [DPCM] 8. cikke által bevezetett új rendelkezések lehetővé teszik, hogy egy Hitelesítésszolgáltató tárolja a Birtokosok magánkulcsait (tehát a digitális aláírás létrehozására használatos kulcsokat) egy speciális biztonsági eszközön (pl. HSM), miközben biztosítják azt, hogy a kulcsok használata kizárólag a Birtokosnak legyen megadva, amint azt a [DPCM] 11. cikk (2) bekezdése előírja.

Következésképpen a digitális aláírás használatának már nem feltétele, hogy a Birtokos tulajdonában legyenek a digitális aláíráskészletek (pl. smart kártya, speciális olvasó és a hozzá tartozó szoftver), és a Hitelesítésszolgáltató és regisztrációs szervezetek közvetlen csatornák útján (pl. web, mobil) nyújthatnak digitális szolgáltatásokat az ügyfeleknek.

A Birtokos a digitális aláírási folyamatot egy OTP használatával indíthatja el (akár úgy, hogy a jelszót a megerősített mobilszámra kapja, akár úgy, hogy távoli banki szolgáltatás esetén a PIN megadása után azt a TOKEN hozza létre), miközben végig biztosított, hogy azt csak a Birtokos használhatja.

A jelen Távoli Digitális Aláírási Működési Szabályzatban a következő eljárásokat kell elmagyarázni:
- Aláírási kulcs generálási és kezelési eljárások az Intesa Sanpaolo által felkínált távoli digitális aláírási szolgáltatás esetén;
- A távoli digitális aláírás aktiválási eljárása és a digitális bankon belüli erős hitelesítési mechanizmus esetén a következők alapján a Nemzetközi leánybankok által meghatározott hitelesítési eljárás útján, (ii) az OTP eszköz;
- Azon műveleti eljárások, amelyek alapján a Hitelesítésszolgáltató és a Regisztrációs szervezet a vonatkozó jogszabályokkal és szabályozásokkal összhangban eljár.

A Távoli Digitális Aláírás Működési Kézikönyv minden, az Intesa Sanpaolo Nemzetközi Leánybanki Divíziójába tartozó Nemzetközi leánybankra vonatkozik.

Az alábbi pontok a [DPCM] 40. cikk 3. bek. a, b. és c. pontjából származnak.

2.1 A Hitelesítésszolgáltató azonosításának részletei

A hitelesítésszolgáltatást az alább azonosított alany nyújtja:

Név:	**Intesa Sanpaolo S.p.A.**
Bejegyzett székhely:	**Piazza San Carlo, 156 10121 Turin**
Jogi képviselő:	**Carlo Messina, Managing Director and CEO**
Regisztrációs szám a Turin Company-nál	**Economic Administrative Register (REA) no.**
Regiszter:	**00799960158**
Adószám:	**10810700152**
Telefonszám (központ):	**(+39) 011 555 1**
ISO objektum-azonosító (OID):	**1.3.6.1.4.1.20052**
Általános honlap (információ):	**www.intesasanpaolo.com**
Digitális tanúsítás szolgáltatás honlapja:	**ca.intesasanpaolo.com**

2.2 A Távoli Digitális Aláírási Működési Szabályzat azonosítása

A jelen Távoli Digitális Aláírási Működési Szabályzatot az ISP-SCD-02-2018-02 dokumentumkód (ez a címoldalon is látható)

A jelen Távoli Digitális Aláírási Működési Szabályzatot közzétették a Hitelesítésszolgáltató honlapján, így online is elérhető.

A jelen Távoli Digitális Aláírási Működési Szabályzat aktuális verziója a következő helyeken érhető el elektronikus formátumban:
- A Hitelesítésszolgáltató honlapján (https://ca.intesasanpaolo.com/);

- Az AgID honlapján;
- A Nemzetközi leánybankok részlegének Internet Bank honlapján

Eltérés esetén az AgID webhelyén közzétett verzió a mérvadó minden esetben.

2.3 A Távoli Digitális Aláírási Működési Szabályzatért felelős személy

A jelen Működési Szabályzatért felelős személy:

Ezio Barbero
Intesa Sanpaolo S.p.A.

3 ÁLTALÁNOS RENDELKEZÉSEK

3.1 A Regisztrációs szervezet, a Hitelesítésszolgáltató és a Birtokos kötelezettségei

3.1.1 A Hitelesítésszolgáltató és a Regisztrációs szervezet kötelezettségei

A Hitelesítésszolgáltatónak a DLgs 82/2005 32. cikkében részletezett rendelkezésekkel összhangban kell eljárnia, betartva az összes szervezeti és technikai intézkedést, amely megakadályozza a harmadik felek minden károsodását.

A [DLgs 82/2005] 25. cikkével összhangban a minősített elektronikus aláírási tanúsítványt kibocsátó Hitelesítésszolgáltatótól az alábbiakat is meg kell követelni:

- Megfelelően azonosítsa a Kérelmezőt; ezt a tevékenységet a Regisztrációs szervezetnek a nemzeti jogszabályokkal összhangban kell végeznie;
- Egyértelműen és teljeskörűen tájékoztassa a Kérelmezőt a minősített elektronikus aláírási tanúsítványok jellemzőiről és használatának korlátozásairól; ezt a tevékenységet a Regisztrációs szervezetnek még a hitelesítésszolgáltatási szerződés megkötése előtt kell végrehajtania;
- A Regisztrációs szervezet által haladéktalanul kiadott utasítások alapján hajtsa végre a minősített elektronikus aláírási tanúsítványok időben történő visszavonását a hozzá tartozó közzététellel együtt;
- Tartsa be a Birtokos személyi adatainak kezelésére vonatkozó biztonsági intézkedéseket, az alkalmazandó jogszabályokkal és szabályozásokkal összhangban; ezt a kötelezettséget mind a Regisztrációs szervezetnek, mind a Hitelesítésszolgáltatónak teljesítenie kell;
- A minősített elektronikus aláírási tanúsítványok kibocsátása a [DPCM] által előírt módon, összhangban a [DLGS196] előírással, annak későbbi módosításaival és kiegészítéseivel együtt történjen;
- Feleljen meg a [DPCM]-ben, valamint a DLgs 82/2005. 71. cikkében részletezett technikai szabályoknak;
- Biztosítsa, hogy az aláírás generálásához használt biztonságos eszköz rendelkezzen a [Dlgs 82/2005] 35. cikke és a [DPCM] 11. cikke szerint előírt jellemzőkkel és biztonsági követelményekkel;
- A minősített elektronikus aláírási tanúsítványokra vonatkozó összes információt elektronikus formában is legalább 20 (húsz) évig őrizze meg azért, hogy minden esetleges jogi lépés esetén bizonyítékot szolgáltathasson a tanúsításról;
- Az elektronikus aláírás kibocsátása céljából minősített tanúsítványok eljárásai során a Birtokos által aláírt összes dokumentumot legalább 20 (húsz) évig elektronikus formában is tárolja; ezt a tevékenységet a Regisztrációs szervezetnek kell végeznie;
- Ne exportálja a Birtokos magánkulcsait abból a HSM-ből, ahol ezeket a kulcsokat generálták és használták.
- A Hitelesítésszolgáltatónak és a Regisztrációs szervezetnek a jelen Távoli Digitális Aláírási Működési Szabályzatot folyamatosan frissítenie kell, és a Regisztrációs szervezetnek haladéktalanul tájékoztatnia kell az Ügyfelet az alkalmazott változásokról.

3.1.2 A Kérelmező/Birtokos kötelezettségei

A Birtokos köteles biztosítani a magánkulcsok használatát lehetővé tevő minden információ biztonságos megőrzését, és betartani az összes technikai és szervezeti intézkedést, mely megelőzi harmadik fél mindenfajta károsodását; a Birtokos köteles arra is, hogy személyesen használja a digitális aláírás létrehozását engedélyező adatokat ([DPCM] 8. cikk. 5. bekezdés).

A Birtokosnak be kell tartania a [DPCM] előírásait, különösen tekintettel az alábbiakra:

- A minősített elektronikus aláírási tanúsítványokat a jelen Távoli Digitális Aláírási Működési Szabályzatban részletezett eljárásoknak megfelelően kérelmezi;
- Köteles a minősített elektronikus aláírási tanúsítvány használatához szükséges kódokat (a TOKEN által generált kódot és az SMS-ben küldött OTP-t) titokban tartani (megőrizni);
- A minősített elektronikus aláírási tanúsítványok visszavonását kérje a jelen Távoli Digitális Aláírási Működési Szabályzatban részletezett eljárások szerint;
- A Regisztrációs szervezet haladéktalan értesítse minden olyan információ megváltozásról, amit a regisztrációs eljárás során a Hitelesítésszolgáltatónak megadott (személyi adatok, címek stb.);
- A magánkulcsokat kizárólag a digitális banki szolgáltatás használati szerződésben és a hitelesítésszolgáltatási szerződésben meghatározott minősített elektronikus aláírási tanúsítványi célokra használja;

- az azonosítást végző személynek vállalja, hogy a tanúsítvány kibocsátására vonatkozó kérelmében az azonosítására vonatkozóan megadott információk helyesek, valódiak és teljes körűek;

- a tanúsítványt csak a jelen Működési Szabályzatban, és a mindenkor hatályos nemzeti és nemzetközi jogszabályokban meghatározott módon használja.

3.1.3 Az aláírást ellenőrző személy kötelezettségei

Az Intesa Sanpaolo által létrehozott kulcsokkal létrehozott elektronikus aláírások ellenőrzését végző személyek az alábbiakat kötelesek elvégezni:

- ellenőrizze a tanúsítvány érvényességi idejét (a hatályos jogszabályokkal összhangban);

- a visszavont minősített tanúsítványi lista ellenőrzésével bizonyosodjon meg arról, hogy az aláírás pillanatában a tanúsítvány vissza volt-e vonva;

- ellenőrizze, hogy az elektronikus aláírás egy olyan minősített elektronikus aláírási tanúsítványhoz tartozik, amelyet olyan Hitelesítésszolgáltató bocsátott ki, aki az aláírás létrehozásának pillanatában az AgID előzetesen jóváhagyott;

- gondoskodjon róla, hogy a létrehozott „előfizetői” kulcstipológia és a tanúsítvány keyUsage 11 (OID:2.3.29.15) bővítménye esetén csak a letagadhatatlansági bitet tartalmazza (1 bit értéke 1) (előírva a [DPCM] 5. cikk 4. a) pontja szerint és CNIPA 45/2009. 12. cikk 5.a) pontja szerint);

- ellenőrizze a minősített tanúsítványban meghatározott, a használattal kapcsolatos korlátozásokat.

3.2 A felelősség korlátozása és a kártalanítás

3.2.1 A felelősség korlátozása

Az Intesa Sanpaolo nem vállal felelősséget semmilyen (szolgáltatás-)megszakadásért, ha a megszakadás oka az, hogy a Birtokos nem tartotta be a vonatkozó jogszabályokat és szabályozásokat, illetve a Birtokos és a Bank között megkötött digitális banki szolgáltatás használati szerződésében, vagy az arra hivatkozó bármely dokumentumban szereplő műszaki/kezelési előírásokat.

Az Intesa Sanpaolo nem felelős semmi olyan kárért, mely abból keletkezik, hogy a szolgáltatás használata során a minősített aláírási tanúsítványokban és/vagy a Bank digitális banki szolgáltatás használati szerződésében és/vagy hitelesítésszolgáltatási szerződésben előírt korlátozásokat megszegték.

A minősített elektronikus aláírási tanúsítványok használatára előírt használati korlátozások a következők:

„A tanúsítvány Birtokosának az Intesa Sanpaolo Csoport vállalataival, vagy a Csoporton kívüli olyan személyekkel fennálló kapcsolatokra vonatkozó dokumentumok korlátozott használata, melyek szolgáltatásaikat a Csoport vállalatainak elektronikus rendszerein kínálják”.

További korlátozás, hogy a minősített elektronikus aláírási tanúsítványt csak a hitelesítésszolgáltatási szerződésben meghatározott célokból lehet használni.

3.2.2 Kártalanítás

Amint a fenti 3.2.1 pont részletezi, az Intesa Sanpaolo nem tehető felelőssé a minősített elektronikus aláírási tanúsítványok semmilyen helytelen használatából származó bármi fajta kárért.

Mindazonáltal a [DPCM] 15. cikk (1) bek. i) pontja szerint az Intesa Sanpaolo kötött egy speciális biztosítást, ami a minősített elektronikus aláírási tanúsítványok kibocsátásával kapcsolatos vagy abból származó releváns kockázatok és mindenfajta kár fedezésére szolgál.

3.3 Szolgáltatási időszak

A Hitelesítésszolgáltató által kínált mindenfajta szolgáltatás (a minősített aláírási tanúsítvány kibocsátása és használata) direkt csatornákon (web és mobil) és fiókban is elérhetőek. A minősített aláírási tanúsítvány visszavonását fiókban lehet kérni.

4 ÜZEMELTETÉSI SZEMPONTOK

4.1 A minősített elektronikus aláírási tanúsítványok tartalma

Az Intesa Sanpaolo által kibocsátott, elektronikus aláírási célú minősített tanúsítványok tartalma megfelel a [Dlgs 82/2005] 28. cikkében és a közigazgatásban használt Információtechnológia Nemzeti Központ (jelenleg AgID) által kibocsátott 45/2009 sz. határozat 12. cikkében részletezett rendelkezéseknek.

A minősített elektronikus aláírási tanúsítványokat tilos közzétenni nyilvánosan rendelkezésre álló nyilvántartásokban. Minden minősített aláírási tanúsítvány érvényességi ideje 3 (három) év.

A távoli digitális aláírás révén a Birtokos képessé válik arra, hogy szerződést kössön a Bankkal. A távoli digitális aláírást bármilyen csatornán keresztül lehet használni a Bank által az adott időszakban biztosított egyedi ajánlatok és az elérhetőség függvényében (így különösen a digitális csatornákon: úgymint digitális fiókban, on-line bankolás, digitális ügyfélszerzés terén).

Ahhoz, hogy a Birtokos távoli digitális aláírást használjon, minősített aláírási tanúsítvánnyal kell rendelkeznie.

4.2 A személyzetre vonatkozó szervezési szabályok

A tanúsítvány szolgáltatás nyújtásáért és ellenőrzéséért felelős személyzetet a [DPCM] szerint kell megszervezni, ami *többek között* a felelősségi szerepkörök megteremtését jelenti a [DPCM] 38. cikkében előírtak szerint.

Kötelezettségük teljesítése során a felelős szerepkörben eljáró személyek maguk is igénybe vehetnek alkalmazottakat és kezelőket, olyanokat is, akik a Bank alkalmazottai.

A Távoli Digitális Aláírási Működési Szabályzatra vonatkozóan a kezelők a Nemzetközi leánybankok fiókirodáiban végzik a hitelesítésszolgáltatást (abban az értelemben, hogy regisztrálják vagy azonosítják a Birtokost), az Intesa Sanpaolo adatfeldolgozó központján kívül; az ilyen kezelők és az Intesa Sanpaolo közötti információcsere biztonságos kommunikációs csatornákon folyik.

A regisztrációs tevékenységet a Bank végzi az adott Bank és az Intesa Sanpaolo között megkötött szerződés alapján.

A Bank részéről eljáró személyek a regisztrációs tevékenységet a Bank és az Intesa Sanpaolo által elfogadott eljárásokkal összhangban végzik, egy előre meghatározott folyamat szerint.

4.3 A kulcsgenerálási eljárás

A [DPCM] 5. cikkében felsorolt minden kulcstípust biztonságos eszközökön belül generálják, tárolják és használják, melyek megfelelnek a vonatkozó jogszabályokban, szabályokban részletezett biztonsági követelményeknek.

A kulcsok jellemzőit a [DPCM] rögzíti.

4.3.1 Tanúsítványkulcs[1] generálási eljárás

A tanúsítványkulcsok generálási eljárása a vonatkozó jogszabályokkal és szabályokkal összhangban történik, különösen az alábbiak szerint:

- A tanúsítványkulcsokat a Hitelesítésszolgáltató által kifejezetten kinevezett alkalmazottak generálják;
- Minden egyes tanúsítvány kulcspárhoz elektronikus aláírási célú konkrét minősített tanúsítványt kell generálni, amint azt a 45/2009 sz. határozat részletezi, aláírva a kulcspár megfelelő magánkulcsával, amelyet már elküldtek az AgID-nek, a Hitelesítésszolgáltató és az AgID között korábban elfogadott eljárásokkal összhangban.

[1] A hitelesítésszolgáltató által a Kérelmező kérése alapján elektronikus aláírási célú minősített tanúsítványok kiadásához használt kulcs.

4.3.2 Időbélyegző kulcs generálási eljárás

A Nemzetközi leánybankoknak nyújtott digitális aláírás szolgáltatásokhoz kapcsolódó időbélyegző szolgáltatást illetően, az Intesa Sanpaolo olyan hitelesítésszolgáltatót használ, amely kielégíti annak az országnak a szolgáltatásnyújtásra vonatkozó követelményeit, ahol a Bank elhelyezkedik.

4.4 Az Ügyfélre vonatkozó azonosítási és regisztrálási eljárás

Minősített elektronikus aláírási tanúsítványt csak olyan Ügyfél kaphat, aki előzőleg hitelesítésszolgáltatási szerződést kötött.

A magánszemély Ügyfél minősített aláírási tanúsítványa a Birtokosról tartalmaz személyes információt.

Az Ügyfél azonosítási és regisztrálási eljárását a Bank végzi el a vonatkozó törvényekkel és szabályozásokkal összhangban, beleértve de nem kizárólag a pénzmosás elleni szabályozást, melyet a szerződéses viszonyba lépés időpontjától számítva be kell tartani.

A Bank a Birtokos és/vagy Kérelmező azonosítását vagy (i) személyesen végzi, az Ügyfél fizikai jelenlétében a Bank helyiségeiben, vagy (ii) távolból, a Magyarországon elismert, megbízhatóság szempontjából ezzel egyenértékű biztosítékot nyújtó azonosítási módszerekkel, figyelembe véve az eIDAS Szabályozás 24. cikkének 1.(d) pontjára.

4.4.1 Az Ügyfél azonosítása és regisztrálása

Az Ügyfél az alkalmazott digitális banki csatornától függő, előre meghatározott eljárások szerint lesz azonosítva. Az Ügyfél vagy személyes jelenlétében vagy távolról lesz azonosítva. Így különösen:

- A Digitális fiókban történő személyes azonosítás esetén az Ügyfél által megadott mobilszámot ellenőrzi a Bank azzal, hogy egy egyszeri jelszót küld rá, és megkéri az Ügyfelet, hogy adja meg az egyszeri jelszót.
- A Távoli Digitális Banki Szolgáltatások esetén az online azonosítás során az Ügyfél egy Mobil vagy reszponzív webes felületen azonosítja magát a belépési azonosítójával és egy olyan egyszeri jelszóval, amit a PIN megadásával a saját TOKEN-jén hoz létre, és egy további OTP megadásával, amit SMS-ben az ellenőrzött mobilszámára kap meg.
- A Digitális akvizíció során történő videoazonosítás esetén az Ügyfél által megadott mobilszámra SMS-ben küldött OTP-vel lesz azonosítva az Ügyfél.

Minden azonosítási eljárást a Bank helyi előírásai szerint hajtanak végre, a pénzmosás elleni szabályozással megfelelő eljárásban vagy személyes jelenlét ellenőrzésével.

Az Ügyfél azonosítását a Bank azelőtt elvégzi, hogy a minősített aláírási tanúsítvány kibocsátása megkezdődne.

Sikeres azonosítás esetén az Ügyfél a Távoli Digitális Aláírási Szolgáltatás aktiválását le tudja folytatni, és alá tudja írni a vonatkozó szerződéseket.

4.4.2 A Távoli Digitális Aláírás szolgáltatás aktiválása magánszemély által és a vonatkozó szerződés aláírása

Ahhoz, hogy a távoli digitális aláírást aktiválja és aláírja a hitelesítésszolgáltatási szerződést, a Kérelmezőnek a következő eljárási lépéseket kell megtennie különféle csatornákon:
Távoli digitális banki szolgáltatások:

- Belép egy Digitális banki szolgáltatásba az érintett Bank által meghatározott hitelesítési eljárások használatával;
- Ha szükséges, személyes adatai helyességének ellenőrzése és megerősítése azzal a céllal, hogy aktiválja a minősített elektronikus aláírási tanúsítványát,
- Megindítja a tanúsítvány igénylését;
- A digitális banki szolgáltatástól függően PIN megadásával a TOKEN segítségével létrehoz egy OTP-t. Ez a folyamat biztosítja az erős ügyfélhitelesítési mechanizmus érvényesülését (lásd a 2017. november 27-i (EU) 2018/389 felhatalmazáson alapuló bizottsági rendelet 4-9. cikkét);
- Megvizsgálja a hitelesítésszolgáltatási szerződés feltételeit, a minősített elektronikus aláírási tanúsítványok kibocsátását elindítja és a szerződést digitális aláírja azáltal, hogy megadja a TOKEN által a PIN beadását követően létrehozott OTP-t;
- Kiegészítő biztonsági intézkedésként további olyan OTP megadása, amit az ellenőrzött mobilszámára kap meg az Ügyfél SMS-ben;
- A Bank aláírásával megerősíti a Távoli Digitális Aláírás szolgáltatás aktiválását.

Fiók vagy Digitális akvizíciós portál:

- Hozzáférés a Digitális akvizíciós portálhoz vagy személyesen befárad a Bank valamely fiókjába;
- Ha szükséges, elfogadja a hitelesítésszolgáltatási szerződés szerinti szabályokat;
- Ha szükséges, személyes adatai helyességének ellenőrzése és megerősítése azzal a céllal, hogy aktiválja a minősített elektronikus aláírási tanúsítványát;
- A tanúsítvány igénylésének megindítása. Ha az Ügyfél a tanúsítvány aktiválását a Digitális fióki csatorna útján igényli, a hitelesítésszolgáltatási szerződés aláírása előtt egy kérelmezői űrlapot kell kitölteni;
- Az ellenőrzött mobilszámára megkapja az OTP-t egy SMS-ben. A személyes és a videoazonosításhoz az Ügyfélnek nem kell biztonsági PIN-t megadnia.
- Megvizsgálja a hitelesítésszolgáltatási szerződés nyújtásához című szerződés feltételeit, a minősített elektronikus aláírási tanúsítvány kibocsátását megindítja, és a szerződést digitálisan aláírja azáltal, hogy megadja az OTP-t. A hitelesítésszolgáltatási szerződést kézzel is alá lehet írni.
- A Bank aláírásával megerősíti a Távoli Digitális Aláírás szolgáltatás aktiválását.

A Távoli digitális aláírási szolgáltatáshoz kapcsolódó kiegészítő dokumentációt a digitális aláírás szolgáltatáshoz kapcsolódó hitelesítésszolgáltatási szerződés megkötése előtt az Ügyfél rendelkezésére kell bocsátani.

4.4.3 A Távoli Digitális Aláírás Szolgáltatás aktiválása Jogi Személy Ügyfél által és a vonatkozó szerződés aláírása

[Magyarországon nem elérhető szolgáltatás.]

4.4.4 A Birtokosok kulcspár generálási eljárása (nyilvános és magánkulcsok)

A digitális aláírás aktiválása és a hitelesítésszolgáltatási szerződés Kérelmező általi aláírása során automatikusan kezdeményezni kell annak a kulcspárnak a generálási eljárását (nyilvános és magánkulcsok), amely lehetővé teszi az Ügyfél számára, hogy használja a digitális aláírás szolgáltatást.

A Birtokos a magánkulcsot különösen az érintett Nemzetközi leánybank által felkínált szolgáltatásokhoz és termékekhez kapcsolódó dokumentumokat aláírására használhatja, míg a nyilvános kulcsot magának az aláírásnak a hitelesség-igazolásához kell használni.

A digitális aláírás védelmére kezdetben használt tanúsítvány jelszót később a Birtokos megváltoztathatja, saját döntésétől függően. A tanúsítvány jelszó megváltoztatásához, a Birtokosnak a választott közvetlen csatornán (azaz web, mobil) belüli speciális funkciót kell használnia, amely OTP-vel védett (lásd az alábbi 4.6 pontot).

A Birtokosnak a tanúsítvány jelszó és az OTP eszköz kombinált használatából adódó adatokat titokban kell tartania, a [DPCM] 8. cikk (5) pontja által előírtak szerint.

A fent említett eljárás használatával létrehozott kulcspárt (nyilvános és magánkulcs) egy – a Hitelesítésszolgáltató tulajdonában levő – biztonságos eszköz generálja (hardver biztonsági modul).

A Birtokos és a Hitelesítésszolgáltató közötti mindenfajta kommunikációt, beleértve a különböző kérelmek beérkezésének visszaigazolását, beleértve a digitális aláírási szolgáltatás aktiválását, a Nemzetközi leánybank által biztosított internetes banki szolgáltatáson / mobilbanki szolgáltatáson belüli aktív postaláda használatával kell elküldeni.

4.4.5 Elektronikus aláírási célú minősített tanúsítványok kibocsátása

A minősített elektronikus aláírási tanúsítványok a kulcspár-generálás véglegesítése után kerülnek kibocsátásra, mint azt fent jeleztük.
A minősített elektronikus aláírási tanúsítványok kibocsátása teljes mértékben transzparens a Kérelmező számára, aki ebben a konkrét fázisban nem áll kapcsolatban a Hitelesítésszolgáltatóval.
A vonatkozó jogszabályoknak megfelelően az elektronikus aláírás kibocsátását szolgáló minősített tanúsítvány iránti kérelmeket a Hitelesítésszolgáltató az elektronikus aláírási célú egyes minősített tanúsítványok kibocsátási dátumát követően legalább 20 (húsz) évig megőrzi. Különösen fontos tárolni elektronikus formában minden olyan követési útvonalat, amely e műveletnek az idők során történő végrehajtási bizonyításához szükséges.

4.5 A minősített elektronikus aláírási tanúsítvány visszavonási eljárása

A [DPCM]-nek megfelelően, a minősített elektronikus aláírási tanúsítvány visszavonását az alábbi felek az alábbiakban meghatározott módon kérhetik:

- a Birtokos,
- a Hitelesítésszolgáltató,
- a Regisztrációs szervezet.

4.5.1 A Birtokos által benyújtott visszavonási kérelem

A Birtokos a minősített aláírási tanúsítvány visszavonására vonatkozó kérelmét a fiókban adhatja be.

A visszavonási kérelem benyújtását követően a minősített elektronikus aláírási tanúsítvány visszavonásához szükséges automatikus mechanizmusok a Birtokos számára átlátható módon történik.

Ha a Birtokos a hitelesítésszolgáltatási szerződést felmondja, a Regisztrációs szervezetnek haladéktalanul értesítenie kell a Hitelesítésszolgáltatót, hogy az intézkedjen a megfelelő aláírási tanúsítvány visszavonása ügyében.
A visszavonás eredményeként a Birtokos már semmilyen dokumentumot nem tud aláírni a korábban hozzárendelt kulcsok használatával, míg az elektronikus aláírási célú minősített tanúsítvány visszavonását megelőzően a Birtokos által aláírt összes dokumentum érvényes és érvényben marad.

4.5.2 Jogi Személyek által benyújtott visszavonási kérelmek

[Magyarországon nem elérhető szolgáltatás]

4.5.3 Regisztrációs szervezet részéről

Kivéve az indokolt sürgősségű eseteket, az elektronikus aláírási célú minősített tanúsítványt visszavonni szándékozó Hitelesítésszolgáltatónak vagy Regisztrációs szervezetnek előre tájékoztatnia kell a Birtokost, megadva a visszavonás okait.

A Regisztrációs szervezetnek haladéktalanul értesítenie kell a Hitelesítésszolgáltatót arról, hogy szükség van egy elektronikus aláírási célú minősített tanúsítvány visszavonására. A Hitelesítésszolgáltatónak a következő esetekben kell visszavonnia a tanúsítványt:

1. ha a Birtokos azt kifejezetten kéri;
2. ha megállapítja, hogy a Birtokos adatai pontatlanok vagy hiányosak a tanúsítvány nyilvántartásában;
3. amennyiben hivatalos értesítést kap a Birtokos haláláról;
4. amennyiben hivatalos értesítést kap a Birtokos üzleti képességeinek elvesztéséről;
5. amennyiben megállapítja, hogy a Birtokos hamis adatokat használt a tanúsítvány kibocsátásához.

4.5.4 A minősített elektronikus aláírási tanúsítvány visszavonási eljárásának befejezése

A minősített elektronikus aláírási célú tanúsítvány visszavonási eljárásának befejezésekor a Hitelesítésszolgáltató egy új CRL-t hoz létre, amelyet közzétesz az internetes kapcsolaton keresztül elérhető címtárjában közzétételre kerül.

A CRL közzétételét a 4.9.2 cikk határozza meg. Ezen túlmenően az elektronikus aláírási célú minősített tanúsítvány eredményes visszavonását ellenőrző napló rögzítik.

4.6 A minősített elektronikus aláírási tanúsítvány felfüggesztésének eljárása

A [DPCM] szerint egy minősített aláírási tanúsítvány felfüggesztését az alábbi személyek kérhetik:

- a Hitelesítésszolgáltató;
- a Regisztrációs szervezet.

Indokolt és sürgős esetek kivételével a Hitelesítésszolgáltató vagy a Regisztrációs szervezet köteles a Birtokost előzetesen értesíteni arról, ha a minősített aláírási tanúsítványt fel kívánja függeszteni, egyben megjelölve a felfüggesztés indokait is.

4.7 A PIN és az OTP eszköz (TOKEN) elvesztése

A Birtokos a hitelesítése egyik lehetséges eszközeként OTP eszközt is használhat. Az OTP eszköz elvesztése vagy ellopása estén a Birtokosnak a hitelesítésszolgáltatási szerződés szerint kell eljárnia. A PIN elvesztése esetén az eljárás azonos az OTP eszköz elvesztésére vonatkozó eljárással.

4.8 Kulcscsere eljárás

4.8.1 A Birtokos aláíró kulcsainak cseréje

A [DPCM] szerint a Hitelesítésszolgáltatónak kell meghatároznia az elektronikus aláírási célú minősített tanúsítvány lejáratát, és a kulcsok érvényességi időszakát, a kulcs hosszától és a kulccsal használt szolgáltatásoktól függően.

A kulcsok érvényességi periódusa egybeesik a kapcsolódó elektronikus aláírási célú minősített tanúsítvány érvényességi idejével, ami három (3) év.

Elektronikus aláírási célú új minősített tanúsítvány kibocsátását csak akkor lehet kérni, ha az előző tanúsítvány lejárt vagy azt visszavonták.

A Birtokos egyidejűleg soha nem rendelkezhet két (2) példánnyal elektronikus aláírási célú aktív minősített tanúsítvánnyal.

4.8.2 Tanúsítványkulcsok cseréje

A tanúsítványkulcsok cseréjét a Hitelesítésszolgáltató végzi, az irányadó jogszabályokat és szabályozásokat előírva.

4.9 A minősített elektronikus aláírási tanúsítványok könyvtár kezelése

4.9.1 A minősített elektronikus aláírási tanúsítványok könyvtár

A Hitelesítésszolgáltató által kibocsátott, elektronikus aláírási célú összes érvényes tanúsítvány egy „tanúsítvány nyilvántartásba” van elmentve.

A nyilvános könyvtár a következő információkat tartalmazza:
- a Hitelesítésszolgáltató kulcsainak tanúsítványait;
- a tanúsítvány szerződéshez kapcsolódó tanúsítványokat;
- az AgID aláírási kulcsainak tanúsítványait;
- az elektronikus aláírási célú visszavont minősített tanúsítványok listáját.

Az elektronikus aláírási célú visszavont minősített tanúsítványok listáját HTTP protokollon keresztül is közzéteszik a következő címeken:
- http://crl2.ca.intesasanpaolo.com/FirmaDigitale01/CRL02.crl, és
- http://crlcl.ca2.intesasanpaolo.com/qc/CRL$$.crl

A Hitelesítésszolgáltató megbízható rendszereket használ az elektronikus aláírási célú minősített tanúsítványok könyvtárai és nyilvános könyvtárai kezeléséhez, és olyan módszereket használ, melyek a következőket biztosítják:
- csak meghatalmazott személyek vihessenek be adatokat és végezhessenek változtatásokat,
- az információ hitelessége legyen ellenőrizhető,
- a tanúsítványok nyilvános megtekintése a Birtokos által megengedett mértékben áll rendelkezésre,
- a kezelő tudomására juthasson minden olyan esemény, ami megsérti a biztonsági követelményeket.

4.9.2 A minősített elektronikus aláírási tanúsítványok és a CRL közzététele

A minősített elektronikus aláírási tanúsítványok a [DPCM] 34. cikkében előírt eljárásnak megfelelően kerülnek közzétételre.

A CRL-t óránként hozzák létre és teszik közzé a nyilvános könyvtárban, kivéve olyan műszaki akadály esetén, mely meghaladja a Hitelesítésszolgáltató hatáskörét.

A nyilvános könyvtárhoz a nyilvános Internet hálózaton lehet hozzáférni, a CRL Elosztási Pont Bővítmény az elektronikus aláírási célú minősített tanúsítványok részében specifikált címen.

4.9.3 A minősített elektronikus aláírási tanúsítványok könyvtárának reprodukálása különböző honlapokon

A [DPCM] előírásainak megfelelően a Hitelesítésszolgáltató átmásolja a tanúsítvány könyvtárt számos honlapra, biztosítva az összes példány konzisztenciáját és sértetlenségét.

A részleteket lásd a 4.13.5 pontban, melynek címe „Fő helyszín sérülése”.

4.10 Személyes adatok védelmével kapcsolatos eljárások

A minősített elektronikus aláírási tanúsítvány szolgáltatások teljesítése során a Hitelesítésszolgáltató által a Birtokossal kapcsolatban kapott információt ellenőrizni kell, kivéve azokat az esteket, ahol a Birtokos írásos jóváhagyást bocsátott ki, arra vonatkozóan, hogy az információk bizalmas jellegűek és nem szabad közzé tenni azokat, kivéve a kifejezetten nyilvános használatra szánt adatokat (pl. nyilvános kulcs, az elektronikus aláírási célú minősített tanúsítvány visszavonási dátuma). A jelen Távoli Digitális Aláírási Működési Szabályzat alapján a Hitelesítésszolgáltató nem dolgoz fel „különleges adatokat a GDPR előírásai szerint.

Az azonosítás és adatvédelem területén végrehajtott tevékenységeknek meg kell felelniük a Regisztrációs szervezeti tevékenységet végző Bank nemzeti jogszabályainak. Az egyértelműség végett: a tanúsítványok és az összes kapcsolódó dokumentum és információ tárolásának időtartamát az olasz jog határozza meg, ennek folytán a tárolás időtartamának az olasz jog előírásainak kell megfelelnie.

A fent említett személyes adatokat a Hitelesítésszolgáltatónak a GDPR előírásaival összhangban kell feldolgoznia.

4.11 Az ellenőrzési napló megszervezésére vonatkozó eljárás

A Hitelesítésszolgáltató automatikusan vagy manuálisan rögzíti az ellenőrzési naplóban a [DPCM] 36. cikkében előírt eseményeket. Különösen a következő eseményeket kell rögzíteni:

- az elektronikus aláírási célú minősített tanúsítványok kibocsátása;
- az elektronikus aláírási célú minősített tanúsítványok visszavonása, megszabva a CRL közzétételének napját és időpontját;
- az elektronikus aláírási célú minősített tanúsítványok generálására használt rendszerek munkamenetének kezdete és vége;
- az aláírás eszközeinek megszemélyesítése;
- a tanúsító rendszer biztonságos szobáiba való belépés és az onnan való kilépés.

A Hitelesítésszolgáltató az ellenőrzési naplót a [DPCM] 41. cikk (2) bekezdésével összhangban kezeli.

4.12 Biztonsági másolatok kezelésére vonatkozó eljárás

A Hitelesítésszolgáltató folytonossági tervet készített és foganatosít a jelen Távoli Aláírási Működési Szabályzat alapján nyújtott szolgáltatások vonatkozásában. A vonatkozó eljárások szerint meghozandó legfontosabb intézkedéseket az alábbiakban ismertetjük.

4.12.1 Biztonsági másolatokra vonatkozó eljárás

Naponta készül biztonsági másolat az adatokról, alkalmazásokról, ellenőrzési naplókról valamint minden olyan fájlról, amely az elektronikus aláírási célú minősített tanúsítványokat kezelő rendszer kritikus eljárásainak teljes helyreállításához szükséges. Ennek a folyamatnak a keretében, a biztonsági másolatok létrehozása távolról történik és egy olyan meghatározott központosított rendszer vezérli, mely megfelel az alábbi követelményeknek:

- minimalizálja az emberi beavatkozás és a technikai helyiségekhez való hozzáférés szükségességét;
- egyszerűsíti a biztonsági mentési műveletek és azok ellenőrzésének az ütemezését;
- megnöveli a biztonsági mentési műveletek megbízhatóságát.

4.13 Balesetek és katasztrófák kezelésére vonatkozó eljárás

Ezen eljárások általános vázlatát az alábbiakban ismertetjük.

4.13.1 Számítógépes hibák

Az elektronikus aláírást szolgáló minősített tanúsítványok szolgáltatására használt összes számítógépre egy olyan karbantartási szerződés vonatkozik, amely 24 (huszonnégy) órán belül garantálja a számítógépek aktív üzembe való visszahelyezését hiba esetén.

4.13.2 Szoftverhibák

Az olyan programok vagy adatok sérülése (elvesztés vagy tönkremenetel) esetén, amelyeket egyébként nem lehet helyreállítani, azokat a tárolt biztonsági mentési fájlokból kell visszaállítani.

4.13.3A Hitelesítésszolgáltató aláíró eszközének meghibásodása

A Hitelesítésszolgáltató aláíró eszközének meghibásodása esetén a magánkulcsot újra létre kell hozni egy új aláíró eszközön, a korábban generált kulcsok szegmenseiből kiindulva, olyan sajátos eljárást követve, amely több kezelő együttes beavatkozását igényli. A legfontosabb szegmenseket rejtjelezett formában és különböző tároló eszközökön őriznek, amelyeket különböző vezetők felügyelnek.

Megjegyzés: a legfontosabb szegmensek nem minősülnek a tanúsítványkulcs "másolatának" ([DPCM]), és csak a teljes kulcs helyreállításának céljára használhatók, a fent leírt eljárásnak megfelelően.

Amennyiben a tanúsítványkulcs helyreállítása nem lehetséges, akkor a tanúsítványkulcs meghibásodásával kapcsolatos eljárást kell követni (lásd a következő bekezdést).

4.13.4A tanúsítványkulcs sérülése

Amennyiben a magán tanúsítványkulcs titkossága sérül, a Hitelesítésszolgáltató köteles:
- visszavonni a sérült magánkulcshoz kapcsolódó tanúsítványt;
- értesítést küldeni az AgID-nek a visszavonást követő 24 (huszonnégy) órán belül;
- a visszavont párhoz tartozó magánkulccsal aláírt összes elektronikus aláírási célú minősített tanúsítvány Birtokosát tájékoztatni;
- a sérült kulccsal aláírt összes elektronikus aláírási célú minősített tanúsítványt visszahívni;
- elektronikus aláírási célú minősített tanúsítványokat kibocsátani az új magánkulcs használatával.

4.13.5A fő helyszín sérülése

Amennyiben a helyszín, az épület vagy a rendszer egésze elérhetetlenné válik valamilyen katasztrófa (tűz, árvíz, földrengés stb.) következtében, akkor a katasztrófa-helyreállítási tervet aktiválni kell; a szóban forgó terv az Intesa Sanpaolo összes operatív erőforrására vonatkozik, valamint az időbélyegző szolgáltatást nyújtó harmadik fél erőforrásaira is.

5 A MINŐSÍTETT ELEKTRONIKUS ALÁÍRÁSI TANÚSÍTVÁNNYAL KAPCSOLATOS HITELESÍTÉSSZOLGÁLTATÁS FELFÜGGESZTÉSE

5.1 A minősített elektronikus aláírási tanúsítvánnyal kapcsolatos hitelesítésszolgáltatás megszüntetésére vonatkozó részletes szabályok

A minősített bizalmi szolgáltató hitelesítésszolgáltatásának befejezése előtt legalább 60 (hatvan) nappal korábban a Hitelesítésszolgáltatónak egy speciális közleményt kell küldenie az AgID számára, megjelölve az új Hitelesítésszolgáltatót (ha van ilyen helyettesítő Hitelesítésszolgáltató), valamint a tanúsítványokra vonatkozó nyilvántartás és a kapcsolódó dokumentáció vezetőjét.

Az AgID számára küldött közleménnyel egy időben az összes Birtokost értesíteni kell a tevékenység felfüggesztéséről.

Ha a Hitelesítésszolgáltató nem nevez ki helyettesítő Hitelesítésszolgáltatót, a közleményben egyértelműen rögzíteni kell, hogy a szolgáltatás felfüggesztésének időpontjában még le nem járt, elektronikus aláírási célú minősített tanúsítványok mindegyikét vissza lesz vonva. A minősített elektronikus aláírási tanúsítványokat a visszavonás időpontjában fel kell venni a visszavonási listára.

A szolgáltatás felfüggesztésével kapcsolatos részleteket az Intesa Sanpaolo a Megszüntetési Tervben rögzíti.

6 AZ IDŐREFERENCIÁK KEZELÉSE

6.1 Időbélyegző szolgáltatás

Ez a fejezet a [DPCM] 40. cikk (3) bekezdés p. pontjára vonatkozik.
A Hitelesítésszolgáltató a [DPCM] kikötéseivel összhangban köteles időbélyegző szolgáltatást biztosítani, felhasználva a Hitelesítésszolgáltató által nyújtott olyan szolgáltatásokat, melyek megfelelnek azon országok működési követelményeinek, ahol a Bank működik. Az időbélyegző kibocsátására és beszerzésére irányuló kérelem továbbítási eljárásainak leírása a vonatkozó törvényekkel és szabályokkal összhangban megtalálható a jelen szolgáltató működési szabályzatában.

6.2 Az időreferencia pontossága

Az időreferencia kezelő rendszer az olasz Istituto Elettrotecnico Nazionale (IEN) „Galileo Ferraris” által kibocsátott jellel szinkronizált rádióvevőtől kérdezi le az időt.
Időbélyegző generálásakor a TSA szerver a rendszerórából lekérdezi a dátumot/időt, ami összhangban van az UTC (Coordinated Universal Time – egyezményes koordinált világidő) pontos idejével, egy külső vevőről kapott szinkronjelnek köszönhetően, amely azonosítja a GPS műholdhálózat által kibocsátott időjel minőségét. Az így kapott időjel megfelel az alkalmazandó törvények és szabályok által megkövetelt pontossági határnak.

7 A DIGITÁLIS ALÁÍRÁS ELLENŐRZÉSÉRE VONATKOZÓ ELJÁRÁS

Ez a fejezet a [DPCM] 40. cikk (3) bek. e. pontjára hivatkozik.

7.1 Az ellenőrzési alkalmazás

A Bank által működtetett közvetlen csatornák „Dokumentumaim” felületén a Birtokosnak lehetősége van digitálisan aláírt dokumentumait megtekinteni. A szóban forgó dokumentumok PDF formátumban vannak elmentve, és a Birtokos által választott távoli csatornától (web, mobil) függően a Birtokos mindig ki tudja választani azt az ahhoz a csatornához tartozó alkalmazást, amely lehetővé teszi számára, hogy ellenőrizze az alkalmazott digitális aláírást. A Birtokos a digitálisan aláírt dokumentumokat emailben is megkaphatja.

A [DPCM] 42. cikk (2) bekezdésében előírtak szerint a Birtokos számára rendelkezésre álló ellenőrző rendszerek és a Hitelesítésszolgáltató által kibocsátott digitális aláírt dokumentumok átjárhatók.

7.2 Dokumentum formátum

A Bank közvetlen csatornáin a Birtokosnak elküldött dokumentumok megfelelnek az irányadó jogszabályoknak és szabályozásoknak, és az elektronikus formátumú dokumentumok nem tartalmazhatnak „*makró utasításokat, végrehajtható kódokat, vagy egyéb olyan elemeket, amelyek az ilyen dokumentumokban szereplő műveletek, tények vagy adatok módosítására képes funkciókat aktiválhatnak*”.

7.3 A CRL elérésével kapcsolatos figyelmeztetés

A Birtokosnak figyelembe kell vennie a CRL-ben szereplő információ frissítéséhez szükséges technikai időket.

Az ilyen technikai idők különösen akkor fontosak, ha a Birtokos, a Regisztrációs szervezet vagy a Hitelesítésszolgáltató az elektronikus aláírási célú minősített tanúsítványt vissza kívánja vonni, vagy azt újra aktiválni kívánja, illetve abban az esetben, amikor a Hitelesítésszolgáltató a visszavonási kérésekhez kapcsolódó technikai/adminisztratív eljárásokat, valamint a CRL-hez kapcsolódó frissítést végzi.

Egy dokumentum minősített aláírási tanúsítvánnyal történő aláírásakor ellenőrizni kell a CRL listát, így győződve meg arról, hogy az adott, elektronikus aláíráshoz használt minősített tanúsítvány nincs-e visszavonva.

8 MŰKÖDÉSI ELJÁRÁS DIGITÁLIS ALÁÍRÁSOK GENERÁLÁSÁHOZ

Ez a fejezet a [DPCM] 40. cikk (3) s bekezdésére vonatkozik.

A szolgáltatás sajátosságai nem tartalmazzák a Kérelmező eszközére (személyi számítógép, okos telefon stb.) telepítendő aláírás alkalmazás kiszállítását; mindazon funkciót, mely lehetővé teszi a Birtokos számára, hogy egy vagy több digitális dokumentumot aláírhasson, ezt közvetlenül a digitális banki szolgáltatás használati szerződésének és/vagy hitelesítésszolgáltatási szerződésének azon különös fejezetébe kell elhelyezni, melyet a Nemzetközi leánybank használ.

Az ezzel az alkalmazással létrehozott digitális aláírások megfelelnek a [DPCM] 4. cikk (2) bekezdésében lefektetett aláíró algoritmusokra vonatkozó követelményeknek.