Manuali Operacional Digical
Divizioni Ndërkombëtar i Bankave Filiale

Shpërndarja:	PUBLIK
Kodi i dokumentit:	ISP - SCD - 04 - 2022 - 06
	Kompania Sherbimi Kodi Viti Versioni

VERSIONET E MANUALIT OPERACIONAL TË NËNSHKRIMIT DIXHITAL NË DISTANCË

Versioni	Data e publikimit	Përshkrimi i ndryshimit
01	01/12/2018	Versioni i parë
02	02/07/2019	Rishikimi vjetor
03	31/10/2019	Rishikimi
04	30/11/2019	Përditësimi i dokumentit pas zëvendësimit të Vendimit 45 AgID
05	31/05/2020	Përditësimi i dokumentit pas krijimit të CA për Vazhdimësinë e Biznesit
06	30/06/2022	Përditësimi pas Inspektimit te AgID

PERMBAJTJA

1. TË DHËNA TË PËRGJITHSHME

1.1 Vështrim i përgjithshëm

"Manuali Operacional i Nënshkrimit Dixhital në Distancë" (siç përcaktohet më poshtë) ka si qëllim rregullimin e certifikatave të kualifikuara për shërbimet e nënshkrimit elektronik të ofruara - në përputhje me Dekretin Legjislativ 82/2005 (Kodi i Administrimit Dixhital), i ndryshuar në vijim, dhe legjislacionin dhe rregulloret kombëtare dhe europiane në fuqi dhe të zbatueshme - nga Intesa Sanpaolo SpA për Përdoruesin (siç përcaktohet më poshtë) të Bankës Ndërkombëtare Filiale (siç përcaktohet më poshtë) në lidhje me shërbimet e kanaleve alternative - multichannel (pra aksesi nga Përdoruesi në shërbimet e ofruara nga Bankat Ndërkombëtare Filialeve përmes kanaleve dhe degës në distancë).
Manuali Operacional i Nënshkrimit Dixhital në Distancë i referohet gjithashtu rregullave teknike për zbatimin e kuadrit ligjor për nënshkrimin dixhital që parashikohet në DPCM, datë 22/02/2013. Nëse ndodh ndonjë ndryshim i ligjit, ky manual operacional do të modifikohet rregullisht për këtë qëllim.

1.2 Përkufizimet dhe interpretimet

Termat në vijim që përdoren në Manualin Operacional të Nënshkrimit Dixhital në Distancë do të kenë kuptimet e mëposhtme:

- **"Aplikant**": personi që kërkon lëshimin e një certifikate të kualifikuar për nënshkrimin elektronik; për individët, aplikanti është i njëjti me Titullarin; për personat juridik, Aplikanti është gjithmonë një përfaqësues ligjor i personit juridik (mund të ketë më shumë se një Përfaqësues Ligjor për Personin Juridik);
- "**Degë**": vendi ku zhvillohet aktiviteti i biznesit midis klientit dhe Bankës, kjo përfshin të gjitha ambientet, zyrat dhe vendndodhjet e Bankës Ndërkombëtare Filiale.
- "**Autoriteti i Certifikimit**": ofruesi i shërbimit të besimit, i cili është i autorizuar të lëshojë certifikata të kualifikuar për nënshkrimin elektronik përmes një procedure certifikimi që është në përputhje me standardet ndërkombëtare dhe ligjet dhe rregulloret europiane dhe kombëtare. Për qëllimet e këtij manuali operacional RDS, Autoriteti i Certifikimit është Intesa Sanpaolo S.p.A
- **"Person juridik":** jo-konsumator, pra një kompani publike ose private ose një person fizik që vepron brenda biznesit të tij / saj ose si një profesionist i vetëpunësuar, i cili nënshkruan Marrëveshjen e Përdorimit të Shërbimit të Bankës Dixhitale me një Bankë Ndërkombëtare Filiale dhe autorizon një Aplikant / Titullar që të përdor certifikatën e kualifikuar për nënshkrimin elektronik të lëshuar në emër të tij;
- **"Përdorues**": Përdoruesi i fundit individ ose person juridik, nënshkrues i Marrëveshjes për Ofrimin e shërbimeve të Certifikimit që lidhet me Bankat Ndërkombëtare Filiale.
- **"Blerje dixhitale"**: një kanal për të kryer një procesin e blerjes dixhitale përmes identifikimit me video që kryhet nga operatori bankë dhe dokumentit të identifikimit që paraqet Klienti;
- **"Bankat Ndërkombëtare Filiale"**: çdo Bankë Ndërkombëtare Filiale që i përket Grupit Intesa Sanpaolo;
- **"Titullari**": Përdoruesi në emër të të cilit është lëshuar një certifikatë e kualifikuar për nënshkrim elektronik; titullari është i autorizuar të përdorë një certifikatë të tillë për të nënshkruar në mënyrë dixhitale dokumente elektronike, duke siguruar autenticitetin e origjinës së dokumenteve elektronike dhe integritetin e përmbajtjes së tij, në përputhje me kufizimet e përcaktuara në Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit të Bankave Ndërkombëtare Filiale;
- **"Intesa Sanpaolo"**: Intesa Sanpaolo S.p.A., ofruesi i certifikatave të kualifikuara për nënshkrimin elektronik
- **"Fjalëkalimi me një përdorim (OTP)":** fjalëkalim i vlefshëm vetëm për një transaksion dhe i cili gjenerohet dhe vihet në dispozicion Titullarit menjëherë përpara operacionit të nënshkrimit dixhital. OTP i dërgohet me sms klientit nëse kanalet janë "blerja dixhitale" ose degë. OTP gjenerohet nga TOKEN për shërbime bankare dixhitale në distancë.

- **"Autoriteti i Regjistrimit**": subjekti i caktuar kryesisht që (i) të identifikojë Aplikantët dhe të lidhë kontratën me Aplikantët, duke garantuar saktësinë e identitetit të tyre, (ii) t'i sigurojë Aplikantëve të gjithë informacionin mbi certifikatat e kualifikuara për nënshkrimin elektronik dhe kufizimet e përdorimit të tyre, (iii) te lidh kontratën me Aplikantët në emër dhe për llogari të Intesa Sanpaolo dhe (iv) t'i dorëzojë Intesa Sanpaolo kërkesat për revokim dhe pezullim të certifikatave. Për qëllimet e këtij manuali operacional RDS, Autoriteti i Regjistrimit është ndonjë prej Bankave Ndërkombëtare Filiale të Intesa Sanpaolo S.p.A që ka nënshkruar me Intesa Sanpaolo S.p.A. një marrëveshje për certifikata të kualifikuar për nënshkrimin elektronik;
- **"Manuali operacional i nënshkrimit Dixhital në Distancë (RDS)"**: ky dokument, i ndryshuar dhe plotësuar në vijim.
- **"Banka"**: çdo Bankë Ndërkombëtare Filiale që i përket Grupit Intesa Sanpaolo
- **"TOKEN"**: Sistemet e sigurta të vërtetimit dhe autentifikimit sigurojnë certifikimin dhe autentifikimin strikt të klientit (SCA); përdoret për të gjeneruar fjalëkalimin me një përdorim (OTP) pas verifikimit të kodi PIN
- **"Kodi Privat":** është elementi i rezervuar i një palë kodeve asimetrikë të cilat ruhen në mënyrë të mbrojtur nga Ofruesi i Shërbimeve të Certifikimit në një pajisje të përshtatshme nënshkrimi
- **"Kodi Publik":** është elementi i një palë kodeve asimetrikë me të cilët kryhet vërtetimi dhe autentifikmi i nënshkrimit elektronik.

1.2.1 Referenca për dispozitat ligjore

[Dekreti legjislativ 82/2005]	Dekreti Legjislativ Nr. 82, datë 7 Mars 2005, publikuar në Fletoren Zyrtare nr. 112, datë 16 maj 2005, - Shtojca e zakonshme nr. 93 "Kodi i Administrimit Dixhital", i përditësuar me Dekretin Legjislativ nr. 217, datë 13 Dhjetor 2017, publikuar në Fletoren Zyrtare nr.9, Janar 2018.
[DPCM]	Dekreti i Kryeministrit, datë 22 shkurt 2013 - Rregullorja teknike për krijimin, aplikimin dhe verifikimin e nënshkrimeve elektronike të avancuara, të kualifikuara dhe dixhitale, në përputhje me nenin 20 (3), 24 (4), 28 (3), 32 (3) germa b), 35 (2), 36 (2) dhe 71.
[CNIPA/CR/48]	CNIPA / CR / 48 Qarkorja nr. 48, datë 6 Shtator 2005 (publikuar në Fletoren Zyrtare nr. 213, datë 13 Shtator 2005), Procedura për paraqitjen e aplikimit për t'u regjistruar në listën publike të ofruesve të shërbimeve të certifikimit, në përputhje me nenin 28 (1) të Dekretit Presidencial nr. 445, datë 28 dhjetor 2000.
Rregullorja BE 910/2014 – eIDAS	Rregullorja (BE) N. 910/2014 e Parlamentit Evropian dhe e Këshillit e 23 korrikut 2014 mbi identifikimin elektronik dhe shërbimet e mirëbesimit për transaksionet elektronike në tregun e brendshëm dhe shfuqizimin e Direktivës 1999/93 / KE.
Rregullorja BE (BE) N°679/2016 – GDPR	Rregullorja (BE) Nr. 679/2016 e Parlamentit dhe e Këshillit Evropian , datë 27 Prill 2016 për mbrojtjen e personave fizikë në lidhje me përpunimin e të dhënave personale dhe lëvizjen e lirë të këtyre të dhënave, dhe shfuqizimin e Direktivës 95/46 / KE (Rregullorja e përgjithshme për mbrojtjen e të dhënave).
Vendimi i AgID nr.121/2019	Udhëzime që përmbajnë Rregullat Teknike dhe Rekomandimet në lidhje me gjenerimin e certifikatave elektronike të kualifikuar, nënshkrimet dhe vulat elektronike të kualifikuara dhe vlefshmërinë e kualifikuar elektronike të kohës

1.3 Referencat për standardet

[LDAP2] Zeilenga, " Protokolli i aksesit në Direktorin Lightweight, version 2", Internet RFC 3494, Mars 2003.

[PKCS7] B. Kaliski, “PKCS#7: Sintaksa e mesazhit kriptografik Versioni 1.5”, Internet RFC 2315, Mars 1998.

[PKCS10] B. Kaliski, "PKCS#10: Sintaksa e Kërkesës së Certifikimit - Versioni 1.7", Internet RFC 2986, Nëntor 2000.

[SHA1] ISO/IEC 10118-3:2018, " Teknologjia e informacionit - Teknika të sigurisë - funksionet Hash - Pjesa 3: Funksionet e përkushtuara Hash", 2018.

[SHA-256] ISO/IEC 10118-3:2018, " Teknologjia e informacionit - Teknika të sigurisë - funksionet Hash - Pjesa 3: Funksionet e përkushtuara Hash".

[X500] ISO/IEC 9594-1:2008, ISO/IEC 9594-2:2008 “Teknologjia e informacionit - Ndërlidhja e sistemeve të hapura - Direktoria: Përmbledhje e koncepteve, modeleve dhe shërbimeve”.

[X509] ISO/IEC 9594-8:2008 “Teknologjia e informacionit - Ndërlidhja e sistemeve të hapura - Direktoria: Kuadrat e certifikatave të kodeve publik dhe dhënies së certifikatave”.

[RFC3647] Internet X.509 Politika e certifikatave të Infrastrukturës kryesore Publike dhe Kuadri i Praktikave të certifikimit të S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu.

[RFC 3778] Aplikacioni PDF Taft, Pravetz, Zilles, Masinter, Maj 2004.

1.4 Shkurtimet

Shprehjet e mëposhtme që përdoren në Manualin Operacional të Nënshkrimit Dixhital në Distancë do të kenë shkurtimet e mëposhtme:

AgID Agjencia për Italinë Dixhitale,

CRL Lista e Revokimit të Certifikatave

CPS Deklarata e Praktikës së Certifikatës

DBMS Sistemi i menaxhimit të bazës së të dhënave

DN Emër i dalluar/njohur

DNS Sistemi i Emrave të Domenit

DPR Dekret Presidencial

HSM Moduli i Sigurisë së Harduerit

HTTP Protokolli i Transferimit HyperText

ITSEC Kriteret e vlerësimit të sigurisë së teknologjisë së informacionit

LDAP Protokolli i aksesit në Direktorinë Lightweight

NEI Instituti Kombëtar elektroteknik "Galileo Ferraris" (në italisht "Istituto Elettrotecnico Nazionale")

OTP Fjalëkalimi me një përdorim

PDF	Formati i Dokumentit Portabël
PIN	Numri Personal i Identifikimit
PKCS	Standardi Kryesor i Kriptografisë Publike
RDS	Nënshkrimi dixhital në distancë
RFC	Kërkesë për komente
RSA	Rivest-Shamir-Adleman
SHA-1	Funksioni i Sigurisë Hash 1
SHA-2	Funksioni i Sigurisë Hash 2
SSL	Secure Sockets Layer - Shtresa e sigurisë
URL	Lokalizuesi Uniform i Burimit

2. HYRJE

Nënshkrimi dixhital bazohet në kodet asimetrikë, një publik dhe një privat, të cilat sigurojnë vërtetësinë dhe autenticitetin e origjinës së dokumenteve elektronike të nënshkruara në mënyrë dixhitale dhe integritetin e përmbajtjes së tyre ndaj një ose më shumë marrësve që, nga ana tjetër, mund të verifikojnë vlefshmërinë përkatëse.

Dispozitat e reja të parashikuara në nenin 8 të [DPCM] lejojnë që Autoriteti Certifikues të ruajë kodet privatë të Mbajtësve (pra kodet që përdoren për të krijuar një nënshkrim dixhital) në pajisjet speciale të sigurisë (pra HSM), duke siguruar që përdorimi i kodeve do t'i jepet ekskluzivisht mbajtësit/titullarit, sikundër parashikohet në nenin 11 (2) [DPCM].

Rrjedhimisht, përdorimi i nënshkrimit dixhital nuk është më subjekt i zotërimit të setit të nënshkrimit dixhital nga titullari/mbajtësi (p.sh. karta inteligjente, lexues special dhe softueri përkatës), dhe autoritetet e certifikimit dhe regjistrimit mund të ofrojnë shërbime të nënshkrimit dixhital përdoruesve përmes kanaleve direkte (pra internetit, ueb, celularit).

Mbajtësi/titullari do të fillojë procesin e nënshkrimit dixhital përmes përdorimit të një fjalëkalimi me një përdorim - OTP (ose marrjes së një numri të certifikuar në celular ose, në Shërbimin Bankar në Distancë, të gjeneruar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN), ndërkohë garantohet kontrolli i vetëm i Mbajtësit/Titullarit. Fillimi i procesit, nëse kryhet në Degë, mund të ndodhë gjithashtu përmes lexuesit të kartave (pra Mbajtësi/Titullari do të jetë në gjendje të kryejë hapin e parë duke skanuar kartën e tij të debitit pranë lexuesit të kartave në Degë).

Në Manualin Operacional të Nënshkrimit Dixhital në Distancë shpjegohen proceset e mëposhtme:

- Procedurat e gjenerimit dhe menaxhimit të kodeve të nënshkrimit në shërbimin e Nënshkrimit Dixhital të Distancë të ofruar nga Intesa Sanpaolo;

- Procedura e aktivizimit të nënshkrimit dixhital në distancë dhe mekanizmi i rreptë i autentifikimit brenda bankës dixhitale në bazë të procedurës së autentifikimit dhe vërtetimit të përcaktuar nga Bankat Ndërkombëtare Filiale;

- Roli i Autoritetit të Certifikimit dhe Autoritetit të Regjistrimit, në përputhje me ligjet dhe rregulloret në fuqi.

Manuali Operacional i Nënshkrimit Dixhital në Distancë i referohet të gjitha Bankave Ndërkombëtare Intesa Sanpaolo që janë pjesë e Divizionit Ndërkombëtar të Bankave Filiale.

Paragrafët e mëposhtëm i referohen kërkesave që burojnë nga neni 40 (3) a, b dhe c të [DPCM].

2.1 Detajet e identifikimit të Autoritetit të Certifikimit

Shërbimi i certifikimit ofruar nga subjekti i mëposhtëm:

Emri:	**Intesa Sanpaolo S.p.A.**
Selia:	**Piazza San Carlo, 156 10121 Turin**
Përfaqësuesi ligjor:	**Carlo Messina, Administrator i Deleguar dhe DPE**
Nr. Regjistrimi në Regjistrin Tregtar të Torinos	**Regjistri Administrativ Ekonomik (REA) nr. 00799960158**
TVSH nr.:	**10810700152**
Nr. i telefonit (paneli):	(+39) 011 555 1
Identifikuesi i Objektit ISO (OID):	**1.3.6.1.4.1.20052**

Uebsajti i përgjithshëm (informacion):	**www.intesasanpaolo.com**
Uebsajti i Shërbimit të Certifikimit Dixhital:	**ca.intesasanpaolo.com**

2.2 Identifikimi i Manualit Operacional të Nënshkrimit Dixhital në Distancë

Manuali Operacional i Nënshkrimit Dixhital në Distancë identifikohet me kodin e dokumentit ISP-SCD-04-2022-06 (që përcaktohet edhe në faqen e titullit) dhe i referohet certifikatave me OID e meposhtme: 1.3.6.1.4.1.20052.1.3.1 dhe 1.3.6.1.4.1.20052.1.4.3.

Manuali Operacional i Nënshkrimit Dixhital në Distancë është botuar në faqen e internetit të Autoritetit të Certifikimit dhe për këtë arsye është e disponueshme në internet.

Versioni aktual Manualit Operacional të Nënshkrimit Dixhital në Distancë është i disponueshëm në formatin elektronik:

- Në faqen e internetit të Autoritetit të Certifikimit (https://ca.intesasanpaolo.com/);
- në faqen e internetit të AgID;
- në faqen e Internet Banking të Divizionit Ndërkombëtar të Bankave Filiale

Në rast mospërputhjesh, versioni që publikohet në faqen e internetit të AgID do të mbizotërojë në çdo kohë.

2.3 Personi përgjegjës për Manualin Operacional të Nënshkrimit Dixhital në Distancë

Veprimi	Zyra pergjegjese	Funksioni
Redaktimi	Zyra: Infrastruktura, Rrjeti, Zgjidhjet Info-fizike dhe te mbrojtjes se te dhenave	Sikuria Kibernetike dhe Menaxhimi i Vazhdimesise se Biznesit
Miratimi	Giorgio Cusmà Lorenzo	Pergjegjes: Siguria Kibernetike dhe Strategjia e Vahdimesise se Biznesit dhe Qeverisja e Grupit

3. DISPOZITA TË PËRGJITHSHME

3.1 Detyrimet e Autoritetit të Regjistrimit, Autoritetit te Certifikimit dhe Titullarit

3.1.1 Detyrimet e Autoritetit të Certifikimit dhe Autoritetit të Regjistrimit

Autoriteti i Certifikimit do të veprojë në përputhje me dispozitat e përcaktuara në Dekretin legjislativ [DLgs 82/2005], neni 32, duke miratuar të gjitha masat organizative dhe teknike për të parandaluar çdo dëmtim të palëve të treta.

Autoriteti i Certifikimit i cili, në përputhje me nenin 27 të Dekretit Legjislativ [DLgs 82/2005], lëshon certifikatat e kualifikuara për nënshkrim elektronik gjithashtu duhet:

- të identifikojë si duhet Aplikantin (dhe mbajtësin/titullarin nëse është i ndryshëm); ky aktivitet kryhet nga Autoriteti i Regjistrimit në përputhje me legjislacionin kombëtar;
- të informojë qartë dhe plotësisht aplikantët (dhe mbajtësin/titullarin nëse është i ndryshëm) mbi karakteristikat e certifikatave të kualifikuara për nënshkrimin elektronik dhe kufizimet e përdorimit të tyre; ky aktivitet kryhet nga Autoriteti i Regjistrimit përpara nënshkrimit të Marrëveshjes për Ofrimin e kontratës së shërbimeve të certifikimit;
- të vazhdojë, në bazë të udhëzimeve të dhëna menjëherë nga Autoriteti i Regjistrimit, me revokimin në kohë të certifikatave të kualifikuara për nënshkrimin elektronik dhe publikimin përkatës;
- të miratojë masa sigurie për përpunimin e të dhënave personale të Përdoruesit, në përputhje me ligjet dhe rregulloret në fuqi; ky detyrim do të përmbushet nga Autoriteti i Regjistrimit dhe Autoriteti i Certifikimit;
- të lëshojë certifikatat e kualifikuara për nënshkrim elektronik, siç përshkruhet në [DPCM], në përputhje me [Rregulloren GDPR], sikundër ndryshohet dhe plotësohet në vijim;
- të respektojë rregullat teknike të përcaktuara në Manual [DPCM] dhe në nenin 71 të Dekretit legjislativ 82/2005;
- të sigurohet që pajisja e sigurt për gjenerimin e nënshkrimeve të ketë karakteristikat dhe kërkesat e sigurisë të përcaktuara në nenin 35 të dekretit legjislativ [DLgs 82/2005] dhe nenin 11 të [DPCM];
- të ruajë regjistrimet, edhe në formë elektronike, të të gjitha informacioneve në lidhje me certifikatat e kualifikuara për nënshkrimin elektronik për të paktën 20 (njëzet) vjet, në mënyrë që të jenë në gjendje të sigurojnë provë të certifikimit për çdo proces të mundshëm gjyqësor;
- të ruajë regjistrime, edhe në formë elektronike, të të gjitha dokumenteve të nënshkruara nga mbajtësi/titullari gjatë certifikatave të kualifikuara për procedurën e lëshimit të nënshkrimeve elektronike për të paktën 20 (njëzet); ky aktivitet kryhet nga Autoriteti i Regjistrimit;
- të mos eksportojë kodet privatë të Mbajtësve/Titullarëve nga HSM, nëse këto kode janë gjeneruar dhe janë përdorur;

- Autoriteti i Certifikimit dhe Autoriteti i Regjistrimit do të përditësojnë në mënyrë të vazhdueshme Manualin Operacional të Nënshkrimit Dixhital në Distancë dhe, Autoriteti i Regjistrimit do të informojë menjëherë përdoruesin për ndryshimet e aplikuara.

3.1.2 Detyrimet e Titullarit

Titullari/Mbajtësi duhet të sigurojë ruajtjen e të gjitha informacioneve që mundësojnë përdorimin e kodit privat dhe do të miratojë të gjitha masat teknike dhe organizative për të parandaluar ndonjë dëmtim të palëve të treta; titullari/mbajtësi duhet gjithashtu të përdorë personalisht të dhënat që mundësojnë krijimin e nënshkrimit dixhital (neni 8 (5) i [DPCM]).

Titullari/Mbajtësi do të respektojë [DPCM]; në veçanti, nga Titullari/Mbajtësi duhet:

- të kërkojë certifikatat e kualifikuara për nënshkrim elektronik, sipas procedurave të përcaktuara në Manualin Operacional të Nënshkrimit Dixhital në Distancë (RDS);
- të mbrojë kodet private (kodin e gjeneruar nga çelësi i sigurisë TOKEN dhe sms fjalëkalim me një përdorim OTP) të nevojshme për të përdorur certifikatat e kualifikuara për nënshkrimin elektronik;
- të kërkojë revokimin e certifikatave të kualifikuara për nënshkrimin elektronik, sipas procedurave të përcaktuara në Manualin Operacional të Nënshkrimit Dixhital në Distancë RDS;
- të njoftojë menjëherë Autoritetin e Regjistrimit për çdo ndryshim të informacionit që i është dhënë Autoritetit të Regjistrimit gjatë procedurës së regjistrimit (të dhënat personale, adresat, etj.);
- të mos përdor kodin privat për qëllime të ndryshme nga ato që janë përcaktuar në kufizimet e përdorimit të përcaktuara në certifikatat e kualifikuara për nënshkrimin elektronik në Marrëveshjen e Përdorimit të Shërbimit Digital Banking dhe Marrëveshjen për Ofrimin e shërbimeve të Certifikimit;
- të sigurojë saktësinë, vërtetësinë dhe plotësinë e informacionit personit që bën identifikimin, për kërkesën e certifikatës;
- të përdorë certifikatën vetëm për metodat e përcaktuara në këtë Manual Operacional dhe në ligjet aktuale kombëtare dhe ndërkombëtare.

3.1.3 Detyrimet e personit juridik (nëse ka)

Në rast se titullari/mbajtësi përdorur një certifikatë të kualifikuar për nënshkrimin elektronik në emër të Subjektit Juridik, i njëjti subjekt juridik do të jetë pjesë e detyrimeve dhe do të duhet të sigurojë autorizimin e duhur për Titullarin/Mbajtësin që të përdorë një certifikatë të kualifikuar për nënshkrim elektronik në emër të tij.

Subjekti juridik duhet të zbatojë [DPCM]; në veçanti, nga subjekti juridik duhet:

- të autorizojë kërkesën e Titullarit/Mbajtësit që të ketë një certifikatë të kualifikuar për nënshkrim elektronik, sipas procedurave të përcaktuara në Manualin Operacional të Nënshkrimit Dixhital në Distancë;
- të kërkojë revokimin e certifikatës së kualifikuar për nënshkrimin elektronik, sipas procedurave të përcaktuara në Manualin Operacional të Nënshkrimit Dixhital në Distancë;

- të njoftojë menjëherë Autoritetin e Regjistrimit për çdo ndryshim të informacionit që i është dhënë Autoritetit të Regjistrimit gjatë procedurës së regjistrimit (të dhënat personale të titullarit/mbajtësit, vdekja e titullarit/mbajtësit, humbja e aftësisë së biznesit të titullarit/mbajtësit, të dhënat e subjektit juridik, etj.);
- të përdorë certifikatën vetëm për metodat e përcaktuara në Manualin Operacional të Nënshkrimit Dixhital në Distancë dhe ligjet aktuale kombëtare dhe ndërkombëtare.

3.1.4 Detyrimet e subjektit që duhet të verifikojë nënshkrimin

Subjektet përgjegjëse për të verifikuar nënshkrimin elektronik të gjeneruar nga kodet e certifikimit nga Intesa Sanpaolo, duhet të:

- verifikojnë periudhën e vlefshmërisë së certifikatës (në përputhje me rregulloren aktuale);
- kontrollojnë ne listën e certifikatave të revokuara të kualifikuara për nënshkrimin elektronik nëse certifikata është revokuar në momentin e nënshkrimit;
- sigurojnë që nënshkrimi elektronik i referohet një certifikate të kualifikuar të lëshuar nga një Autoritet Certifikimi i aprovuar më parë nga AgID në momentin e nënshkrimit;
- sigurojnë që tipologjia e kodeve "abonim" të gjeneruar (siç parashikon [DPCM], neni 5, pika 4, shkronja a) dhe kodi i përdorimit shtesë 11 të certifikatës (OID: 2.3.29.15) të ketë vetëm vlerën e refuzimit (bit 1 vendoset në 1) ;
- verifikojnë kufizimet e përdorimit të specifikuara në certifikatën e kualifikuar.

3.2 Kufizimi i përgjegjësisë dhe dëmshpërblimi

3.2.1 Kufizimi i përgjegjësisë

Intesa Sanpaolo nuk do të jetë përgjegjëse për asnjë ndërprerje që rezulton nga moszbatimi i ligjeve dhe rregulloreve në fuqi nga ana e Titullarit/mbajtësit, si dhe nga mosrespektimi i specifikave teknike / operacionale që parashikohen në Marrëveshjen e Përdorimit të Shërbimit Digital Banking nënshkruar nga dhe ndërmjet titullarit/mbajtësit dhe Bankës përkatëse ose në çdo dokumenti që referohet.

Intesa Sanpaolo nuk do të jetë përgjegjëse për dëmet që rezultojnë nga çdo përdorim që tejkalon kufijtë e specifikuar në certifikatat e kualifikuara për nënshkrimin elektronik dhe / ose në Marrëveshjen e Përdorimit të Shërbimit Digital banking dhe / ose Marrëveshjen për Ofrimin e shërbimeve të Certifikimit.

Kufizimet e përdorimit të specifikuara në certifikatat e kualifikuara për nënshkrimin elektronik janë si më poshtë vijon:

Nenshkrimi Elektronik i Kualifikuar i Intesa Sanpaolo CA 2:

Perdorim i kufizuar per dokumentet ne lidhje me marredheniet e titullarit te certifikates me kompanite e Grupit Intesa Sanpaolo ose persona te tjere jashte Grupit te cilet ofrojne sherbimet e tyre per sistemet elektronike te kompanive te Grupit "

Nenshkrimi i Kualifikuar CA i Intesa Sanpaolo S.p.A.:

Perdorim i kufizuar per dokumentet ne lidhje me marredheniet e titullarit te certifikates me kompanite e Grupit Intesa Sanpaolo ose persona te tjere jashte Grupit te cilet ofrojne sherbimet e tyre per sistemet elektronike te kompanive te Grupit "

Gjithashtu, përdorimi i certifikatave të kualifikuara për nënshkrimin elektronik do të kufizohet në domenin e specifikuar në Marrëveshjen për ofrimin e shërbimeve të Certifikimit.

Kufizime të tjera specifike për një produkt të vetëm ose një ligj kombëtar do të trajtohen në Manualet Operacionale që i dedikohet një produkti specifik.

3.2.2 Dëmshpërblimi

Sikundër parashikohet në mënyrë të detajuar në nenin 3.2.1 më lart Intesa Sanpaolo nuk do të jetë përgjegjës për dëmet që rezultojnë nga përdorimi i papërshtatshëm i certifikatave të kualifikuara për nënshkrimin elektronik.

Megjithatë, në bazë të nenit 15 (1) i) të [DPCM], Intesa Sanpaolo ka përcaktuar një sigurim të caktuar specifik për të mbuluar rreziqet përkatëse dhe dëmet që rezultojnë nga ose në lidhje me lëshimin e certifikatave të kualifikuara për nënshkrimin elektronik.

3.3 Orari i disponueshmërisë

Shërbimet që ofrohen nga Autoriteti i Certifikimit (lëshimi i certifikatave të kualifikuara për nënshkrimin elektronik dhe përdorimi i nënshkrimit elektronik) janë në dispozicion përmes kanaleve direkte (në internet dhe celular) dhe nëpërmjet degës. Revokimi i certifikatave të kualifikuara për nënshkrimin elektronik ofrohet edhe nëpërmjet degës.

4. ASPEKTET OPERACIONALE

4.1 Përmbajtja e certifikatave të kualifikuara për nënshkrimin elektronik

Përmbajtja e certifikatave të kualifikuara për nënshkrimin elektronik të lëshuar nga Intesa Sanpaolo është në përputhje me dispozitat e përcaktuara në nenin 28 të dekretit legjislativ [Dlgs 82/2005] për specifikimin ITU-T X.509 v3 (ISO/IEC 9594-8:2005) dhe me Rregulloren Europiane ETSI EN 319 411 ed ETSI EN 319 412 (nëse zbatohet).

Duke iu referuar Vendimit të AgID nr 121/2019, në të parashikohet se certifikatat e kualifikuara lëshohen nga Intesa Sanpaolo sipas rekomandimeve të cilat janë referuar në kapitullin 4 të dispozitave të sipërpërmendur, me përjashtim të fushave të mëposhtme:

- Subjekti DN: numri i serisë (OID 2.5.4.5): një kod unik që lidhet me titullarin përdoret nëpërmjet një kushti emërtimi të ndryshme nga ai që përcaktohet në rekomandimet e referuara në kapitullin 4 të vendimit nr. 121/2019 të AgID
- Subjekti DN: emri i organizatës (OID 2.5.4.10): nëse pronari është një klient I thjeshtë i organizatës, fusha e emrit të organizatës ende përdoret, por përforcohet me fjalën “jo prezent”.

Duke qenë se të gjitha rekomandimet e vendimit nr. 121/2019 nuk zbatohen, certifikatat që janë lëshuar nga Intesa Sanpaolo nuk përmbajnë kodimin në fushën e Politikave të Certifikatës (OID 2.5.29.32) në një element të identifikuesit të politikës me vlerën e AgID (OID 1.3.76.16.6). Certifikatat e kualifikuara për nënshkrimin elektronik nuk do të publikohen në regjistrat që janë të disponueshëm për publikun.
Periudha e vlefshmërisë për secilën certifikatë të kualifikuar është 3 (tre) vjet.

Nënshkrimi Dixhital në distancë autorizon mbajtësin/titullarin dhe subjektin juridik (nëse aplikohet) të lidhin një kontratë me Bankën. Nënshkrimi dixhital në distancë mund të përdoret nëpërmjet të gjitha kanaleve (përfshirë kanalet dixhitale: dega dixhitale, on-line banking dhe blerja dixhitale) sipas ofertës dhe mundësive në kohë të Bankës Një certifikatë e kualifikuar për nënshkrimin elektronik duhet t'i lejojë mbajtësit/titullarit përdorimin e nënshkrimit dixhital në distancë.

4.2 Rregullat për organizimin e punonjësve

Punonjësit përgjegjës për ofrimin dhe kontrollin e shërbimit të certifikimit është i organizuar në bazë të kuptimit të [DPCM 2013] që do të thotë që, ndër të tjera, rolet e përgjegjësisë janë parashikuar sikundër përcaktohet në nenin 38 të [DPCM].

Gjatë kryerjes së detyrave të tyre, punonjësi që ka role përgjegjësie mund të përfitojë nga punonjësit dhe operatorët, që gjithashtu i përkasin Bankave.

Lidhur me Manualin Operacional RDS, operatorët kryejnë shërbimin e certifikimit (këtu ka kuptimin e regjistrimit ose identifikimit të mbajtësit/titullarit) në degët e Bankave, jashtë qendrës së përpunimit të të dhënave të Intesa Sanpaolo; shkëmbimi i informacionit ndërmjet operatorëve dhe Intesa Sanpaolo bëhet përmes kanaleve të sigurta të komunikimit.
Aktiviteti i regjistrimit kryhet nga Bankat në bazë të një kontrate specifike që lidhet nga dhe ndërmjet Bankës përkatëse dhe Intesa Sanpaolo.
Operatorët e Bankave kryejnë veprimtarinë e regjistrimit në përputhje me procedurat e dakordësuara midis Bankave dhe Intesa Sanpaolo dhe kryhen përmes një procedure në përputhshmëri të plotë.

4.3 Procedura e gjenerimit të kodit

Çdo lloj kodi i listuar në nenin 5 të [DPCM] gjenerohet, ruhet dhe përdoret brenda pajisjeve të sigurta, të cilat janë në përputhje me kërkesat e sigurisë të përcaktuara dhe parashikuara në ligjet dhe rregulloret në fuqi.

Kodet kanë karakteristikat e përcaktuara në [DPCM].

4.3.1 Certifikimi i procedurës së gjenerimit të kodit[1]

Gjenerimi i kodeve të certifikimit kryhet në përputhje me ligjet dhe rregulloret në fuqi, dhe veçanërisht:

- kodet e certifikimit gjenerohen nga punonjësit e caktuar shprehimisht nga Autoriteti i Certifikimit;
- një certifikatë specifike e kualifikuar për nënshkrimin elektronik gjenerohet për secilën palë të kodeve të certifikimit, sikundër përcaktohet në paragrafin 4.1, nënshkruar me kodin privat përkatës të çiftit, i cili i dërgohet AgID-it në përputhje me procedurat e dakordësuara më parë midis Autoritetit të Certifikimit dhe AgID.

4.3.2 Vula datare/orës procedura e gjenerimit të kodit

Në lidhje me shërbimin e vulës datare/orës për shërbimet e nënshkrimit dixhital, që i sigurohen Bankës, Intesa Sanpaolo përdor një autoritet certifikimi që plotëson kërkesat e nevojshme për të ofruar shërbime në vendin ku ndodhet Banka përkatëse.

4.4 Procedura e identifikimit dhe regjistrimit të përdoruesit

Lëshimi i certifikatave të kualifikuara për nënshkrimin elektronik është e vlefshme vetëm për ata që janë kualifikuar si Përdorues, përkatësisht personi që nënshkruan Marrëveshjen për Ofrimin e shërbimeve të Certifikimit me Bankën.

Certifikatat e Kualifikuara të Përdoruesit individual për nënshkrimin elektronik përmbajnë informacion dhe të dhëna personale të mbajtësit/titullarit. Certifikatat e kualifikuara të Subjektit Ligjor të Përdoruesit përfundimtar për nënshkrimin elektronik mund të përmbajnë të dhëna personale për mbajtësin, si dhe informacione rreth subjektit juridik.

Procedurat e identifikimit dhe regjistrimit të përdoruesit kryhen nga Banka përkatëse në përputhje me ligjet dhe rregulloret në fuqi, duke përfshirë por pa u kufizuar në rregulloren për parandalimin e pastrimit të parave, të cilat do të respektohen në kohën e lidhjes së marrëdhënieve kontraktuale me këtë të fundit.
Për Subjektet Juridike, rregullorja për parandalimin e pastrimit të parave është e zbatueshme për Subjektin Juridik dhe jo për Mbajtësin/Titullarin. Në këtë rast, identifikimi i mbajtësit kryhet personalisht.

Identifikimi i mbajtësit/titullarit dhe / ose aplikantit do të bëhet personalisht (i) me prezencë fizike të Përdoruesit në mjediset e Bankës, ose (ii) në distancë, me anë të përdorimit të metodave të identifikimit që njihen për sigurimin dhe ofrimin e një sigurie ekuivalente për sa i përket besueshmërisë. Këto aktivitete kryhen përmes një procedure në përputhje me aspektet për parandalimin e pastrimit të parave ose një procedurë me prezencë fizike, e cila merr gjithashtu dhe në konsideratë nenin 24 1. (d) të Rregullores së Eidas.

4.4.1 Identifikimi dhe regjistrimi i përdoruesit

Përdoruesi identifikohet përmes procedurave të përcaktuara paraprakisht që ndryshojnë në varësi të kanalit të bankës dixhitale.
Identifikimi i Përdoruesit kryhet ose përmes prezencës fizike ose në distancë. Në veçanti:

[1] Kodet përdoren nga Autoriteti i Certifikimit për të lëshuar certifikata të kualifikuara për nënshkrime elektronike, sipas kërkesës së Titullarit

- Gjatë identifikimit personalisht në Degën Dixhitale, numri celular që jepet nga Përdoruesi certifikohet duke dërguar fjalëkalimin me një përdorim OTP përmes një mesazhi telefonik sms dhe duke i kërkuar përdoruesit që ta vendosë atë. Përdoruesi gjithashtu do të identifikohet duke skanuar kartën e tij të debitit në lexuesin e kartave;
- Gjatë identifikimit online në Shërbimet Bankare Dixhitale në distancë, Përdoruesi vërteton në celular / Përgjegjës me ID e regjistrimit dhe fjalëkalimin me një përdorim OTP të gjeneruar duke future kodin PIN në çelësin e tij të sigurisë TOKEN të tij / saj në përputhje me Shërbimin Bankar Dixhital dhe fjalëkalimit me një përdorim OTP shtesë që Përdoruesi merr përmes mesazhit sms në numrin e tij të celularit të certifikuar;
- Gjatë identifikimit nëpërmjet videos për Blerjen Dixhitale, certifikohet numri celular që jep përdoruesi duke dërguar fjalëkalimin me një përdorim OTP përmes mesazhit telefonik sms dhe duke i kërkuar përdoruesit ta vendos atë.

Të gjitha procedurat e identifikimit kryhen duke ndjekur rregulloren lokale të Bankës dhe përmes një procedure në përputhje me aspektet për parandalimin e pastrimit të parave ose një procedurës që kryhet me prani fizike.
Identifikimi i Përdoruesit kryhet nga Banka përkatëse përpara regjistrimit të certifikatës së kualifikuar për nënshkrimit elektronik.
Pas identifikimit me sukses, Përdoruesi është në gjendje të vazhdojë me aktivizimin e shërbimit të nënshkrimit dixhital në distancë dhe me nënshkrimin e kontratës përkatëse.

4.4.2 Aktivizimi i individëve të shërbimit për Nënshkrimin Dixhital në Distancë dhe nënshkrimi i kontratës përkatëse.

Për të aktivizuar një nënshkrim dixhital në distancë dhe për të nënshkruar Marrëveshjen për Ofrimin e shërbimeve të Certifikimit, Aplikanti duhet të përmbushë hapat e mëposhtëm procedurale në kanale të ndryshme

Shërbimet Bankare Dixhitale në Distancë:

- akseson Shërbimin Bankar Dixhital duke përdorur procedurat e vërtetimit dhe autentifikimit të përcaktuara nga Banka përkatëse;
- sipas kërkesës, pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e shërbimeve të Certifikimit;
- sipas kërkesës, kontrollon dhe konfirmon saktësinë e të dhënave personale të tij / saj me qëllim për të aktivizuar certifikatën e kualifikuar për nënshkrimin elektronik;
- kërkesa për regjistrimin e certifikatës;
- gjeneron fjalëkalimin me një përdorim - OTP të krijuar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN, në varësi të Shërbimit Bankar Dixhital. Ky fluks garanton mekanizmin e fortë të autentifikimit;
- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, regjistron certifikatat e kualifikuara për nënshkrimin elektronik dhe nënshkruan në mënyrë dixhitale duke vendosur fjalëkalimin me një përdorim OTP, të krijuar nga çelësi i sigurisë TOKEN duke vendosur dhe kodin PIN;
- fjalëkalimi me një përdorim OTP shtesë që Përdoruesi i fundit merr përmes mesazhit telefonik sms në numrin e tij të certifikuar të celularit kërkohet për kontrolle plotësuese shtesë;
- Nënshkrimi i Bankës konfirmon aktivizimin e shërbimit RDS

Dega ose portali i blerjes dixhitale:

- Akseson Blerjen Dixhitale ose shkon personalisht në mjediset e Bankës;
- sipas kërkesës, pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e shërbimeve të Certifikimit;
- sipas kërkesës, kontrollon dhe konfirmon saktësinë e të dhënave personale të tij / saj me qëllim për të aktivizuar certifikatën e kualifikuar për nënshkrimin elektronik;
- kërkon regjistrimin e certifikatës. Nëse Përdoruesi kërkon aktivizimin e certifikatës përmes kanalit të Degës Dixhitale, do të krijohet formulari i duhur i aplikimit përpara nënshkrimit të Marrëveshjes për Ofrimin e Shërbimeve të Certifikimit;
- Merr fjalëkalimin me një përdorim OTP përmes mesazhit sms në numrin e tij të certifikuar të celularit. Për Identifikimin personalisht dhe identifikimin përmes videos, Përdoruesi nuk do të duhet të vendos kodin e

sigurisë PIN. Në Degë, Aplikanti do të skanojë kartën e tij të debitit për të kryer hapin e parë të autorizimit përmes lexuesit të kartave;

- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, regjistron certifikatat e kualifikuara për nënshkrimin elektronik dhe nënshkruan në mënyrë dixhitale duke vendosur fjalëkalimin me një përdorim OTP. Marrëveshja për Ofrimin e Shërbimeve të Certifikimit duhet të nënshkruhet me shkrim;
- Nënshkrimi i Bankës konfirmon aktivizimin e shërbimit RDS.

Dokumentacioni mbështetës në lidhje me shërbimin RDS do t'i sigurohet Përdoruesit përpara përfundimit të Marrëveshjes për Ofrimin e Shërbimeve të Certifikimit në lidhje me shërbimet e nënshkrimit dixhital.

4.4.3 Aktivizimi i përdoruesit person juridik i Shërbimit për Nënshkrimin Dixhital në Distancë dhe nënshkrimi i kontratës përkatëse

Për të aktivizuar nënshkrimin dixhital në distancë dhe nënshkrimin e Marrëveshjes për Ofrimin e Shërbimeve të Certifikimit, Aplikanti dhe Mbajtësi/Titullari duhet të ndjekin hapat e mëposhtëm procedurale në kanale të ndryshme.

Për të nënshkruar Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit përmes Shërbimeve Bankare Dixhitale në Distancë, Mbajtësi/titullari (pavarësisht nëse është i njëjti i Aplikant ose jo) duhet të përmbushë dhe ndjek hapat e mëposhtëm procedurale:

- Merr miratimin e Subjektit Juridik, nëse ai / ajo nuk është i njëjtë si Aplikanti
- Akseson Shërbimin Bankar Dixhital duke përdorur procedurat e vërtetimit dhe autentifikimit të përcaktuara nga Banka përkatëse;
- pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit;
- sipas kërkesës, kontrollon dhe konfirmon saktësinë e të dhënave personale të tij / saj me qëllim për të aktivizuar certifikatën e kualifikuar për nënshkrimin elektronik;
- kërkon regjistrimin e certifikatës;
- gjeneron fjalëkalimin me një përdorim - OTP të krijuar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN, në varësi të Shërbimit Bankar Dixhital. Ky fluks garanton mekanizmin e fortë të autentifikimit
- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, regjistron certifikatat e kualifikuara për nënshkrimin elektronik dhe nënshkruan në mënyrë dixhitale duke vendosur fjalëkalimin me një përdorim OTP të gjeneruar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN;
- fjalëkalimi me një përdorim OTP shtesë që Përdoruesi i fundit merr përmes mesazhit telefonik sms në numrin e tij të certifikuar të celularit duhet për kontrolle plotësuese shtesë;
- Nënshkrimi i Bankës konfirmon aktivizimin e shërbimit RDS.

Për të nënshkruar Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit përmes Shërbimeve Bankare Dixhitale në Distancë, në rast se Aplikanti nuk është i njëjtë me Mbajtësin/Titullarin, Aplikanti duhet të përmbushë dhe të ndjek hapat e mëposhtëm procedurale:

- Akseson Shërbimin Bankar Dixhital duke përdorur procedurat e vërtetimit dhe autentifikimit të përcaktuara nga Banka përkatëse;
- pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit;
- gjeneron fjalëkalimin me një përdorim - OTP të krijuar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN, në varësi të Shërbimit Bankar Dixhital. Ky fluks garanton mekanizmin e fortë të autentifikimit;
- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, dhe nënshkruan në mënyrë dixhitale duke vendosur fjalëkalimin me një përdorim OTP të gjeneruar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN;
- fjalëkalimi me një përdorim OTP shtesë që Përdoruesi i fundit merr përmes mesazhit telefonik sms në numrin e tij të certifikuar të celularit duhet për kontrolle plotësuese shtesë.

Për të nënshkruar Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit në Degë, Mbajtësi/Titullari (pavarësisht nëse është i njëjti Aplikant ose jo) duhet të përmbushë dhe ndjek hapat e mëposhtëm procedurale:

- Merr miratimin e Subjektit Juridik, nëse ai / ajo nuk është i njëjtë si Aplikanti
- shkon personalisht në ambientet e Bankës;
- pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit;
- sipas kërkesës, kontrollon dhe konfirmon saktësinë e të dhënave personale të tij / saj me qëllim për të aktivizuar certifikatën e kualifikuar për nënshkrimin elektronik;
- kërkon regjistrimin e certifikatës;
- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, dhe nënshkruan në mënyrë dixhitale ose me shkrim;

- Në rastin e nënshkrimit dixhital:
    - Mbajtësi/Titullari merr fjalëkalimin me një përdorim OTP përmes sms në numrin e tij të certifikuar të celularit. Për Identifikimin personalisht, Përdoruesit nuk do t'i kërkohet të vendosë kodin e sigurisë PIN;
    - Mbajtësi/Titullari regjistron certifikatën e kualifikuar për nënshkrimin elektronik dhe e nënshkruan në mënyrë dixhitale duke vendosur fjalëkalimin me një përdorim OTP;
- Nënshkrimi i Bankës konfirmon aktivizimin e shërbimit RDS

Për të nënshkruar Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit në Degë, në rast se Aplikanti nuk është i njëjtë me Mbajtësin/Titullarin, Aplikanti duhet të përmbushë dhe ndjek hapat e mëposhtëm procedural:

- shkon personalisht në ambientet e Bankës;
- pranon rregullat që rregullojnë Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit;
- ekzaminon dhe shqyrton Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit, dhe nënshkruan në mënyrë dixhitale ose me shkrim dore

Dokumentacioni mbështetës në lidhje me shërbimin RDS do t'i vihet në dispozicion klientit përpara se të nënshkruajë Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit në lidhje me shërbimet e nënshkrimit dixhital.

Në rastin e nënshkrimit të Marrëveshjes për Ofrimin e Shërbimeve të Certifikimit në Degë me shkrim, regjistrimi i certifikatës së kualifikuar për nënshkrimin elektronik mund të bëhet online përmes Shërbimit Bankar Dixhital të Bankës. Në këtë rast, Mbajtësi/Titullari duhet të përmbushë hapat e mëposhtëm procedurale për të aktivizuar shërbimin RDS:

- Akseson Shërbimin Bankar Dixhital duke përdorur procedurat e vërtetimit dhe autentifikimit të përcaktuara nga Banka përkatëse;
- sipas kërkesës, kontrollon dhe konfirmon saktësinë e të dhënave personale të tij / saj me qëllim për të aktivizuar certifikatën e kualifikuar për nënshkrimin elektronik
- gjeneron fjalëkalimin me një përdorim - OTP të krijuar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN, në varësi të Shërbimit Bankar Dixhital. Ky fluks garanton mekanizmin e fortë të autentifikimit
- regjistron certifikatën e kualifikuar për nënshkrim elektronik duke vendosur fjalëkalimin me një përdorim OTP të krijuar nga çelësi i sigurisë TOKEN duke vendosur kodin PIN;
- fjalëkalimi me një përdorim OTP shtesë që Përdoruesi i fundit merr përmes mesazhit telefonik sms në numrin e tij të certifikuar të celularit duhet për kontrolle plotësuese shtesë

4.4.4 Lëshimi i certifikatave të kualifikuara të certifikatave për nënshkrimin elektronik

Certifikatat e kualifikuara për nënshkrimin elektronik lëshohen pas përfundimit të gjenerimit të çiftit kryesor, siç tregohet më lart.

Lëshimi i certifikatës së kualifikuar për procedurën e nënshkrimit elektronik është plotësisht transparent për Aplikantin i cili, në këtë fazë specifike nuk bashkëvepron me Autoritetin e certifikimit.

Sipas legjislacionit në fuqi, kërkesa për certifikatë të kualifikuar për lëshimin e nënshkrimit elektronik ruhet nga Autoriteti i Certifikimit për të paktën 20 (njëzet) vjet nga data e lëshimit të secilit certifikatë të kualifikuar për nënshkrimin elektronik. Në mënyrë të veçantë, të gjitha gjurmët e nevojshme për të demonstruar në kohë ekzekutimin e këtij operacioni ruhen në mënyrë elektronike.

4.5 Procedura për certifikatën e revokimit të nënshkrimit elektronik të kualifikuar

Sipas [DPCM] revokimi i një certifikatë të kualifikuar për nënshkrimin elektronik ndodh me kërkesën e palëve të mëposhtme:

- Titullari/mbajtësi;
- Personi juridik;
- Autoriteti i certifikimit;
- Autoriteti i Regjistrimit

4.5.1 Kërkesa për revokim paraqitur nga Titullari

Mbajtësi/Titullari do të paraqesë një kërkesë për certifikatë të kualifikuar për revokimin e nënshkrimit elektronik duke shkuar në degë.

Pas paraqitjes së kërkesës për revokim, iniciohet mekanizmi automatik që duhet për revokimin e certifikatës në mënyrë transparente me Titullarin/Mbajtësin.

Në rast të përfundimit të njëanshëm të Marrëveshjes për Ofrimin e shërbimeve të certifikimit të Bankës, nga Mbajtësi/titullari Autoriteti i Regjistrimit do të njoftojë menjëherë Autoritetin e Certifikimit i cili do të vijojë me revokimin e certifikatës përkatëse për nënshkrimin elektronik.

Si rezultat i revokimit, Mbajtësi/Titullari nuk mund të nënshkruajë më asnjë dokument duke përdorur kodet që i janë dhënë më parë atij / saj, ndërsa të gjitha dokumentet e nënshkruara nga mbajtësi para heqjes së certifikatës janë dhe mbesin të vlefshme.
Në lidhje me efektivitetit e revokimit të certifikatës, revokimi do të jetë efektiv duke filluar nga data e marrjes së njoftimit të revokimit nga banka.

4.5.2 Kërkesa për revokim paraqitur nga personi juridik

Personi juridik do të paraqesë përmes degës kërkesën për certifikatë të kualifikuar për revokimin e nënshkrimit elektronik të një Mbajtësi/Titullari të një shërbimi RDS në emër të të njëjtit person juridik.

Pas paraqitjes së kërkesës për revokim, iniciohet mekanizmi automatik që duhet për revokimin e certifikatës në mënyrë transparente me Titullarin/Mbajtësin.

Në rast të përfundimit të njëanshëm të Marrëveshjes për Ofrimin e shërbimeve të certifikimit të Bankës, nga personi juridik, Autoriteti i Regjistrimit do të njoftojë menjëherë Autoritetin e Certifikimit i cili do të vijojë me revokimin e certifikatës përkatëse për nënshkrimin elektronik.
Si rezultat i revokimit, Mbajtësi/Titullari nuk mund të nënshkruajë më asnjë dokument duke përdorur kodet që i janë dhënë më parë atij / saj, ndërsa të gjitha dokumentet e nënshkruara nga mbajtësi para heqjes së certifikatës janë dhe mbesin të vlefshme.
Në lidhje me efektivitetit e revokimit të certifikatës, revokimi do të jetë efektiv duke filluar nga data e marrjes së njoftimit të revokimit nga banka.

4.5.3 Revokimi paraqitur nga Autoriteti i Certifikimit ose nga Autoriteti i Regjistrimit

Me përjashtim të rasteve të justifikuara të urgjencës, Autoriteti i Certifikimit ose Autoriteti i Regjistrimit që synon të revokojë një certifikatë të kualifikuar për nënshkrimin elektronik, do të njoftojë paraprakisht Mbajtësin/Titullarin/Personin Juridik, duke specifikuar arsyet e revokimit.

Autoriteti i Regjistrimit duhet të njoftojë menjëherë Autoritetin e Certifikimit për domosdoshmërinë e revokimit të një certifikate të kualifikuar për nënshkrimin elektronik.
Autoriteti i Certifikimit duhet të revokojë certifikatën në rastet e mëposhtme:

- me kërkesë të shprehur qartë të Mbajtësit/titullarit
- me kërkesë të shprehur të personit juridik për llogari të të cilit titullari/mbajtësi merr certifikatën;
- në rast se vendoset se të dhënat e mbajtësit/titullarit janë të pasakta ose jo të plota në informacionin e Certifikatës;
- në rastin e marrjes së një njoftimi zyrtar për vdekjen e mbajtësit/titullarit;
- në rastin e marrjes së një njoftimi zyrtar për humbjen e aftësisë së biznesit të mbajtësit/titullarit;
- në rast se personi juridik pushon së ekzistuari;
- në rast të përfundimit të Marrëveshjes për Ofrimin e Shërbimeve të Certifikimit;
- në rast se vendoset që Mbajtësi ka përdorur të dhëna false për lëshimin e certifikatës

4.5.4 Plotësimi i certifikatës së kualifikuar për procedurën e revokimit të nënshkrimit elektronik

Pas përfundimit të procedurës së revokimit të certifikatës, krijohet një CRL i re, i cila publikohet në direktorinë përkatëse të disponueshme përmes lidhjes në internet.
CRL publikohet siç tregohet në paragraf. 4.9.2. Për më tepër, revokimi efektiv i një certifikate të kualifikuar për nënshkrimin elektronik regjistrohet në regjistrin e kontrollit.

4.6 Certifikata e kualifikuar për procedurën e pezullimit të nënshkrimit elektronik

Sipas [DPCM] pezullimi i një certifikate të kualifikuar për nënshkrimin elektronik ndodh me kërkesën e palëve të mëposhtme:

- Autoritetit të certifikimit;
- Autoritetit të regjistrimit

Me përjashtim të rasteve të justifikuar të urgjencës, Autoriteti i Certifikimit ose Autoriteti i Regjistrimit që synon të pezullojë një certifikatë të kualifikuar për nënshkrimin elektronik, do të njoftojë paraprakisht Mbajtësin/Titullarin/Personin Juridik, duke specifikuar arsyet e pezullimit

4.7 Procedura për humbjen e kodit PIN dhe pajisjes OTP (TOKEN)

Mbajtësi/Titullari do të ketë mundësinë të përdorë, si një nga metodat e vërtetimit dhe autentifikimit, pajisjen OTP
Në rast të humbjes ose vjedhjes së pajisjes OTP, Mbajtësi duhet të veprojë në bazë të Marrëveshjes së Shërbimit Bankar Dixhital.
Procedura për humbjen e PIN është e njëjta me atë të humbjes së pajisjes OTP.

4.8 Procedura për zëvendësimin e kodeve

4.8.1 Zëvendësimi i kodeve të nënshkrimit të titullarëve

Në bazë të [DPCM], Autoriteti i Certifikimit përcakton skadimin e certifikatës së kualifikuar për nënshkrimin elektronik dhe periudhën e vlefshmërisë së kodeve sipas gjatësisë së kodeve dhe shërbimeve për të cilat do të përdoren kodet.

Periudha e vlefshmërisë së kodeve përkon me periudhën e vlefshmërisë së certifikatës përkatëse të kualifikuar për nënshkrimin elektronik, që është 3 (tre) vjet.

Kërkesa për lëshimin e një certifikate të re të kualifikuar për nënshkrimin elektronik lejohet vetëm nëse certifikata e mëparshme ka skaduar ose revokuar, ose ka skaduar ose është revokuar nga Mbajtësi/Titullari.
Mbajtësi/Titullari nuk mund të ketë 2 (dy) certifikata të kualifikuara aktive për nënshkrim elektronik në të njëjtën kohë për të njëjtin person juridik

4.8.2 Zëvendësimi i kodeve të certifikimit

Zëvendësimi i kodeve të certifikimit kryhet nga Autoriteti i Certifikimit në përputhje me ligjet dhe rregulloret në fuqi.

4.9 Menaxhimi i certifikatave të kualifikuara për direktorinë e nënshkrimit elektronik

4.9.1 Certifikatat e kualifikuara për direktorinë e nënshkrimit elektronik

Të gjitha certifikatat e vlefshme të kualifikuara për nënshkrimin elektronik të lëshuar nga Autoriteti i Certifikimit ruhen në "regjistrin e certifikatave".

Në vend të kësaj, direktoria publike përmban informacionet e mëposhtme:

- certifikatat për kodet e Autoritetit të Certifikimit;
- certifikatat që lidhen me marrëveshjet e certifikimit;
- certifikatat për kodet e nënshkrimit të AgID;
- lista e certifikatave të revokuara të kualifikuara për nënshkrimin elektronik.

Lista e certifikatave të revokuara të kualifikuara për nënshkrimin elektronik publikohet gjithashtu përmes protokollit HTTP
(http://crlcl.ca2.intesasanpaolo.com/qc/CRL$$.crl per CA "Nenshkrimin elektronik te kualifikuar te Intesa Sanpaolo CA2”
http://crl2.ca.intesasanpaolo.com/FirmaQualificata/CRL$$.crl per CA “Nenshkrimi i Kualifikuar CA te Intesa Sanpaolo S.p.A.”

Autoriteti i Certifikimit përdor sisteme të besueshme për administrimin e certifikatave të kualifikuara për direktorinë elektronike të nënshkrimeve dhe drejtorinë publike dhe përdor metoda që sigurojnë që:

- vetëm personat e autorizuar do të regjistrojnë të dhëna dhe bëjnë ndryshime;
- vërtetësia dhe autentifikimi i informacionit është i verifikueshëm;
- certifikatat janë të disponueshme për konsultime publike deri në masën e lejuar nga Mbajtësi/titullari;
- operatori do të jetë i vetëdijshëm për çdo ngjarje që komprometon kërkesat e sigurisë.
- NB: $$ tregon numrin progresiv te CRL-s (numrin qe lidhet me CRL-n perkatese specifikohet ne secilen certifikate, ish http://crl.ca2.intesasanpaolo.com/qc/CRL11.crl)

4.9.2 Publikimi i certifikatave të kualifikuara për nënshkrimin elektronik dhe CRL

Certifikatat e kualifikuara për nënshkrimin elektronik publikohen sipas procedurave të përcaktuara në nenin 34 të [DPCM].

CRL krijohet dhe publikohet në direktorinë publike çdo orë, përveçse në rastin kur ka një pengese teknike e cila është përtej kontrollit të Autoritetit të Certifikimit.

Aksesi në direktorinë publike lejohet përmes rrjetit publik të internetit në adresën e specifikuar në zgjerimin e pikës së shpërndarjes CRL në certifikatën e kualifikuar për nënshkrimin elektronik.

Per tju lejuar juve te kontrolloni statusin e revokimit te certifikates pa bere nje kerkese ne CRL, Intesa Sanpaolo mundeson ofrimin e sherbimeve OCSP.

Informacioni per profilet CRL dhe OCSP raportohet tek CP-CPS e certifikuesit.

4.9.3 Riprodhimi i certifikatave të kualifikuara për direktorinë e nënshkrimit elektronike në uebsajte të ndryshme

Në përputhje me [DPCM], Autoriteti i Certifikimit kopjon direktorinë e certifikatave në një numër faqesh në internet, duke siguruar konsistencën dhe integritetin e kopjeve.

Ju lutemi shikoni paragrafin 4.13. për më shumë detaje.

4.10 Procedurat për mbrojtjen e të dhënave personale

Informacioni në lidhje me mbajtësin/titullarin që merr Autoriteti i Certifikimit gjatë lëshimit të certifikatave të kualifikuara për shërbimet e nënshkrimit elektronik, do të merren në konsideratë, përveç rasteve kur titullari/mbajtësi jep miratimin me shkrim, i cili është konfidencial dhe nuk do të publikohet, me përjashtim të atyre rasteve kur janë të destinuara shprehimisht për përdorim publik (p.sh. kodi publik, data e revokimit të certifikatës së kualifikuar për nënshkrimin elektronik). Bazuar në këtë manual, Autoriteti i Certifikimit nuk përpunon "të dhëna sensitive ose gjyqësore" sikundër parashikohet në Rregulloren GDPR.

Në fushën e identifikimit dhe mbrojtjes së të dhënave, aktivitetet që do të kryhen do të jenë në përputhje me ligjin kombëtar të Bankës e cila kryen aktivitetet e autoritetit të regjistrimit. Për sqarime të tjera, afati i ruajtjes së certifikatave dhe të gjitha dokumentet dhe informacionet përcaktohen parashikohen në bazë të ligjit italian, prandaj afati i ruajtjes do të jetë në përputhje me ligjin italian.

Të dhënat personale të lartpërmendura do të përpunohen nga Autoriteti i Certifikimit në përputhje me Rregulloren GDPR.

4.11 Procedura për organizimin dhe kontrollin e skedarit log

Autoriteti i Certifikimit regjistron në regjistrin e kontrollit, automatikisht ose manualisht, ngjarjet e parashikuara në nenin 36 të [DPCM]. Në mënyrë të veçantë janë regjistruar ngjarjet e mëposhtme:

- lëshimi i certifikatave të kualifikuara për nënshkrimin elektronik;
- revokimi i certifikatave të kualifikuara për nënshkrimin elektronik, duke specifikuar datën dhe kohën e publikimit të CRL;
- fillimi dhe përfundimi i sesionit të punës së sistemeve që përdoren për gjenerimin e certifikatave të kualifikuara për nënshkrimin elektronik;
- personalizimi i pajisjeve të nënshkrimit;
- hyrja dhe dalja nga dhomat e sigurisë së sistemit të certifikimit.

Autoriteti i Certifikimit administron regjistrin e kontrollit në përputhje me nenin 41 (2) [DPCM].

4.12 Procedura për menaxhimin e kopjeve rezervë

Autoriteti i Certifikimit ka përgatitur dhe implementuar një plan për vazhdimësinë e shërbimit të ofruar në bazë të këtij manuali operacional; veprimet dhe masat kryesore që duhen të merren sipas procedurave përkatëse që përshkruhen më poshtë.

4.12.1 Procedura e ruajtjes back up

Kopjet rezervë prodhohen çdo ditë për të dhënat, aplikacionet, regjistrat e kontrollit dhe çdo skedar tjetër të nevojshëm që duhet për të rikuperuar kthyer plotësisht procesorët kritikë të certifikatës së kualifikuar për sistemin e menaxhimit elektronik të nënshkrimeve. Në lidhje me këta përpunues, prodhimi i kopjeve rezervë kryhet në distancë dhe kontrollohet nga një sistem i centralizuar specifik që plotëson kërkesat e mëposhtme:

- minimizon nevojën për ndërhyrje njerëzore dhe hyrjen në dhomat teknike;
- thjeshton planifikimin e operacioneve të ruajtjes back up dhe auditimin e tyre;
- rrit besueshmërinë e operacioneve rezervë.

4.13 Procedura për menaxhimin e aksidenteve dhe ngjarjeve të katastrofave

Në vijim paraqitet një vështrim i përgjithshëm për këto procedura.

4.13.1 Dështimet kompjuterike

Të gjithë kompjuterët që përdoren për ofrimin e certifikatave të kualifikuara për shërbimin e nënshkrimit elektronik janë subjekt i një marrëveshje mirëmbajtjeje, në bazë të së cilës garantohet riaktivizimi i kompjuterëve, në rast të mosfunksionimi dhe dështimi, brenda 24 (njëzet e katër) orë.

4.13.2 Dëmtimet e programeve kompjuterike

Në rast mosfunksionimi (humbje ose korruptim) të programeve ose pamundësi për të rikuperuar të dhënat, ato do të merren nga skedarët e ruajtur rezervë.

4.13.3 Mosfunksionimi i pajisjes së nënshkrimit të Autoritetit të Certifikimit

Në rast mosfunksionimi të pajisjes së nënshkrimit të Autoritetit të Certifikimit, kodi privat do të rivendoset në një pajisje të re nënshkrimi, duke filluar nga segmentet e kodeve të krijuar më parë, duke ndjekur një procedurë specifike që kërkon një ndërhyrje të përbashkët të më shumë operatorëve. Segmentet kryesore ruhen në një formë të koduar dhe në vende të ndryshme, të cila kontrollohen nga menaxherë të ndryshëm.

Shënim: segmentet kryesore nuk përbëjnë një "kopje" të kodit të certifikimit ([DPCM]) dhe mund të përdoren vetëm me qëllim të rikuperimit të tërësisë së kodit, sipas procedurës së përshkruar më lart.

Në rast se rikuperimi kodit të certifikimit nuk është i mundur, duhet të respektohet procedura për mosfunksionimin e kodit të certifikimit (shiko paragrafin e mëposhtëm).

4.13.4 Dëmtimet e kodit të certifikimit

Në rast të mosfunksionimit të ruajtjes së konfidencialitetit të kodit privat të certifikimit, Autoriteti i Certifikimit do të:

- revokojë certifikatën në lidhje me kodin privat që nuk funksionon;

- njoftojë AgID për revokimin brenda 24 (njëzet e katër) orë nga momenti i revokimit;
- informojë mbajtësit e të gjitha certifikatave të kualifikuara për nënshkrimin elektronik të nënshkruar me kodin privat që i përket palës së revokuar;
- revokojë të gjitha certifikatat e kualifikuara për nënshkrimin elektronik të nënshkruar me kodin që nuk funksionon;
- lëshojë certifikata të reja të kualifikuara për nënshkrimin elektronik duke përdorur një kod të ri privat.

4.13.5 Kompromentimi i sajtit kryesor

Në rastin e mosdisponueshmërisë së mjediseve, ndërtesave ose sistemit në tërësi, pas një ngjarje fatkeqësie (zjarri, përmbytje, shembje, etj.), do të aktivizohet plani i rikuperimit në rast fatkeqësie; ky plan zbatohet për të gjitha burimet operacionale të Intesa Sanpaolo dhe për burimet e palës së tretë që ofron shërbimin e vulës datare/kohës.

5. NDËRPRERJA E NJË CERTIFIKATE TË KUALIFIKUAR PËR SHËRBIMIN E NËNSHKRIMIT ELEKTRONIK

5.1 Detaje për ndërprerjen e certifikatës së kualifikuar për shërbimin e nënshkrimit elektronik

Në rast të përfundimit të shërbimit të Ofruesit të Shërbimit të Kualifikuar të Besimit, AGID do t'i dërgohet një komunikim specifik, të paktën 60 (gjashtëdhjetë) ditë përpara, duke përcaktuar, Autoritetin e ri të Certifikimit nëse është identifikuar Autoriteti i Certifikimit Zëvendësues. Si dhe menaxheri i regjistrit të certifikatave dhe dokumentacionit përkatës.
Në të njëjtën kohë me komunikimin për AgID, të gjithë Mbajtësit/Titullarët do të njoftohen për ndërprerjen e veprimtarisë.

Nëse nuk është identifikuar Autoriteti i Certifikimit Zëvendësues, në komunikim do të specifikohet qartë që të gjitha certifikatat e kualifikuara për nënshkrimin elektronik që ende nuk kanë skaduar në kohën e ndërprerjes së shërbimit do të revokohen. Certifikatat e kualifikuara për nënshkrimin elektronik përfshihen në listën e revokimit, në momentin e revokimit.

Për më shumë detaje në lidhje me ndërprerjen e shërbimit, i referohemi Planit të Ndërprerjes që ka përgatitur nga Intesa Sanpaolo.

6. MENAXHIMI I REFERENCAVE TË KOHËS

6.1 Shërbimi për vulën kohore/datare

Ky seksion i referohet nenit 40 (3) shkronja p e [DPCM].

Autoriteti i Certifikimit mundëson ofrimin e shërbimit të vulës datare/kohore në përputhje me [DPCM], duke përdorur shërbimet që ofrohen nga autoriteti i certifikimit që plotëson kërkesat për ushtrimin e aktivitetit në vendet ku ndodhen Bankat. Për përshkrimin e procedurave në lidhje me transmetimin e kërkesës për lëshimin e një vule datare/kohore dhe për blerjen e tij, në përputhje me ligjet dhe rregulloret në fuqi, ju lutemi referojuni manualit operacional të ofruesit të këtij shërbimi.

6.2 Saktësia e referencës kohore

Sistemi i menaxhimit të referencës së kohës arrin të nxjerrë kohën nga një radiomarrës i sinkronizuar me një sinjal të lëshuar nga Instituti Kombëtar i Elektroteknikës (IEN- Isituto Elettrotecnico Nazionale) "Galileo Ferraris".

Gjatë gjenerimit të vulës datare/kohore, serveri TSA nxjerr datën / kohën nga ora e sistemit, e cila mbahet në përputhje me kohën e saktë UTC (Ora e Koordinuar Universale) në sajë të sinjalit të sinkronizimit i cili merret nga një marrës i jashtëm që identifikon cilësinë e sinjalit të lëshuar nga rrjeti satelitor GPS. Sinjali kohor që merret në këtë mënyrë përputhet me marzhet e saktësisë të parashikuara në bazë të ligjeve dhe rregulloreve në fuqi.

7. PROCESI I VERIFIKIMIT TË NËNSHKRIMIT DIXHITAL

Ky seksion i referohet nenit 40 (3) germa r e [DPCM].

7.1 Aplikacioni i verifikimit

Në fushën "Dokumentet e mia" të kanaleve të drejtpërdrejta që ekzistojnë brenda Bankave, Mbajtësi/Titullari ka mundësinë të shohë dokumentet e tij / saj të nënshkruara në mënyrë dixhitale. Këto dokumente do të ruhen në formatin PDF dhe në varësi të kanalit në distancë (ueb, celular) të zgjedhur nga ana e mbajtësit/titullarit, ai / ajo gjithmonë do të ketë në dispozicionin e tij / saj aplikacionin vendas për atë kanal që i lejon atij / saj të verifikojë nënshkrimin dixhital që është përdorur/aplikuar.
Mbajtësi/Titullari gjithashtu mund të marrë dokumentet e nënshkruara në mënyrë dixhitale me email.

Sikundër përcaktohet në nenin 42 (2) të [DPCM], sistemet e verifikimit në dispozicion të mbajtësit/titullarit përdoren dhe ndërveprojnë me dokumentet e nënshkruara duke përdorur nënshkrimin dixhital të lëshuar nga Autoriteti i Certifikimit.

7.2 Formati i dokumenteve

Dokumentet që i paraqiten mbajtësit/titullarit përmes kanaleve të direkte të Bankave, janë në përputhje me ligjet dhe rregulloret në fuqi; në veçanti, dokumentet në formë elektronike, nuk mund të përmbajnë "*udhëzime makro, kode ekzekutuese ose elementë të tjerë që mund të aktivizojnë funksione që mund të modifikojnë aktet, faktet ose të dhënat e përfshira në to*".

7.3 Paralajmërimet për konsultimet CRL

Koha e nevojshme teknike për përditësimin e informacionit të përfshirë në CRL do të merren parasysh nga Mbajtësi/Titullari dhe subjekti juridik gjatë konsultimit të tij.

Në veçanti, këto orare të nevojshme teknike duhen në rast se Mbajtësi, Personi Juridik, Autoriteti i Regjistrimit ose Autoriteti i Certifikimit synon të revokojë ose riaktivizojë një certifikatë të kualifikuar për nënshkrimin elektronik, si dhe në rast se Autoriteti i Certifikimit kryen procedurat teknike / administrative që lidhen me kërkesat për revokim dhe përditësimin përkatës me CRL.

Nëse nënshkruani një dokument duke përdorur certifikatën e kualifikuar për nënshkrimin elektronik, lista CRL kontrollohet që të sigurojë që certifikata përkatëse e kualifikuar për nënshkrimin elektronik të mos jetë e revokuar.

8. PROCEDURA OPERACIONALE PËR GJENERIMIN E NËNSHKRIMEVE DIXHITALE

Ky seksion i referohet nenit. 40 (3) germa s të [DPCM].

Veçoritë e shërbimit nuk përfshijnë dorëzimin e një aplikimi për nënshkrim që do të instalohet në pajisjen e Mbajtësve/Titullarëve (kompjuter personal, telefon inteligjent smartphone, etj.); të gjitha funksionet që lejojnë mbajtësin të nënshkruajë një ose më shumë dokument (et) dixhitale, do të përfshihen drejtpërdrejt në një seksion specifik në Marrëveshjen e Përdorimit të Shërbimit Bankar Dixhital dhe / ose Marrëveshjen për Ofrimin e Shërbimeve të Certifikimit që përdoren nga Bankat.

Nënshkrimet dixhitale që krijohen me Shërbimin Bankar Dixhital plotësojnë kërkesat e parashikuara për algoritmet e nënshkrimit të përcaktuara në nenin 4 (2) të [DPCM].