Uporabniški priročnik za elektronski podpis #withSIGN

Distribucija:	JAVNO								
Šifra dokumenta:	ISP	-	SCD	-	04	-	2018	-	01
	Družba		*Storitev*		*Šifra*		*Leto*		*Različica*

RAZLIČICE UPORABNIŠKEGA PRIROČNIKA ZA ELEKTRONSKI PODPIS #WITHSIGN

Različica	Datum izdaje	Opis sprememb
01	1.12.2018	Prva različica
02	02.07.2019	Letni pregled
03	31.10.2019	Review
04	30.11.2019	Posodobitev dokumenta po zamenjavi ločljivosti 45 AgID

VSEBINA

1. SPLOŠNE INFORMACIJE

1.1 Pregled

Ta Uporabniški priročnik za elektronski podpis #withSIGN (kot je opredeljen v nadaljevanju) ureja kvalificirana potrdila za storitve elektronskega podpisovanja, nudene Imetnikom (kot so opredeljeni v nadaljevanju) mednarodne hčerinske Banke (kot je opredeljena v nadaljevanju), v skladu z zakonsko uredbo 82/2005 Kodeks za digitalno upravo), kot je bila naknadno spremenjena, ter veljavno nacionalno in evropsko zakonodajo, s strani Intesa Sanpaolo S.p.A., v zvezi s storitvami preko več poti (se pravi dostop Imetnikov do storitev, ki jih nudijo mednarodne hčerinske Banke preko poti na daljavo in v poslovalnicah).
Uporabniški priročnik za elektronski podpis #withSIGNse sklicuje tudi na tehnična pravila za izvedbo pravnega okvirja za elektronske podpise, vsebovana v [DPCM] 22.02.2013. V primeru spremembe zakonodaje se Uporabniški priročnik za elektronski podpis #withSIGN ustrezno spremeni.

1.2 Opredelitev pojmov in razlaga

V nadaljevanju navedeni pojmi, uporabljeni v tem porabniškem priročniku za elektronski podpis na daljavo, imajo naslednji pomen:

- **»vlagatelj«**: uporabnik, ki zaprosi za izdajo kvalificiranega potrdila za elektronski podpis, ko je kvalificirano potrdilo za elektronski podpis izdano, vlagatelj postane Imetnik,
- **»poslovalnica«**: lokacija, kjer se izvaja poslovanje med komitentom in banko, to vključuje vse prostore, pisarne in lokacije mednarodne hčerinske Banke,
- **»certifikacijski organ«**: ponudnik storitev zaupanja, ki je pooblaščen za izdajo kvalificiranih potrdil za elektronski podpis v certifikacijskem postopku, ki je skladen z mednarodnimi standardi ter evropskimi in nacionalnimi zakoni in predpisi. Za namene tega Uporabniškega priročnika za elektronski podpis »withSIGN je certifikacijski organ Intesa Sanpaolo S.p.A.,
- **»družba«:** javna ali zasebna družba, ki je z mednarodno hčerinsko Banko podpisala pogodbo o uporabi elektronskih bančnih storitev,
- **»podjetja«:** vse javne ali zasebne družbe, ki so komitenti mednarodnih hčerinskih Bank,
- **«Imetnik«:** končni Imetnik, fizična ali pravna oseba, ki je z mednarodno hčerinsko Banko podpisala pogodbo o uporabi elektronskih bančnih storitev,
- **»sklepanje pogodbe na daljavo preko spletne strani Banke«**: predstavlja kanal za izvedbo postopka procesa sklepanja pogodbe na daljavo na podlagi video identifikacije, ki vključuje osebno identifikacijo posameznika na podlagi predložitve osebnega dokumenta, ki je izvedena s strani bančnega delavca,
- **»mednarodne hčerinske Banke«**: katerakoli mednarodna hčerinska Banka, ki je del skupine Intesa Sanpaolo,
- **»imetnik«**: Imetnik, ki mu je bilo izdano kvalificirano potrdilo za elektronski podpis, Imetnik sme potrdilo uporabljati za elektronsko podpisovanje elektronskih dokumentov, ob zagotavljanju avtentičnega izvora tovrstnih elektronskih dokumentov in integritete njihove vsebine, v skladu z omejitvami, vsebovanimi v Pogodbi o upravljanju storitev s kvalificiranimi potrdili za fizične osebe
- **»Intesa Sanpaolo«**: Intesa Sanpaolo S.p.A., ponudnik kvalificiranih storitev zaupanja,
- **»enkratno geslo (OTP)«:** geslo, ki je veljavno zgolj za eno transakcijo, katero se ustvari in da na razpolago Imetniku neposredno pred elektronskim podpisovanjem. OTP se komitentu pošlje preko sporočila SMS, če je pot digitalni prevzem ali poslovalnica Banke. Pri storitvah digitalnega bančništva na daljavo OTP generira TOKEN.
- **»Registracijski organ«**: subjekt, zadolžen predvsem za: (i) identifikacijo vlagateljev, za zagotavljanje točnosti njihove identitete (i), zagotavljanje vseh informacij o kvalificiranih potrdilih za elektronski podpis in omejitvi njihove uporabe, (iii) sklenitev pogodb z vlagatelji v imenu in za račun Intesa Sanpaolo, (iv) predložitev Intesi Sanpaolo zahteve za preklic in začasno ukinitev kvalificiranih potrdil za elektronski podpis. Za namene tega Uporabniškega priročnika je registracijski organ katerakoli od mednarodnih hčerinskih Bank Intese Sanpaolo S.p.A., ki je z Banko Intesa Sanpaolo S.p.A. sklenila sporazum o kvalificiranih potrdilih za elektronski podpis.

- **»Uporabniški priročnik za elektronski podpis #withSIGN «**: ta dokument, kot je morebiti spremenjen in dopolnjen.
- **»Banka«**: vse mednarodne hčerinske banke, ki pripadajo k skupini Intesa Sanpaolo.
- **»TOKEN«**: varni avtentikacijski sistemi, ki zagotavljajo močno preverjanje pristnosti strank (SCA); uporablja se za generiranje OTP (enkratno geslo) po verifikaciji oz. preverjanju PIN številke.
- **»Zasebni ključ«:** pomeni rezerviran element para asimetričnih ključev shranjenih na zaščiten način s strani Ponudnika kvalificiranih storitev zaupanja na ustrezni napravi za podpisovanje.
- **»Javni ključ«:** pomeni element para asimetričnih ključev shranjenih s katerim se izvaja overjanje elektronskega podpisa.

1.2.1 Sklicevanje na pravne akte

[Dlgs 82/2005]	Zakonodajna uredba št. 82 z dne 7. marca 2005, objavljena v Uradnem listu št. 112 z dne 16. maja 2005 – Redni dodatek št. 93 »Kodeks digitalne uprave«, posodobljen z zakonsko uredbo št. 217 z dne 13. decembra 2017, objavljeno v Uradnem listu št. 9 januarja 2018.
[DPCM]	Odlok predsednika vlade z dne 22. februarja 2013 – Tehnična pravila za kreiranje, uporabo in potrjevanje naprednih, kvalificiranih in elektronskih podpisov, v skladu s členi 20 (3), 24 (4), 28 (3), 32 (3) črka b), 35 (2), 36 (2) in 71.
[CNIPA/CR/48]	CNIPA/CR/ 48 Okrožnica št. 48 z dne 6. septembra 2005 (objavljena v Uradnem listu št. 213 z dne 13. septembra 2005), Postopek za predložitev vloge za vpis v javni seznam ponudnikov storitev certifikacije, v skladu s členom 28 (1) Predsedniškega odloka št. 445 z dne 28. decembra 2000.
[Del 45/2009]	Sklep št. 45 z dne 21. maja 2009 – Pravila za priznavanje in potrjevanje elektronskih dokumentov.
Uredba EU 910/2014 – eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES.
Uredba (EU) št. 679/2016 – GDPR	Uredba (EU) št. 679/2016 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).
Razprava AgID n.121/2019	Smernice, ki vsebujejo tehnična pravila in priporočila v zvezi s kreiranjem kvalificiranih elektronskih potrdil, kvalificiranega elektronskega podpisa in žigov ter kvalificiranih elektronskih časovnih potrditev.

1.3 Sklicevanja na standarde

[LDAP2] Zeilenga, »Lahki protokol za dostop do imenikov, različica 2«, Internet RFC 3494, marec 2003.
[PKCS7] B. Kaliski, »PKCS#7: Sintaksa za šifriranje sporočil, različica 1,5«, Internet RFC 2315, marec 1998.

[PKCS10] B. Kaliski, »PKCS#10: Sintaksa za zahtevke za certifikacijo, različica 1,7«, Internet RFC 2986, november 2000.

[SHA1] ISO/IEC 10118-3-2018, »Informacijska tehnologija – varnostne tehnike – funkcije razpršitve – Del 3: Namenske funkcije razpršitve«, 2018.

[SHA-256] ISO/IEC 10118-3:2018, »Informacijska tehnologija – varnostne tehnike – funkcije razpršitve – Del 3: Namenske funkcije razpršitve«

[X500] ISO/IEC 9594-1: 2008, ISO/IEC 9594-2:2008 »Informacijska tehnologija – povezava med odprtimi sistemi – imenik: pregled konceptov, modelov in storitev«.

[X509] ISO/IEC 9594-8: 2008 »Informacijska tehnologija – povezava med odprtimi sistemi – imenik: javni ključ in okvirji atributov potrdila«.

[RFC3647] Internet X.509 Usmeritve glede infrastrukture javnih ključev potrdil in okvirji certifikacijskih praks, S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu.

[RFC 3778] PDF aplikacija, Taft, Pravetz, Zilles, Masinter, maj 2004.

1.4 Kratice

V nadaljevanju navedenim pojmom, uporabljenim v tem Uporabniškem priročniku za elektronski podpis #withSIGN, ustrezajo naslednje kratice:

AgID Agencija za digitalno Italijo

CRL Seznam preklicev potrdil

CPS Izjava o praksi v zvezi s potrdili

DBMS Sistem upravljanja podatkovnih baz

DN Razločevalno ime

DNS Sistem domenskih imen

DPR Predsedniški odlok

HSM Strojni varnostni modul

HTTP Protokol prenosa za hipertekst

ITSEC Merila za ocenjevanje varnosti informacijske tehnologije

LDAP Lahki protokol za dostop do imenikov

NEI Nacionalni elektrotehniški inštitut »Galileo Ferraris« (»Istituto Elettrotecnico Nazionale« v italijanskem jeziku)

OTP Enkratno geslo

PDF Format prenosljivih dokumentov

PIN Osebna identifikacijska številka

PKCS	Standard šifriranja z javnim ključem
RDS	Oddaljeni elektronski podpis
RFC	Zahtevek za komentarje
RSA	Rivest-Shamir-Adleman
SHA-1	Varne funkcije razpršitve 1
SHA-2	Varne funkcije razpršitve 2
SSL	Sloj varnih vtičnic
URL	Enolični krajevnik vira

2. UVOD

Elektronski podpis temelji na asimetričnih ključih, enemu javnemu in enemu zasebnemu, ki zagotavljata pristnost izvora digitalno podpisanih elektronskih dokumentov in integritete njihove vsebine za enega ali več prejemnikov, ki lahko preverijo veljavnost.

Nove določbe, uveljavljene s členom 8 DPCM certifikacijskemu organu omogočajo hrambo zasebnih ključev Imetnikov (se pravi ključev, ki se uporabljajo za kreiranje elektronskega podpisa) na posebnih varnostnih napravah (se pravi HSM), ob zagotavljanju, da je uporaba ključev omogočena izključno Imetniku, v skladu s členom 11 (2) [DPCM].

Posledično za uporabo digitalnega podpisa imetniku ni več potrebno posedovati opreme za elektronsko podpisovanje (npr. pametnih kartic, posebnih čitalnikov in ustrezne programske opreme), certifikacijski in registracijski organi pa lahko storitve digitalnega podpisovanja Imetnikom nudijo preko neposrednih poti (se pravi spleta ali mobilnikov).

Imetnik lahko prične postopek elektronskega podpisovanja z uporabo OTP (ki je bodisi prejeto na certificirano mobilno številko ali v storitvi oddaljenega bančništva, ki ga ustvari TOKEN z vnosom PIN), medtem je zagotovljen izključni nadzor Imetnika. Proces se lahko v poslovalnici sproži tudi z uporabo čitalnika kartic (se pravi vlagatelj/Imetnik lahko izvede prvi korak, tako da v poslovalnici svojo debetno kartico skenira s čitalnikom kartic).

Ta Uporabniški priročnik za elektronski podpis # wtihSIGN # pojasnjuje naslednje procese:

- kreiranje ključa podpisa in upravljavski postopki v okviru storitev digitalnega podpisa na daljavo, ki jih nudi Intesa Sanpaolo,
- aktivacijski postopek digitalnega podpisa na daljavo in mehanizem močne avtentikacije v elektronski banki, na podlagi postopka avtentikacije, ki ga opredelijo mednarodne hčerinske banke,
- vlogo tako certifikacijskega kot registracijskega organa, v skladu z veljavno zakonodajo in predpisi,

Uporabniški priročnik velja za vse mednarodne banke Intesa Sanpaolo v okviru področja mednarodnih odvisnih bank.

Spodnji odstavki se nanašajo na zahteve, ki izhajajo iz člena 40 (3) a, b in c [DPCM].

2.1 Identifikacijski podatki certifikacijskega organa

Storitev certifikacije nudi spodaj navedeni subjekt:

Naziv:	**Intesa Sanpaolo S.p.A.**
Sedež:	**Piazza San Carlo, 156 10121 Torino**
Pravni zastopnik:	**Carlo Messina, glavni in izvršni direktor**
Registracijska številka v torinskem poslovnem registru:	**Poslovni administrativni register (REA) št. 00799960158**
Št. za DDV:	**10810700152**
Tel. (centrala):	(+39) 011 555 1
ISO identifikator predmeta (OID):	**1.3.6.1.4.1.20052**
Splošna spletna stran (informacije):	**www.intesasanpaolo.com**
Spletna stran za storitev digitalne certifikacije:	**ca.intesasanpaolo.com**

Identifikacija uporabniškega priročnika za elektronski podpis Uporabniški priročnik se identificira s pomočjo šifre dokumenta ISP-SCD-04-2018-01 (ki je navedena tudi na naslovni strani).

Uporabniški priročnik za elektronski podpis #withSIGN je objavljen na spletni strani certifikacijskega organa in je tako na voljo na spletu.

Trenutno veljavna različica uporabniškega priročnika #withSIGN je na voljo v elektronski obliki:

- na spletni strani certifikacijskega organa (https://ca.intesasanpaolo.com/),
- na spletni strani AgID,
- na bančni spletni strani področja mednarodnih hčerinskih Bank (Intesa Sanpaolo Slovenija – Uporabniški priročnik za elektronski podpis #withSIGN).

V primeru neskladja velja različica, objavljena na spletni strani AgID.

2.2 Oseba, odgovorna za uporabniški priročnik

Oseba, odgovorna za ta Uporabniški priročnik je:

Ezio Barbero
Intesa Sanpaolo S.p.A.

3. SPLOŠNE DOLOČBE

3.1 Obveznosti registracijskega organa, certifikacijskega organa in Imetnika

3.1.1 Obveznosti certifikacijskega in registracijskega organa

Certifikacijski organ deluje v skladu z določbami DLgs 82/2005, člen 32, in sprejema vse organizacijske in tehnične ukrepe za preprečitev povzročanja škode tretjim osebam.

Certifikacijski organ, ki izdaja, v skladu s členom 27 DLgs 82/2005, kvalificirana potrdila za elektronski podpis mora tudi:

- ustrezno identificirati vlagatelja, to registracijski organ opravi v skladu z nacionalni zakonodajo,
- jasno in v celoti informirati vlagatelja o lastnostih kvalificiranega potrdila za elektronski podpis in omejitvah njegove uporabe, to registracijski organ opravi pred sklenitvijo Pogodbe o upravljanju storitev s kvalificiranimi potrdili za fizične osebe ,
- izvede, na podlagi navodil, ki jih brez odlašanja poda registracijski organ, pravočasni preklic kvalificiranih potrdil za elektronski podpis in ustrezno objavo,
- sprejme varnostne ukrepe za obdelavo osebnih podatkov, v skladu z ustrezno zakonodajo in predpisi, to je obveza tako registracijskega kot tudi certifikacijskega organa,
- izda kvalificirana potrdila za elektronski podpis, kot to predpisuje DPCM, v skladu z Uredbo GDPR, kot je bila spremenjena in dopolnjena,
- ravna v skladu s tehničnimi pravili iz DPCM in člena 71 DLgs 82/2005,
- zagotavlja, da ima varna naprava za kreiranje podpisov lastnosti in varnostne zahteve, kot jih predpisuje člen 35 od [DLgs 82/2005 in člen 11 DPCM,
- hrani evidence, tudi v elektronski obliki, za vse podatke, ki zadevajo kvalificirana potrdila za elektronski podpis, vsaj 20 (dvajset) let, da lahko dokaže certifikacijo v morebitnih sodnih primerih,
- hrani evidence, tudi v elektronski obliki, za vse dokumente, ki jih podpiše Imetnik med postopkom izdaje kvalificiranih potrdil za elektronski podpis, vsaj 20 (dvajset) let, to izvaja registracijski organ,
- ne izvaža zasebnih ključev imetnikov iz HSM, kjer so tovrstni ključi kreirani in uporabljeni,
- certifikacijski in registracijski organ tudi posodabljata Uporabniški priročnik na daljavo, registracijski organ pa o vseh spremembah brez odlašanja obvesti Imetnika.

3.1.2 Obveznosti vlagatelja/Imetnika

Imetnik zagotavlja varovanje vseh informacij, ki mu omogočajo uporabo zasebnega ključa, in sprejme vse tehnične in organizacijske ukrepe za preprečitev nastanka škode tretjim osebam, Imetnik mora tudi osebno uporabljati podatke, ki omogočajo kreiranje digitalnega podpisa (člen 8 (5) DPCM).

Vlagatelj/Imetnik mora tudi ravnati v skladu z DPCM [DPCM];, še zlasti mora vlagatelj/Imetnik:

- vložiti zahtevo za kvalificirano potrdilo za elektronski podpis v skladu s postopki, navedenimi v tem Uporabniškem priročniku za elektronski podpis #withSIGN
- varovati zasebne šifre (šifre, ki jih generira TOKEN – programski generator gesel in OTP, ki ga prejme preko SMS sporočila), ki je potrebna za uporabo kvalificiranih potrdil za elektronski podpis
- vložiti zahtevo za preklic kvalificiranega potrdila za elektronski podpis v skladu s postopki, navedenimi v tem Uporabniškem priročniku zaelektronski podpis #withSIGN ,
- nemudoma obvestiti registracijski organ o vseh spremembah podatkov, ki so bili podani registracijskemu organu v postopku registracije (osebni podatki, naslovi ...),
- ne sme uporabiti zasebnega ključa za namene, ki niso tisti, navedeni v omejitvah uporabe, opredeljenih za kvalificirana potrdila za elektronski podpis v pogodbi o uporabi bančnih storitev (Vloga in Splošni pogoji za digitalno bančništvo) in Pogodbi o upravljanju storitev s kvalificiranimi potrdili za fizične osebe,

- podati točne, resnične in popolne informacije osebi, ki opravlja identifikacijo v zvezi z zahtevkom za certifikacijo,
- uporabljati potrdilo samo za metode, opredeljene v tem Uporabniškem priročniku in veljavni nacionalni in nadnacionalni zakonodaji.

3.1.3 Obveznosti Pravnih oseb

Če Imentik v imenu pravne osebe uporablja kvalificirano potrdilo za elektronski podpis mora pravna oseba Imetniku zagotoviti ustrezno poooblastilo za uporabo kvalifiricanega potrdila za elektronski podpis na njegovo ime.

Pravna oseba mora ravnati v skladu z [DPCM]; še zlasti mora pravna oseba:

- zahtevati preklic kvalificiranega potrdila za elektronski podpis v skladu s postopki, ki so določeni v tem Uporabniškem priročniku;
- nemudoma obvestiti registracijski organ o vseh spremembah podatkov, ki so bili med postopkom registracije posredovani registracijskemu organu (osebni podatki Imetnika, smrt Imetnika, izguba poslovne sposobnosti, podatki pravne osebe, itd…)-;
- uporabljati kvalificiran elektronski podpis samo za metode, ki so določene v tem Uporabniškem priročniku in veljavni nacionalni in mednarodni zakonodaji.

3.1.4 Obveznosti subjekta, ki mora preveriti podpis

Subjekti, ki preverjajo elektronske podpise, ki jih kreirajo certifikacijski ključi Intesa Sanpaolo, morajo:

- preveriti obdobje veljavnosti potrdila (v skladu z veljavno zakonodajo),
- preveriti, s pomočjo seznama preklicanih kvalificiranih potrdil za elektronski podpis, če je bilo potrdilo preklicano trenutku podpisa,
- preveriti, ali se elektronski podpis nanaša na kvalificirano potrdilo, ki ga je izdal certifikacijski organ, ki ga predhodno odobri AgID, ob času podpisa,
- zagotoviti, da ima tipologija kreiranih »naročniških« ključev (kot to predpisuje DPCM, člen 5, odstavek 4, črka a) in ključ podaljšanja uporabe potrdila 11 (OID: 2.3.29.15) zgolj nezavrnjene vrednosti (bit 1 nizi na 1) (kot to predpisuje CNIPA 45/2009, člen 12, odstavek 5, črka a),
- preveriti morebitne omejitve uporabe, navedene v kvalificiranem potrdilu.

3.2 Omejitev odgovornosti in odškodovanje

3.2.1 Omejitev odgovornosti

Intesa Sanpaolo ne prevzema odgovornosti za morebitne motnje, ki bi izhajale iz nespoštovanja s strani imetnika veljavne zakonodaje in predpisov ali tehničnih/operativnih specifikacij, vsebovanih v pogodbi o uporabi elektronskih bančnih storitev banke, ki jo skleneta Imetnik in mednarodna hčerinska Banka, ali drugimi tam navedenimi dokumenti.

Intesa Sanpaolo ne prevzema odgovornosti za škodo, ki bi izhajala iz uporabe, ki presega omejitve, opredeljene v kvalificiranih potrdilih za elektronski podpis in/ali pogodbi o uporabi digitalnih bančnih storitev mednarodne hčerinske banke in/ali pogodbi o upravljanju storitev s kvalificiranimi potrdili za fizične osebe.

Omejitve uporabe, opredeljene v kvalificiranih potrdilih za elektronski podpis, so naslednje:
»uporaba je omejena na dokumente, povezane z odnosom med Imetnikom potrdila in družbami skupine Intesa Sanpaolo ali subjekti izven te skupine, ki ponujajo storitve na elektronskih sistemih družb skupine.«

Poleg tega je uporaba kfvalificiranih potrdil za elektronski podpis omejena na domeno, določeno v Pogodbi o upravljanju storitev s kvalificiranimi potrdili za fizične osebe.

Nadaljnje omejitve, ki so značilne za posamezen produkt / storitev ali nacionalno zakonodajo bodo obravnavane v Splošnih pogojih za posamezen produkt / storitev.

3.2.2 Odškodovanje

Kot je opredeljeno v členu 3.2.1. zgoraj, Intesa Sanpaolo ne prevzema odgovornosti za škodo, ki bi izhajala iz neprimerne uporabe kvalificiranih potrdil za elektronski podpis.

Vendar pa je, v skladu s členom 15 (1) i) [DPCM], Intesa Sanpaolo opredelila posebno zavarovanje za kritje tveganj in škode, ki bi izhajala iz ali bila v zvezi z izdajo kvalificiranih potrdil za elektronski podpis.

3.3 Čas razpoložljivosti

Storitve, ki jih ponuja kvalificiran ponudnik storitev zaupanja (izdaja kvalificiranih potrdil za elektronski podpis in uporaba kvalificiranega elektronskega podpisa), so vedno na voljo preko neposrednih kanalov (na spletu in preko mobilnikov) in v poslovalnicah Banke.

4. OPERATIVNI VIDIKI

4.1 Vsebina kvalificiranih potrdil za elektronski podpis

Vsebina kvalificiranih potrdil za elektronski podpis, ki jih izdaja Intesa Sanpaolo, je skladna z določbami člena 28 [Dlgs 82/2005] in člena 12 Sklepa št. 45/2009, ki ga je izdal Nacionalni center za informacijsko tehnologijo v javni upravi (trenutno AgID).

Kvalificirana potrdila za elektronski podpis ne bodo objavljena v javnih registrih.
Kvalificirano potrdilo za elektronski podpis je veljavno 3 (tri) leta.

Elektronski podpis na daljavo Imetniku omogoča sklepanje pogodb z Banko. Storitev je mogoča preko vseh kanalov, ki jih vsebuje digitalno bančništvo (Digitalna Poslovalnica, mobilna in spletna banka, ter spletna stran Banke).
Za uporabo podpisana daljavo mora Imetnik imeti kvalificirano potrdilo za elektronski podpis.

4.2 Organizacijska pravila za zaposlene

Zaposleni, odgovorni za nudenje in nadzor certifikacijskih storitev, so organizirani v skladu z DPCM 2013, kar med drugim pomeni, da so vloge glede odgovornosti opredeljene, kot je navedeno v členu 38 DPCM.

Med opravljanjem svojih nalog si lahko odgovorni zaposleni pomagajo z drugimi zaposlenimi ostalih Bank.
V zvezi z Uporabniškim priročnikom za elektronski podpis #withSIGN delavci opravljajo storitve certifikacije (kar ima tukaj pomen registracije ali identifikacije Imetnika) v poslovalnicah Banke, izven centra za obdelavo podatkov Intesa Sanpaolo, izmenjava podatkov med temi delavci in banko Intesa Sanpaolo poteka preko varnih komunikacijskih poti. Registracijo izvaja Banka na podlagi posebne pogodbe, ki jo skleneta mednarodna Banka in Intesa Sanpaolo.

Dejavnosti registracije izvajajo banke na podlagi posebne pogodbe, ki jo skleneta Banka in Intesa Sanpaolo.
Bančni operaterji izvajajo aktivnost registracije v skladu s procesi, ki so bili dogovorjeni med Bankami in Intesa Sanpaolo. Omenjene aktivnosti in procesi se izvajajo po postopkih v skladu z Zakonom o preprečevanje pranja denarja in financiranje terorizma.

4.3 Postopek kreiranja ključev

Vsaka vrsta ključev, navedena v členu 5 [DPCM], se kreira, hrani in uporablja v varnih napravah, ki so skladne z varnostnimi zahtevami, opredeljenimi v veljavni zakonodaji in predpisih.

Ključi imajo lastnosti, opredeljene v [DPCM].

4.3.1 Postopek kreiranja[1] certifikacijskih ključev

Certifikacijski ključi se kreirajo v skladu z veljavno zakonodajo in predpisi, še zlasti pa so:

- certifikacijski ključi kreirani s strani zaposlenih, ki so izrecno imenovani s strani certifikacijskega organa,
- posebno kvalificirano potrdilo za elektronski podpis se kreira za vsak par certifikacijskih ključev, kot je opredeljeno v sklepu št. 45/2009, podpisano z ustreznim zasebnim ključem para, ki se pošlje AgID v skladu s postopki, predhodno dogovorjenimi med certifikacijskim organom in AgID.

[1] Ključi, ki jih uporabi certifikacijski organ za izdajo kvalificiranih potrdil za elektronski podpis na zahtevo Imetnika.

4.3.2 Postopek kreiranja ključa časovnega žiga

Glede storitve časovnega žiga v zvezi s storitvami digitalnega podpisovanja, ki jih nudijo Banke, Intesa Sanpaolo uporablja certifikacijski organ, ki izpolnjuje potrebne zahteve za nudenje storitev v državi, kjer se nahaja ustrezna Banka.

4.4 Postopek identifikacije in registracije Imetnika

Izdaja kvalificiranih potrdil za elektronski podpis je veljavna zgolj za tiste, ki se kvalificirajo kot Imetniki, se pravi tiste, ki so že sklenili Pogodba o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis fizičnih oseb_v1glava Banke.

Kvalificirano potrdilo za elektronski podpis za Imetnika vsebuje tudi podatke o Podjetju in Davčno številko.
Pri pravnih osebah lahko vsak Imetnik pridobi kvalificirano potrdilo za elektronski podpis za vsako podjetje za katerega je pooblaščen.
Postopke identifikacije in registracije Imetnika izvaja ustrezna Banka, v skladu z veljavno zakonodajo in predpisi, vključno z Zakonom o preprečevanju pranja denarja in financiranja terorizma, kar se upošteva ob sklenitvi pogodbe z Imetnikom.

Identifikacijo potencialnega Imetnika Banke se izvede bodisi (i) osebno, s fizično prisotnostjo komitenta v prostorih banke, bodisi (ii) na daljavo z uporabo identifikacijskih metod, ki nudijo enakovredna zagotovila v smislu zanesljivosti. To dejavnosti se izvajajo v skladu s postopki skladnimi z Zakonom o preprečevanju pranja denarja in financiranja terorizma, ki so skladni s postopki na podlagi fizične prisotnosti komitenta v prostorih Banke, kar pomeni tudi upoštevanje člena 24 1.(d) Uredbe Eidas.

4.4.1 Identifikacija in registracija Imetnika

Imetnik je identificiran v predhodno opredeljenih postopkih, ki se razlikujejo glede na kanal digitalne Banke.
Identifikacija Imetnika se izvede bodisi s fizično prisotnostjo bodisi na daljavo. Zlasti:

- pri identifikaciji osebe v Digitalni Poslovalnici se mobilna številka, ki jo poda Imetnik, certificira tako, da se preko SMS sporočila pošlje OTP in Imetnika zaprosi, da ga vnese. Imetnik se lahko identificira tudi s skeniranjem njegove debetne kartice na čitalniku kartic,
- med spletno identifikacijo pri oddaljenih storitvah digitalnega bančništva se Imetnik v mobilni ali spletni banki avtenticira z vnosom PIN kode v svoj TOKEN, v skladu s storitvijo digitalnega bančništva in dodatno OTP kodo, ki jo prejme prek SMS sporočila. Pri video identifikaciji osebe v procesu sklepanja pogodb preko spleta se mobilna številka, ki jo poda Imetnik, certificira tako, da preko SMS sporočila prejme OTP in jo vnese.

Vsi postopki identifikacije se izvedejo v skladu z lokalno bančno zakonodajo in skladno z Zakonom o preprečevanju pranja denarja in financiranja terorizma ali na podlagi fizične prisotnosti komitenta v prostorih Banke. Identifikacijo Imetnika izvede ustrezna Banka pred sklenitvijo Pogodbe o uporabi digitalnega bančništva ter Pogodbe o upravljanju storitev s kvalificiranimi potrdili za fizične osebe.

Po uspešni identifikaciji lahko Imetnik nadaljuje z aktivacijo storitve izdaje kvalificiranega potrdila za elektronski podpis in podpisom ustrezne pogodbe.

4.4.2 Aktivacija storitve Elektronskega podpisa na daljavo in podpis ustrezne pogodbe

Za aktivacijo elektronskega podpisa mora Imetnik opraviti naslednje postopke na različnih kanalih.

Storitve digitalnega bančništva:

- dostop do storitve digitalnega bančništva z uporabo postopkov avtentikacije, kot jih opredeli ustrezna Banka;
- po potrebi potrditev seznanitve s pravili, ki urejajo Pogodbo o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis;
- po potrebi preveriti in potrditi pravilnost osebnih podatkov vlagatelja z namenom aktivacije kvalificiranega potrdila za elektronski podpis. ;zahtevati vpis kvalificiranega potrdila za elektronski podpis;
- kreiranje OTP s strani TOKNA in vnos PIN kode, odvisno od storitve digitalnega bančništva. Ta proces zagotavlja mehanizem Močne avtentikacije;
- pregledati / preučiti Pogodbo o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis, zahtevati vpis kvalificiranega potrdila za elektronski podpis ter podpisati Pogodbo z elektronskim podpisom na podlagi vnosa OTP kode, ki jo generira TOKEN;
- dodatna OTP koda, ki jo prejme Imetnik prek SMS sporočila na njegovo potrjeno mobilno številko se zahteva zaradi dodatne kontrole;
- podpis Banke potrjuje aktivacijo storitve izdaje kvalificiranega potrdila za elektronski podpis.

Digitalna poslovalnica ali Spletna stran Banke:

- dostop do Spletne strani Banke ali osebni obisk v prostorih Banke;
- po potrebi sprejeti pravila, ki urejajo Pogodbo o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis;
- po potrebi preveriti in potrditi pravilnost osebnih podatkov z namenom aktiviranja kvalificiranega potrdila za elektronski podpis;
- zahtevati vpis kvalificiranega potrdila za elektronski podpis;
- prejeti OTP kodo preko SMS sporočila na njegovo potrjeno mobilno številko. Pri osebni identifikaciji in videoidentifikaciji Imetniku ni potrebno vnesti varnostne PIN kode. V poslovalnici Banke lahko Imetnik tudi skenira svojo debetno kartico, da izvede prvi korak avtorizacije prek čitalnika kartic;
- preučiti Pogodbo o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis in jo podpisati elektronsko na podlagi vnosa OTP in varnostne PIN kode. Pri osebni in video identifikaciji vnos varnostne PIN kode ni potreben.

Potrebna dokumentacija v zvezi s storitvijo kvalificiranih elektronskih potrdil bo stranki na voljo pred sklenitvijo Pogodbe o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis.

4.4.3 Izdaja kvalificiranih potrdil za elektronski podpis

Kvalificirana potrdila za elektronski podpis se izdajo po zaključku kreiranja para ključev, kot je navedeno zgoraj.

Postopek izdaje kvalificiranega potrdila za elektronski podpis je povsem pregleden za vlagatelja, ki v tej fazi ni v interakciji s certifikacijskim organom.

V skladu z veljavno zakonodajo mora certifikacijski organ zahtevek za izdajo kvalificiranega potrdila za elektronski podpis hraniti vsaj 20 (dvajset) let od datuma izdaje vsakega kvalificiranega potrdila za elektronski podpis. Še zlasti se elektronsko hranijo vsi sledovi, potrebni za kasnejše dokazovanje izvedbe teh dejanj.

4.5 Postopek preklica kvalificiranega potrdila za elektronski podpis

V skladu z [DPCM] do preklica kvalificiranega potrdila za elektronski podpis pride na zahtevo naslednjih subjektov, kot je navedeno v nadaljevanju:

- imetnik,
- podjetje,
- certifikacijski organ,
- registracijski organ.

4.5.1 Zahtevek za preklic s strani Imetnika

Imetnik lahko poda zahtevek za /preklic kvalificiranega potrdila za elektronski podpis poslovalnici Banke.

Ko je zahtevek za preklic podan, se sproži za Imetnika pregleden avtomatski mehanizem preklica kvalificiranega potrdila za elektronski podpis.

V primeru enostranske prekinitve Pogodbe o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis fizičnih oseb s strani Imetnika, registracijski organ o tem nemudoma obvesti certifikacijski organ, ki nato prekliče ustrezno kvalificirano potrdilo za elektronski podpis.
Po preklicu Imetnik ne more več podpisovati dokumentov z uporabo predhodno dodeljenih ključev, medtem ko vsi dokumenti, ki jih je Imetnik podpisal pred preklicem kvalificiranega potrdila za elektronski podpis, ostanejo v veljavi.
Glede učinkovanja preklica potrdil velja naslednje: (i) če preklic potrdila zahteva Imetnik, potem preklic prične učinkovati od datuma, ko Banka prejme obvestilo o preklicu,
(ii) če preklic potrdila zahteva Banka, potem preklic prične učinkovati od datuma, ko obvestilo o preklicu prejme Imetnik.

4.5.2 Preklic s strani certifikacijskega ali registracijskega organa

Razen v upravičeno nujnih primerih, bo certifikacijski ali registracijski organ, ki namerava preklicati kvalificirano potrdilo za elektronski podpis, Imetnika o tem obvestil vnaprej, z navedbo razlogov za preklic.

Registracijski organ mora certifikacijski organ nemudoma obvestiti o potrebi po preklicu kvalificiranega potrdila za elektronski podpis.
Certifikacijski organ mora potrdilo preklicati v naslednjih primerih:

- na izrecno zahtevo imetnika,
- če se izkaže, da so podatki o Imetniku v evidencah potrdila nepravilni ali nepopolni,
- če prejme uradno obvestilo o smrti Imetnika,
- če prejme uradno obvestilo o izgubi poslovne sposobnosti Imetnika,
- v primeru odpovedi Pogodbe o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis fizičnih oseb;
- če ugotovi, da je Imetnik za izdajo potrdila podal neresnične podatke.

4.5.3 Zaključek postopka preklica kvalificiranega potrdila za elektronski podpis

Ob zaključku postopka preklica kvalificiranega potrdila za elektronski podpis se kreira nov CRL, ki se objavi v ustreznem imeniku, ki je na voljo preko spletne povezave.
CRL se objavi, kot je navedeno v odstavku 4.9.2. Nadalje se učinkovanje preklica kvalificiranega potrdila za elektronski podpis zabeleži v kontrolni dnevnik.

4.6 Postopek preklica kvalificiranega potrdila za elektronski podpis

Glede na [DPCM] začasna ukinitev kvalificiranega potrdila za elektronski podpis nastane na zahtevo naslednjih strank:
• certifikacijski organ;

• registracijski organ.
Razen v primerih upravičene nujnosti certifikacijski ali registracijski organ, ki namerava začasno preklicati kvalificirano potrdilo za elektronski podpis o tem v naprej obvesti Imetnika / pravno osebo z navedbo razlogov začasne prekinitve.

4.7 Postopek ob izgubi naprave za PIN in OTP (TOKEN)

Imetnik lahko za metodo avtentikacije uporabi napravo za OTP.
V primeru izgube ali kraje naprave za OTP mora Imetnik ravnati v skladu s Splošnimi pogoji digitalnega bančništva.
Postopek glede izgube PIN-a je enak kot pri izgubi naprave za OTP.

4.8 Postopek zamenjave ključev

4.8.1 Zamenjava ključev za podpis Imetnika

V skladu z [DPCM] certifikacijski organ določi iztek kvalificiranega potrdila za elektronski podpis in obdobje veljavnosti ključev, na podlagi dolžine ključev in storitev, za katere se le-ti uporabljajo.

Obdobje veljavnosti ključev je enako obdobju veljavnosti ustreznih kvalificiranih potrdil za elektronski podpis, ki je 3 (tri) leta.

Zahtevek za izdajo novih kvalificiranih potrdil za elektronski podpis je dovoljen le, če je prejšnje potrdilo poteklo ali je bilo preklicano.
Imetnik ne more hkrati imeti 2 (dveh) aktivnih kvalificiranih potrdil za elektronski podpis za isto podjetje.

4.8.2 Zamenjava certifikacijskih ključev

Zamenjavo certifikacijskih ključev certifikacijski organ izvede v skladu z veljavno zakonodajo in predpisi.

4.9 Vodenje imenika kvalificiranih potrdil za elektronski podpis

4.9.1 Imenik kvalificiranih potrdil za elektronski podpis

Vsa veljavna kvalificirana potrdila za elektronski podpis, ki jih izda certifikacijski organ, se hranijo v »imeniku potrdil«.

Javni imenik vsebuje naslednje podatke:

- potrdila za ključe certifikacijskega organa,
- potrdila, povezana s Pogodbo o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis fizičnih oseb
- potrdila za AgID podpisne ključe,
- seznam preklicanih kvalificiranih potrdil za elektronski podpis.

Seznam preklicanih kvalificiranih potrdil za elektronski podpis se objavi tudi z uporabo protokola HTTP http://crl2.ca.intesasanpaolo.com/FirmaQualificata/CRL20.crl.

Certifikacijski organ uporablja zanesljive sisteme za vodenje imenika kvalificiranih potrdil za elektronski podpis in javnega imenika ter uporablja metode, ki zagotavljajo, da:

- lahko podatke vnašajo in spreminjajo samo pooblaščene osebe,
- se lahko avtentičnost podatkov preveri,

- so potrdila na voljo za javnost, kolikor to dovoli imetnik,
- je delavec lahko seznanjen z dogodki, ki ogrožajo varnostne zahteve.

4.9.2 Objava kvalificiranih potrdil za elektronski podpis in CRL

Kvalificirana potrdila za elektronski podpis se objavijo v skladu s postopki iz člena 34 [DPCM].

CRL se kreira in objavlja v javnem imeniku vsako uro, razen v primeru tehničnih težav, ki so izven kontrole certifikacijskega organa.

Dostop do javnega imenika je mogoč preko javnega spletnega omrežja, na naslovu, navedenem v podaljšku CRL distribucijske točke v kvalificiranem potrdilu za elektronski podpis.

4.9.3 Reprodukcija imenika kvalificiranih potrdil za elektronski podpis na različnih spletnih mestih

V skladu z [DPCM] certifikacijski organ kopira imenik potrdil na več spletnih mest, z zagotavljanjem konsistentnosti in integritete kopij.

Za več podrobnosti glejte odstavek **Error! Reference source not found.**3.

4.10 Postopki varstva osebnih podatkov

Podatki, ki jih v zvezi z Imetnikom pridobi certifikacijski organ med nudenjem storitev kvalificiranih potrdil za elektronski podpis, se štejejo, razen, če je bilo pridobljeno pisno soglasje Imetnika, za zaupne in ne bodo objavljeni, z izjemo podatkov, ki so izrecno javni (npr. javni ključ, datum preklica kvalificiranega potrdila za elektronski podpis). Na podlagi Uporabniškega priročnika za elektronski podpis «withSIGN« certifikacijski organ ne obdeluje »posebne kategorije osebnih podatkov«, kot so opredeljeni v Uredbi GDPR.

Aktivnosti glede identifikacije in zaščite podatkov se izvajajo v skladu z nacionalno zakonodajo mednarodne Banke, ki izvaja dejavnost registracijskega organa. V razjasnitev, trajanje hrambe potrdil in z njimi povezanih dokumentov in podatkov je opredeljeno v italijanski zakonodaji, tako da je obdobje hrambe skladno z italijansko zakonodajo.

Predhodno omenjene osebne podatke certifikacijski organ obdeluje v skladu z Uredbo GDPR.

4.11 Postopek za urejanje kontrolnega dnevnika

Certifikacijski organ v kontrolni dnevnik bodisi ročno bodisi avtomatsko beleži dogodke, v skladu s členom 36 [DPCM]. Še zlasti se beleži naslednje:

- izdaja kvalificiranih potrdil za elektronski podpis,
- preklic kvalificiranih potrdil za elektronski podpis, z navedbo datuma in ure objave CRL,
- začetek in konec delovne seje sistemov, ki se uporabljajo za kreiranje kvalificiranih potrdil za elektronski podpis,
- personalizacija naprav za podpisovanje,
- vstop in izstop iz varnih prostorov certifikacijskega sistema.

Certifikacijski organ vodi kontrolni dnevnik v skladu s členom 41 (2) [DPCM].

4.12 Postopek vodenja varnostnih kopij

Certifikacijski organ je pripravil in izvaja načrt zagotavljanja neprekinjenega poslovanja za storitve, nudene v skladu s tem Uporabniškim priročnikom za elektronski podpis #withSIGN na daljavo, glavne aktivnosti, ki se izvajajo v skladu z ustreznimi postopki, so opisane v nadaljevanju.

4.12.1 Postopek varnostnega kopiranja

Varnostne kopije se kreirajo dnevno za podatke, aplikacije, kontrolne dnevnike in druge datoteke, ki so potrebne za popolno obnovo kritičnih procesov upravljavskega sistema za kvalificirana potrdila za elektronski podpis. Glede teh procesov se varnostne kopije kreirajo na daljavo in jih nadzira poseben centraliziran sistem, ki izpolnjuje naslednje zahteve:

- čim manjša potreba po posegu ljudi in vstopanju v tehnične prostore,
- poenostavljen razpored varnostnega kopiranja in pregledovanja,
- povečanje zanesljivosti varnostnega kopiranja.

4.13 Postopki v zvezi z nesrečami in katastrofami

Splošen pregled teh postopkov je naveden v nadaljevanju.

4.13.1 Izpad računalnikov

Računalniki, ki se uporabljajo za nudenje storitev kvalificiranih potrdil za elektronski podpis, so predmet vzdrževalne pogodbe, s katero je v primeru izpada ponovno delovanje računalnikov zagotovljeno v 24 (štiriindvajsetih) urah.

4.13.2 Napake programske opreme

V primeru napak (nedelovanja ali okvar) programov ali podatkov, ki jih ni mogoče obnoviti na drug način, se le-ti obnovijo iz shranjenih varnostnih kopij.

4.13.3 Nedelovanje naprave certifikacijskega organa za podpisovanje

V primeru nedelovanja naprave certifikacijskega organa za podpisovanje se zasebni ključ ponovno vzpostavi na novi napravi za podpisovanje, začenši s segmenti predhodno kreiranih ključev, po posebnem postopku, ki zahteva skupno intervencijo več delavcev. Segmenti ključa se ohranijo v šifrirani obliki in v različnih vsebnikih, ki jih nadzirajo različni upravljavci.

Opomba: ključni segmenti ne predstavljajo »kopije« certifikacijskega ključa ([DPCM]) in se lahko uporabijo zgolj za obnovo celotnega ključa v skladu z zgoraj opisanim postopkom.

Če obnova certifikacijskega ključa ni mogoča, se upošteva postopek glede napak certifikacijskega ključa (glejte naslednji odstavek).

4.13.4 Napake certifikacijskega ključa

V primeru napak v zvezi z zaupnostjo zasebnega certifikacijskega ključa, bo certifikacijski organ:

- preklical potrdilo, ki se nanaša na zasebni ključ z napako,
- o preklicu AgID obvestil v roku 24 (štiriindvajsetih) ur od preklica,
- obvestil Imetnike vseh kvalificiranih potrdil za elektronski podpis z zasebnim ključem, ki pripada paru z napako,
- preklical vsa kvalificirana potrdila za elektronski podpis, podpisana s ključem z napako,

- izdal nova kvalificirana potrdila za elektronski podpis z uporabo novega zasebnega ključa.

4.13.5 Nerazpoložljivost glavnih prostorov

Če prostori, zgradba ali celoten sistem niso razpoložljivi, zaradi kakršnekoli katastrofe (požar, poplava, vdor ...), se aktivira načrt obnove po katastrofi, ta načrt velja za vsa operativna sredstva banke Intesa Sanpaolo in sredstva tretje osebe, ki nudi storitve časovnih žigov.

5. PRENEHANJE NUDENJA STORITEV KVALIFICIRANIH POTRDIL ZA ELEKTRONSKI PODPIS

5.1 Podrobnosti prenehanja nudenja storitev kvalificiranih potrdil za elektronski podpis

V primeru prenehanja nudenja storitev kvalificiranega ponudnika storitev zaupanja, se to sporoči AgID vsaj 60 (šestdeset) dni vnaprej, z navedbo novega certifikacijskega organa, če je bil določen nadomestni certifikacijski organ, ter upravljavca registra potrdil in spremljajoče dokumentacije.
Hkrati s sporočilom AgID se o prenehanju dejavnosti obvesti tudi vse Imetnike.

Če nadomestni certifikacijski organ ni bil določen, se v sporočilu jasno navede, da se vsa kvalificirana potrdila za elektronski podpis, ki na dan prenehanja nudenja storitve še niso potekla, prekličejo. Kvalificirana potrdila za elektronski podpis se ob času preklica vključijo na seznam preklicev.

Za več podrobnosti glede prenehanja nudenja storitve glejte načrt prenehanja, ki ga ja pripravila Intesa Sanpaolo.

6. UPRAVLJANJE ČASOVNIH SKLICEV

6.1 Storitev časovnih žigov

To poglavje se sklicuje na člen 40 (3), črka p, [DPCM].

Certifikacijski organ zagotavlja skladnost storitev časovnih žigov z [DPCM], z uporabo storitev, ki jih nudi certifikacijski organ, ki izpolnjuje zahteve za delovanje v državah, kjer se nahajajo Banke. Za opis postopkov v zvezi s podajanjem zahtevkov za izdajo časovnega žiga in njegovo pridobitvijo, v skladu z veljavno zakonodajo in predpisi, glejte Uporabniški priročnik ponudnika kvalificiranih storitev zaupanja.

6.2 Natančnost časovnega žiga

Upravljavski sistem za časovne žige uro pridobi iz radijskega sprejemnika, ki je sinhroniziran s signalom, ki ga oddaja Elettrotecnico Nazionale (IEN) »Galileo Ferraris«.

Ob kreiranju časovnega žiga strežnik TSA pridobi datum in uro iz sistemske ure, ki je poravnana z natančnim časom UTC (koordiniran univerzalni čas), s sinhronizacijo signala, ki ga pridobi zunanji sprejemnik, ki določi kakovost signala iz mreže GPS satelitov. Tako pridobljen časovni signal je skladen z mejami natančnosti, ki jo zahtevajo veljavna zakonodaja in predpisi.

7. POSTOPEK PREVERITVE DIGITALNEGA PODPISA

To poglavje se sklicuje na člen 40 (3), črka r, [DPCM].

7.1 Preveritev

V »Mojih dokumentih« v digitalnih kanalih Banke si lahko Imetnik ogleda svoje digitalno podpisane dokumente. Dokumenti so shranjeni v formatu PDF ter so, odvisno od digitalnega kanala (spletna ali mobilna), ki ga izbere Imetnik, vedno na voljo preko izbranega digitalnega kanala , ki Imetniku omogoča preveritev digitalnega podpisa.

Kot je opredeljeno v členu 42 (2) [DPCM], so sistemi za preverjanje, ki so na voljo Imetniku, združljivi z dokumenti, podpisanimi z elektronskim podpisom, ki ga izda certifikacijski organ.
Imetnik lahko digitalno podpisane dokumente prejme tudi po elektronski pošti.

7.2 Format dokumentov

Dokumenti, ki so predloženi imetniku preko neposrednih poti Bank, so skladni z veljavno zakonodajo in predpisi, še zlasti dokumenti v elektronski obliki ne smejo vsebovati »*makrojev, izvršljivih kod ali drugih elementov, ki lahko aktivirajo funkcije, ki lahko spremenijo, dokumente, navedbe ali podatke, ki se tam nahajajo*«.

7.3 Opozorila glede vpogleda v CRL

Pri vpogledu v CRL mora Imetnik in Pravna oseba upoštevati čas, ki je tehnično potreben za posodabljanje podatkov, vsebovanih v CRL.

Zlasti je tehnični čas potreben, ko Imetnik, Pravna oseba, registracijski organ ali certifikacijski organ namerava preklicati ali ponovno aktivirati kvalificirano potrdilo za elektronski podpis, kot tudi ko certifikacijski organ izvaja tehnične/administrativne postopke v zvezi z zahtevki za preklic in s tem povezano posodobitvijo CRL.

Ob podpisu dokumenta z uporabo kvalificiranega potrdila za elektronski podpis se preveri CRL za zagotovitev, da uporabljeno kvalificirano potrdilo za elektronski podpis ni bilo preklicano.

8. OPERATIVNI POSTOPKI ZA KREIRANJE ELEKTRONSKIH PODPISOV

To poglavje se sklicuje na člen 40 (3), črka s, [DPCM].

Storitev ne vključuje dobavo aplikacije za podpis za namestitev na napravi Imetnika (osebni računalnik, pameten telefon ...), vse funkcije, ki Imetniku omogočajo podpis enega ali več elektronskih dokumentov, se neposredno vključijo v poseben razdelek pogodbe o uporabi elektronskih bančnih storitev in/ali Pogodbe o upravljanju storitev s kvalificiranimi potrdili za elektronski podpis fizičnih oseb , sklenjene z Banko.

Elektronski podpisi, kreirani z digitalno bančno storitvijo, izpolnjujejo zahteve, predvidene za algoritme za podpis v členu 4 (2) [DPCM].