PRIVREDNA BANKA ZAGREB

Operativni priručnik za uslugu udaljenog kvalificiranog elektroničkog potpisa (#withSIGN)

SADRŽAJ

VERZIJE OPERATIVNOG PRIRUČNIKA ZA USLUGU UDALJENOG ELEKTRONIČKOG POTPISA

Verzija	Datum izdavanja	Opis promjene
01	24.06.2020	Prva verzija
02	21.03.2021	Ažurirana verzija

1. OPĆE INFORMACIJE

1.1 Pregled

Ovaj Operativni priručnik za uslugu udaljenog elektroničkog potpisa (#withSIGN)" (sukladno definiciji u nastavku), izrađen na temelju Operativnog priručnika za uslugu udaljenog elektroničkog potpisa (pod oznakom: ISP-SCD-04-2018-01), za cilj ima regulirati kvalificirane certifikate za usluge elektroničkog potpisa koje Intesa Sanpaolo S.p.A. sukladno Zakonodavnoj uredbi 82/2005 (Zakon o digitalnoj upravi) s naknadnim izmjenama i dopunama te važećim nacionalnim i Europskim zakonima i propisima pruža Korisniku (sukladno definiciji u nastavku) Međunarodne banke društva kćeri (sukladno definiciji u nastavku) u vezi s višekanalnim uslugama (odnosno pristupanja Korisnika uslugama koje Međunarodne banke društva kćeri pružaju putem daljinskih kanala i poslovnice/ organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom).

Operativni priručnik za uslugu udaljenog elektroničkog potpisa također je povezan s tehničkim pravilima za primjenu zakonskog okvira za elektronički potpis sadržanog u uredbi DPCM od 22. veljače 2013. U slučaju izmjena zakona, ovaj se Operativni priručnik za uslugu udaljenog elektroničkog potpisa mijenja sukladno istima.

1.2 Definicije i tumačenje

Sljedeći pojmovi korišteni u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa(#withSIGN) imaju sljedeća značenja:

„**Podnositelj zahtjeva**": osoba koja traži izdavanje kvalificiranog certifikata za elektronički potpis; za fizičke osobe, Podnositelj zahtjeva naziva se Nositeljem; za Poslovnog subjekta, Podnositelj zahtjeva uvijek je zakonski zastupnik Poslovnog subjekta (Poslovni subjekt može imati više zakonskih zastupnika);

„**Poslovnica**": mjesto na kojem se obavlja posao između klijenta i Banke, uključujući sve prostorije, urede i lokacije Banke, organizacijski dio Banke nadležan za vođenje poslovnog odnosa s klijentom;

„**Certifikacijski autoritet**": davatelj usluga povjerenja ovlašten za izdavanje kvalificiranih certifikata za elektronički potpis putem certifikacijskog postupka usklađenog s međunarodnim normama i europskim i nacionalnim zakonima i propisima. U smislu ovog Operativnog priručnika za uslugu udaljenog elektroničkog potpisa, Certifikacijski autoritet je Intesa Sanpaolo S.p.A.

„Poslovni subjekt": nepotrošač, tj. pravna ili fizička osoba koja djeluje u okviru svoje gospodarske djelatnosti ili slobodnog zanimanja, koji s Bankom potpisuje ugovor o usluzi digitalnog bankarstva i ovlašćuje Podnositelja zahtjeva / Nositelja za korištenje kvalificiranog certifikata za elektronički potpis koji je izdan u njegovo ime;

„**Korisnik**": fizička osoba ili krajnji korisnik poslovnog subjekta, koja je sklopila s Privrednom bankom Zagreb d.d. ugovor o usluzi certificiranja;

„**Digitalna akvizicija**": kanal za provođenje postupka digitalne akvizicije putem video identifikacije koju obavlja operater Banke i osobnog dokumenta klijenta;

„**Međunarodne banke društva kćeri**": bilo koja međunarodna banka društvo kćer iz grupacije Intesa Sanpaolo;

„**Nositelj**": Korisnik kome je izdan kvalificirani certifikat za elektronički potpis; Nositelj je ovlašten upotrebljavati certifikat za elektroničko potpisivanje elektroničkih dokumenata, uz istovremeno osiguravanje autentičnosti porijekla tih elektroničkih dokumenata i integriteta njihovog sadržaja uz poštivanje ograničenja predviđenih ugovorom o pružanju usluga certificiranja Banke;

„**Intesa Sanpaolo**": Intesa Sanpaolo S.p.A., izdavatelj kvalificiranih certifikata za elektronički potpis;

„Jednokratna lozinka (OTP)": lozinka valjana samo za jednu transakciju koja se generira i stavlja na raspolaganje

Nositelju neposredno prije izvođenja radnje elektroničkog potpisivanja. OTP se šalje klijentu putem SMS poruke ako su korišteni kanali digitalne akvizicije ili poslovnice. OTP se generira s pomoću TOKENA u okviru usluga daljinskog digitalnog bankarstva;

„Privredna banka Zagreb d.d.": banka društvo kćer iz grupe Intesa Sanpaolo;

„**Registracijski autoritet subjekt**": subjekt uglavnom zadužen za i) identificiranje Podnositelja zahtjeva i sklapanje ugovora s Podnositeljima zahtjeva uz jamčenje točnosti njihovog identiteta, ii) davanje Podnositeljima zahtjeva svih informacija o kvalificiranim certifikatima za elektronički potpis i ograničenjima njihove uporabe, iii) sklapanje ugovora s Podnositeljima zahtjeva u ime društva Intesa Sanpaolo i iv) podnošenje zahtjeva za opoziv i suspenziju navedenih certifikata društvu Intesa Sanpaolo. U smislu ovog Operativnog priručnika za uslugu udaljenog elektroničkog potpisa, Registracijski autoritet je bilo koja Međunarodna banka društvo kćer društva Intesa Sanpaolo S.p.A. koja je s društvom Intesa Sanpaolo S.p.A. sklopila ugovor o kvalificiranim certifikatima za elektronički potpis;

- „**Operativni priručnik za uslugu udaljenog elektroničkog potpisa (#withSIGN)**": ovaj dokument sa svim naknadnim izmjenama i dopunama.
- „**Banka**": bilo koja Međunarodna banka društvo kćer iz grupacije Intesa Sanpaolo, a u ovom dokumentu pojam Banka odnosi se na Privrednu banku Zagreb d.d.
- „**TOKEN**": sigurni autentikacijski sustavi osiguravaju snažnu provjeru autentičnosti (SCA); upotrebljava se za generiranje OTP-a (jednokratne lozinke) nakon provjere PIN-a
- **„Privatni ključ":** znači rezervirani element para asimetričnih ključeva koji na siguran način pohranjuje Davatelj usluga certifikacije na odgovarajući potpisni uređaj.
- **„Javni ključ":** znači element para asimetričnih ključeva s pomoću kojeg se izvodi autentikacija elektroničkog potpisa.

1.2.1 Reference na zakonske odredbe

[Dlgs 82/2005]	Zakonodavna uredba br. 82 od 7. ožujka 2005., objavljena u Službenom listu br. 112 od 16. svibnja 2005. – Redovna dopuna br. 93 „Zakona o digitalnoj upravi" izmijenjenog Zakonodavnom uredbom br. 217 od 13. prosinca 2017. objavljenom u Službenom listu br. 9 iz siječnja 2018.
[DPCM]	Premijerova uredba od 22 veljače 2013. – Tehnička pravila za izradu, primjenu i verifikaciju naprednih, kvalificiranih i digitalnih elektroničkih potpisa temeljem čl. 20. (3), 24. (4), 28. (3), 32. (3) t. b), 35. (2), 36. (2) i 71.
[CNIPA/CR/48]	CNIPA/CR/ 48 Okružnica br. 48 od 6. rujna 2005. (objavljena u Službenom listu br. 213 od 13. rujna 2005.), Postupak podnošenja zahtjeva za uvrštenje na javnu listu davatelja usluga certificiranja u skladu s čl. 28. (1) Predsjedničke uredbe br. 445 od 28. prosinca 2000.
Uredba (EU) br. 910/2014 –eIDAS	Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.
Uredba (EU) br. 679/2016 – GDPR	Uredba (EU) br. 679/2016 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).
Rasprava AgID-a br. 121/2019	Smjernice koje sadrže tehnička pravila i preporuke za generiranje kvalificiranih elektroničkih certifikata, kvalificiranog elektroničkog potpisa i pečata i kvalificirane elektroničke provjere vremena

1.3 Reference na norme

[LDAP2] Zeilenga, „Lightweight Directory Access Protocol version 2“, Internet RFC 3494, ožujak 2003.
[PKCS7] B. Kaliski, „PKCS#7: Cryptographic Message Syntax Version 1.5“, Internet RFC 2315, ožujak 1998.
[PKCS10] B. Kaliski, „PKCS#10: Certification Request Syntax - Version 1.7“, Internet RFC 2986, studeni 2000.
[SHA1] ISO/IEC 10118-3:2018, „Informacijska tehnologija – Sigurnosne tehnike – Hash-funkcije – 3. dio: Namjenske hash-funkcije“, 2018.
[SHA-256] ISO/IEC 10118-3:2018, „Informacijska tehnologija – Sigurnosne tehnike – Hash-funkcije – 3. dio: Namjenske hash-funkcije“.
[X500] ISO/IEC 9594-1:2008, ISO/IEC 9594-2:2008 „Informacijska tehnologija — Međusobno povezivanje otvorenih sustava — Imenik: Pregled koncepata, modela i usluga“.
[X509] ISO/IEC 9594-8:2008 „Informacijska tehnologija — Međusobno povezivanje otvorenih sustava — Imenik: Okviri certifikata javnog ključa i atributnog certifikata“.
[RFC3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu.
[RFC 3778] The application PDF Taft, Pravetz, Zilles, Masinter, svibanj 2004.

1.4 Kratice

Sljedeći se pojmovi korišteni u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa krate na sljedeći način:

AgID	Agencija za digitalnu Italiju,
CRL	Lista opozvanih certifikata
CPS	Pravilnik o postupcima pružanja usluga izdavanja certifikata
DBMS	Sustav upravljanja bazom podataka
DN	Razlikovno ime
DNS	Sustav domenskih imena
DPR	Predsjednička uredba
HSM	Hardverski sigurnosni modul
HTTP	HyperText Transfer Protocol
ITSEC	Kriteriji vrednovanja sigurnosti informatičke tehnologije
LDAP	Lightweight Directory Access Protocol
NEI	Nacionalni elektrotehnički institut „Galileo Ferraris“ (na talijanskom: „Istituto Elettrotecnico Nazionale“)
OTP	Jednokratna lozinka
PDF	Prenosivi format dokumenta
PIN	Osobni identifikacijski broj
PKCS	Norma kriptografije javnog ključa
RDS	Udaljeni elektronički potpis
RFC	Zahtjev za očitovanje
RSA	Rivest-Shamir-Adleman
SHA-1	Sigurna hash-funkcija 1
SHA-2	Sigurna hash-funkcija 2
SSL	Secure Sockets Layer
URL	Jedinstveni lokator resursa

2. UVOD

Elektronički potpis temelji se na asimetričnim ključevima, jednom javnom i jednom privatnom, koji jednom ili više primatelja jamče autentičnost podrijetla elektronički potpisanih elektroničkih dokumenata i cjelovitost njihovog sadržaja, a ti primatelji mogu verificirati valjanost.

Novim se odredbama uvedenima čl. 8. [DPCM-a] Certifikacijskom autoritetu omogućuje pohrana privatnih ključeva Nositelja (odnosno ključeva koji se upotrebljavaju za izradu elektroničkog potpisa) na posebnim sigurnosnim uređajima (odnosno HSM-ima), a da se pritom korištenje ključeva odobrava isključivo Nositelju, sukladno čl. 11. (2) [DPCM-a].

Tako korištenje elektroničkog potpisa više nije uvjetovano Nositeljevim posjedovanjem kompleta za elektronički potpis (npr. pametne kartice, posebnog čitača i potrebnog softvera), a certifikacijski i registracijski autoriteti mogu pružati korisnicima usluge elektroničkog potpisa putem izravnih kanala (internetskih i mobilnih).

Nositelj može pokrenuti postupak elektroničkog potpisa putem OTP-a (na certificiranom mobilnom broju koji je evidentiran prilikom ugovaranja usluge daljinskog bankarstva, generiranog s pomoću TOKENA unošenjem PIN-a) uz zajamčenu isključivu kontrolu Nositelja. Ako se obavlja u poslovnici/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom, postupak se može pokrenuti i putem čitača kartica (odnosno Nositelj može obaviti prvi korak skeniranjem svoje debitne kartice s pomoću čitača kartica u poslovnici).

U ovom su Operativnom priručniku za uslugu udaljenog elektroničkog potpisa objašnjeni sljedeći postupci:

- postupci generiranja ključa za potpis i upravljanja u okviru usluge udaljenog elektroničkog potpisa koje nudi Intesa Sanpaolo;
- postupak aktiviranja udaljenog elektroničkog potpisa i mehanizama snažne autentikacije u Banci na temelju postupka autentikacije kojeg definiraju Međunarodne banke društva kćeri
- uloga Certifikacijskog autoriteta i Registracijskog autoriteta u skladu s primjenjivim zakonima i propisima;

Operativni priručnik za uslugu udaljenog elektroničkog potpisa(pod oznakom: ISP-SCD-04-2018-01) primjenjuje se u svim međunarodnim bankama Grupe Intesa Sanpaolo u okviru Sektora međunarodnih banaka društava kćeri. Ovaj Operativni priručnik za uslugu udaljenog elektroničkog potpisa (#withSIGN) primjenjuje se u Privrednoj banci Zagreb d.d. te je sačinjen na temelju Operativnom priručniku za uslugu udaljenog elektroničkog potpisa (pod oznakom: ISP-SCD-04-2018-01)

Sljedeće se poglavlje odnosi na zahtjeve propisane čl. 40 (3) a, b i c [DPCM-a].

2.1 Identifikacijski podaci Certifikacijskog autoriteta

Uslugu certificiranja pruža sljedeći subjekt:

Naziv:	**Intesa Sanpaolo S.p.A.**
Sjedište:	**Piazza San Carlo, 156 10121 Torino**
Osoba po zakonu ovlaštena za zastupanje:	**Carlo Messina, glavni direktor i predsjednik uprave**
Matični br. u Registru trgovačkih društava Torina:	**Gospodarsko-upravni registar (REA) br. 00799960158**
PDV ID br.:	**10810700152**
Telefon (centrala):	**(+39) 011 555 1**
ISO identifikacijska oznaka objekta (OID):	**1.3.6.1.4.1.20052**
Glavna web-lokacija (informacije):	**www.intesasanpaolo.com**
Web-lokacija za uslugu izdavanja digitalnih certifikata:	**ca.intesasanpaolo.com**

2.2 Oznaka Operativnog priručnika za uslugu udaljenog elektroničkog potpisa

Operativni priručnik za uslugu udaljenog elektroničkog potpisa označen je oznakom dokumenta ISP-SCD-04-2018-01 i objavljena je na web-lokaciji Certifikacijskog autoriteta pa je stoga dostupna putem interneta.

Važeća verzija Operativnog priručnika za uslugu udaljenog elektroničkog potpis dostupna je u elektroničkom formatu:

- na web-lokaciji Certifikacijskog autoriteta (https://ca.intesasanpaolo.com/);
- na AgID-ovoj web-lokaciji;

Ovaj Operativni priručnik za uslugu udaljenog elektroničkog potpisa (#withSign) dostupan je u elektroničkom formatu:

- na web-lokaciji internetskog bankarstva Banke

te je sačinjen na temelju Operativnog priručnika za uslugu udaljenog elektroničkog potpisa označen je oznakom dokumenta ISP-SCD-04-2018-01.

U slučaju odstupanja, uvijek je mjerodavan Operativni priručnik za uslugu udaljenog elektroničkog potpisa objavljen na AgID-ovoj web-lokaciji.

2.3 Osoba odgovorna za Operativni priručnik za uslugu udaljenog elektroničkog potpisa

Osoba odgovorna za Operativni priručnik za uslugu udaljenog elektroničkog potpis:

Ezio Barbero
Intesa Sanpaolo S.p.A.

3. OPĆE ODREDBE

3.1 Obveze Registracijskog autoriteta, Certifikacijskog autoriteta i Nositelja

3.1.1 Obveze Certifikacijskog autoriteta i Registracijskog autoriteta

Certifikacijski autoritet dužan je postupati u skladu s odredbama uredbe DLgs 82/2005, čl. 32., kojima se usvajaju sve organizacijske i tehničke mjere sprječavanja nastanka štete kod trećih osoba.

Certifikacijski autoritet koji sukladno čl. 27. [DLgs 82/2005] izdaje kvalificirane certifikate za elektronički potpis usto je dužan:

- uredno identificirati Podnositelja zahtjeva (i Nositelja, ako je različit od Podnositelja zahtjeva), a taj posao obavlja Registracijski autoritet u skladu s nacionalnim pravom;
- jasno i potpuno obavijestiti Podnositelja zahtjeva (i Nositelja, ako je različit od Podnositelja zahtjeva) o svojstvima kvalificiranih certifikata za elektronički potpis i ograničenjima u korištenju istih; taj posao obavlja Registracijski autoritet prije sklapanja ugovora o pružanju usluga certificiranja;
- temeljem uputa koje bez odlaganja isporučuje Registracijski autoritet pristupiti pravovremenom opozivu kvalificiranih certifikata za elektronički potpis i potrebnoj objavi;
- usvojiti sigurnosne mjere za obradu osobnih podataka u skladu s važećim zakonima i propisima; tu obvezu izvršavaju Registracijski autoritet i Certifikacijski autoritet;
- izdavati kvalificirane certifikate za elektronički potpis na način propisan [DPCM-om] u skladu s [uredbom GDPR] i sa svim naknadnim izmjenama i dopunama;

- pridržavati se tehničkih pravila iz [DPCM-a] i čl. 71. uredbe DLgs 82/2005;
- voditi računa da sigurni uređaj za generiranje potpisa ima svojstva i ispunjava sigurnosne zahtjeve iz čl. 35. uredbe [Dlgs 82/2005] i čl. 11. uredbe [DPCM];
- čuvati evidencije, uključujući evidencije u elektroničkom formatu, svih informacija u vezi s kvalificiranim certifikatima za elektronički potpis u razdoblju od najmanje 20 (dvadeset) godina kako bi se mogao pružiti dokaz o certifikaciji u eventualnom sudskom postupku;
- čuvati evidencije, uključujući evidencije u elektroničkom formatu, svih dokumenata koje je Nositelj potpisao tijekom postupka izdavanja kvalificiranih certifikata za elektronički potpis u razdoblju od najmanje 20 (dvadeset) godina; taj posao obavlja Registracijski autoritet;
- ne izvoziti privatne ključeve Nositelja iz HSM-a ako su ključevi generirani i u uporabi;
- Certifikacijski autoritet i Registracijski autoritet stalno će ažurirati Operativni priručnik za uslugu udaljenog elektroničkog potpisa i ovaj Operativni priručnik za uslugu udaljenog elektroničkog potpisa (#withSIGN) a Registracijski autoritet pravovremeno će obavještavati Korisnika o izmjenama.

3.1.2 Obveze Nositelja

Nositelj je dužan osigurati čuvanje svih informacija kojima se omogućuje korištenje privatnog ključa i usvojiti sve tehničke i organizacijske mjere za sprječavanje nastanka štete trećim osobama. Nositelj je usto dužan osobno koristiti podatke kojima se omogućuje izrada elektroničkog potpisa (čl. 8. (5) [DPCM-a]).

Nositelj je dužan pridržavati se [DPCM-a]; posebice je dužan:

- zatražiti kvalificirane certifikate za elektronički potpis u skladu s postupcima utvrđenima u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa (#withSIGN);
- čuvati šifre (šifru generiranu s pomoću TOKENA i OTP primljen putem SMS poruke) koje su nužne za korištenje kvalificiranih certifikata za elektronički potpis
- zatražiti opoziv kvalificiranih certifikata za elektronički potpis u skladu s postupcima utvrđenima u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa(#withSIGN);
- bez odlaganja obavijestiti Registracijski autoritet o svim promjenama informacija dostavljenih Registracijskom autoritetu tijekom postupka registracije (osobni podaci, adresa i sl.);
- ne koristiti privatni ključ u bilo koje svrhe osim svrha predviđenih ograničenjima korištenja utvrđenim u kvalificiranim certifikatima za elektronički potpis, ugovoru o usluzi digitalnog bankarstva i ugovoru o pružanju usluga certificiranja;
- osigurati ispravnost, istinitost i cjelovitost podataka osobi koja vrši identifikaciju, prilikom ugovaranja usluge certificiranja;
- koristiti certifikat samo za metode utvrđene u ovom Operativnom priručniku i propisane važećim nacionalnim i međunarodnim zakonima.

3.1.3 Obveze Poslovnog subjekta (ako postoji)

U slučaju da Nositelj koristi kvalificirani certifikat za elektronički potpis u ime Poslovnog subjekta, isti će Poslovni subjekt preuzeti obveze i osigurati odgovarajuće ovlaštenje za Nositelja kako bi Nositelj koristio kvalificirani certifikat za elektronički potpis u njegovo ime.

Poslovni subjekt dužan je pridržavati se [DPCM-a]; posebice je dužan:

- ovlastiti Nositelja za posjedovanje kvalificiranog certifikata za elektronički potpis u skladu s postupcima utvrđenima u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa(#withSIGN);

- zatražiti opoziv kvalificiranog certifikata za elektronički potpis u skladu s postupcima utvrđenima u ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa(#withSIGN);
- bez odlaganja obavijestiti Registracijski autoritet o svim promjenama informacija dostavljenih Registracijskom autoritetu tijekom postupka registracije (osobni podaci Nositelja, smrt Nositelja, nemogućnost poslovanja Nositelja, podaci Poslovnog subjekta i sl.);
- koristiti certifikat samo za metode utvrđene u ovom Operativnom priručniku i propisane važećim nacionalnim i međunarodnim zakonima.

3.1.4 Obveze subjekta potrebne za verifikaciju potpisa

Subjekti zaduženi za verifikaciju elektroničkog potpisa generiranog s pomoću certifikacijskih ključeva društva Intesa Sanpaolo dužni su:

- verificirati razdoblje valjanosti certifikata (u skladu s važećim propisom);
- provjeriti popis opozvanih kvalificiranih certifikata za elektronički potpis radi potvrđivanja je li certifikat opozvan u trenutku potpisivanja;
- osigurati u trenutku potpisivanja da se elektronički potpis odnosi na kvalificirani certifikat koji je izdao Certifikacijski autoritet kojeg je prethodno odobrio AgID;
- osigurati da tipologija generiranih ključeva za „pretplatu" (kako je propisano u čl. 5., stavku 4., slovu a [DPCM-a]) i proširenje ključa keyUsage 11 (OID: 2.3.29.15) imaju samo nerepudijacijsku vrijednost (bit 1 postavljen na 1);
- verificirati ograničenja korištenja utvrđena u kvalificiranom certifikatu.

3.2 Ograničenje odgovornosti i odšteta

3.2.1 Ograničenje odgovornosti

Intesa Sanpaolo nije odgovorna za smetnje nastale uslijed Nositeljevog nepridržavanja važećih zakona i propisa, kao i tehničkih/radnih specifikacija sadržanih u ugovoru o usluzi digitalnog bankarstva sklopljenom između Nositelja i Banke ili pripadajućim dokumentima.

Intesa Sanpaolo nije odgovorna za štete nastale uslijed korištenja izvan ograničenja predviđenih kvalificiranim certifikatima za elektronički potpis i/ili ugovorom o usluzi digitalnog bankarstva i/ili ugovorom o pružanju usluga certificiranja.

Ograničenja u korištenju predviđena kvalificiranim certifikatima za elektronički potpis su sljedeća:

„Korištenje je ograničeno na dokumente u vezi s odnosom Nositelja certifikata s društvima iz Grupe Intesa Sanpaolo ili drugim osobama izvan Grupe koje nude usluge na elektroničkim sustavima društava iz Grupe".

Pored navedenog, korištenje kvalificiranih certifikata za elektronički potpis ograničeno je na domenu koja je navedena u ugovoru o pružanju usluga certificiranja.

Daljnja ograničenja koja se odnose na pojedine proizvode ili nacionalni zakon navedena su u Operativnim priručnicima određenih proizvoda.

3.2.2 Odšteta

Sukladno čl. 3.2.1. ovog dokumenta, društvo Intesa Sanpaolo nije odgovorno za štete nastale uslijed neprimjerenog korištenja kvalificiranih certifikata za elektronički potpis.

Međutim, sukladno čl. 15. (1) i) [DPCM-a], društvo Intesa Sanpaolo ugovorilo je posebno osiguranje za pokriće rizika i šteta nastalih u vezi s izdavanjem kvalificiranih certifikata za elektronički potpis.

3.3 Vrijeme dostupnosti

Sve su usluge koje nudi Certifikacijski autoritet (izdavanje i korištenje kvalificiranih certifikata za elektronički potpis i korištenje elektroničkog potpisa) uvijek dostupne putem izravnih kanala (internetskih i mobilnih) i poslovnice/ organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom. Opoziv kvalificiranih certifikata za elektronički potpis bit će dostupan putem poslovnice/organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom.

4. OPERATIVNI ASPEKTI

4.1 Sadržaj kvalificiranih certifikata za elektronički potpis

Sadržaj kvalificiranih certifikata za elektronički potpis koje izdaje Intesa Sanpaolo sukladan je odredbama čl. 28. uredbe [Dlgs 82/2005]

specifikaciji norme ITU-T X.509 v3 (ISO/IEC 9594-8:2005) i Europskim pravilima ETSI EN 319 411 ed ETSI EN 319 412 (gdje je to primjenjivo).

Prema Raspravi AgID-a br. 121/2019, utvrđuje se da kvalificirane certifikate izdaje Intesa Sanpaolo u skladu s preporukama navedenim u poglavlju 4. navedene odredbe s izuzetkom sljedećih polja:

- SubjectDN: serialNumber (OID 2.5.4.5): za jedinstvenu šifru povezanu s Nositeljem koristi se konvencija o određivanju naziva koja se razlikuje od konvencije navedene u preporukama iz poglavlja 4. Rasprave AgID-a br. 121/2019
- SubjectDN: organizationName (OID 2.5.4.10): ako je vlasnik samo klijent organizacije, polje organizationName i dalje se koristi, ali prošireno nizom „nije prisutan".

Budući da se ne primjenjuju sve preporuke iz Rasprave AgID-a br. 121/2019, certifikati koje izdaje društvo Intesa Sanpaolo ne sadrže šifriranja u polju CertificatePolicies (OID 2.5.29.32) u elementu PolicyIdentifier s vrijednošću AgID (OID 1.3.76.16.6). Kvalificirani certifikati za elektronički potpis ne smiju se objavljivati u javno dostupnim registrima.

Svaki kvalificirani certifikat za elektronički potpis vrijedi 3 (tri) godine.

Udaljeni elektronički potpis ovlašćuje Nositelja i Poslovnog subjekta (ako je primjenjivo) da sklope ugovor s Bankom. Udaljeni elektronički potpis može se koristiti putem svih kanala (uključujući digitalne kanale: poslovnica Banke/ organizacijski dio Banke nadležan za vođenje poslovnog odnosa s klijentom, internetsko bankarstvo i digitalna akvizicija) u skladu s pravovremenom ponudom i mogućnostima Banke. Kvalificirani certifikat za elektronički potpis omogućuje Nositelju korištenje udaljenog elektroničkog potpisa.

4.2 Pravila organizacije djelatnika

Djelatnici zaduženi za pružanje i kontrolu usluge certificiranja organizirani su u skladu s [DPCM-om 2013] što, između ostalog, znači da su im nadležne funkcije predviđene sukladno čl. 38. [DPCM-a].

Djelatnici na nadležnim funkcijama mogu prilikom obavljanja dužnosti koristiti usluge zaposlenika i operatera banaka.

U vezi s Operativnim priručnikom za uslugu udaljenog elektroničkog potpisa (#withSIGN), operateri obavljaju uslugu certificiranja (u smislu registracije ili identifikacije Nositelja) u poslovnicama banaka/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom, izvan centra za obradu podataka društva Intesa Sanpaolo; razmjena informacija između tih operatera i društva Intesa Sanpaolo obavlja se putem sigurnih komunikacijskih kanala.

Poslove registracije obavljaju banke temeljem posebnog ugovora sklopljenog između banke i Intese Sanpaolo.

Operateri banaka obavljaju poslove registracije u skladu s postupcima ugovorenim između banaka i Intese Sanpaolo.

4.3 Postupak generiranja ključeva

Svaki se tip ključa iz čl. 5. (4) [DPCM-a] generira, čuva i koristi unutar sigurnih uređaja sukladnih sigurnosnim zahtjevima propisanim važećim zakonima i propisima.

Svojstva ključeva utvrđena su u [DPCM-u].

4.3.1 Postupak generiranja[1] certifikacijskih ključeva

Generiranje certifikacijskih ključeva izvodi se u skladu s važećim zakonima i propisima, kako slijedi:

- certifikacijske ključeve generiraju zaposlenici koje izričito imenuje Certifikacijski autoritet;
- za svaki par certifikacijskih ključeva generira se poseban kvalificirani certifikat za elektronički potpis, kako je navedeno u poglavlju 4.1, pa se potpisuje odgovarajućim privatnim ključem iz para koji se šalje AgID-u u skladu s postupcima prethodno dogovorenim između Certifikacijskog autoriteta i AgID-a.

4.3.2 Postupak generiranja ključeva za vremenski žig

U pogledu usluge izdavanja vremenskog žiga u odnosu na usluge elektroničkog potpisa koje se pružaju bankama, društvo Intesa Sanpaolo koristi certifikacijski autoritet koji ispunjava potrebne uvjete za rad u državi gdje se Banka nalazi.

4.4 Postupak identifikacije i registracije Korisnika

Izdavanje kvalificiranih certifikata za elektronički potpis vrijedi samo za one koji su kvalificirani kao Korisnik, točnije one koji sklope s Bankom ugovor o pružanju usluga certificiranja.

Kvalificirani certifikati za elektronički potpis Korisnika fizičke osobe sadrže osobne podatke o Nositelju. Kvalificirani certifikati za elektronički potpis krajnjeg korisnika Poslovnog subjekta mogu sadržavati osobne podatke o Nositelju i podatke o Poslovnom subjektu.

Postupak identifikacije i registracije Korisnika provodi Banka u skladu s važećim zakonima i propisima, uključujući, ali ne ograničavajući se na, propise o sprječavanju pranja novca, važeće prilikom zasnivanja ugovornog odnosa s istom.

Za Poslovne subjekte, propis o sprječavanju pranja novca primjenjiv je na Poslovnog subjekta, a ne na Nositelja. U tom se slučaju identifikacija Nositelja izvodi licem u lice.

Identifikacija Nositelja i/ili Podnositelja zahtjeva izvodi se i) osobno, fizičkim prisustvom Korisnika u prostorijama Banke, ili ii) daljinski, primjenom identifikacijskih metoda za koje je utvrđeno da pružaju jednaku sigurnost u pogledu pouzdanosti. Navedene se aktivnosti obavljaju u skladu s propisanim postupkom sprječavanja pranja novca i financiranja terorizma ili licem u lice, što znači sukladno članku 24. 1. (d) Uredbe eIDAS.

4.4.1 Identifikacija i registracija Korisnika

Identifikacija Korisnika izvodi se sukladno unaprijed definiranim postupcima koji se razlikuju ovisno o kanalu Banke.

Identifikacija se vrši uz fizičku prisutnost Korisnika ili daljinskim postupkom. Posebice:

- prilikom identifikacije licem u lice u poslovnici/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom certificira se mobilni broj Korisnika slanjem OTP-a u SMS poruci i zatim se Korisnika traži taj OTP. Korisnik se može identificirati i skeniranjem njegove debitne kartice s pomoću čitača kartica;

[1] Ključevi kojima se koristi Certifikacijski autoritet za izdavanje kvalificiranih certifikata za elektronički potpis na zahtjev Nositelja.

- prilikom internetske identifikacije putem usluga daljinskog digitalnog bankarstva, Korisnik vrši autentikaciju putem Mobilnog i Internetskog s pomoću korisničkog broja za prijavu i OTP-a koji je generiran unošenjem PIN-a u TOKEN sukladno usluzi digitalnog bankarstva i dodatnog OTP-a koji Korisnik primi putem SMS poruke koja je poslana na njegov certificirani broj mobilnog telefona;
- prilikom video identifikacije za Digitalnu akviziciju, certificira se broj mobilnog telefona Korisnika slanjem OTP-a putem SMS poruke i zatim se Korisnika traži taj OTP.

Svi postupci identifikacije provode se u skladu s lokalnim propisima o bankarstvu, korištenjem postupka sprječavanja pranja novca i financiranja terorizma ili licem u lice.

Identifikaciju Korisnika obavlja Banka prije upisivanja kvalificiranog certifikata za elektronički potpis.

Nakon uspješne identifikacije, Korisnik može nastaviti s aktiviranjem usluge udaljenog elektroničkog potpisa i potpisivanjem odgovarajućeg ugovora.

4.4.2 Aktivacija usluge udaljenog elektroničkog potpisa i potpisivanje ugovora od strane Podnositelja zahtjeva fizičke osobe

Kako bi aktivirao uslugu udaljenog elektroničkog potpisa i potpisao ugovor o pružanju usluga certificiranja, Podnositelj zahtjeva mora poduzeti sljedeće proceduralne korake na različitim kanalima.

Usluge daljinskog digitalnog bankarstva:

- pristupiti usluzi digitalnog bankarstva koristeći se autentikacijskim postupcima koje je definirala Banka;
- ako je potrebno, potvrditi pravila koja su regulirana ugovorom o pružanju usluga certificiranja;
- ako je potrebno, provjeriti i potvrditi točnost svojih osobnih podataka s ciljem aktiviranja kvalificiranog certifikata za elektronički potpis;
- zatražiti izdavanje i aktivaciju certifikata;
- generirati OTP unošenjem PIN-a u TOKEN, ovisno o korištenoj usluzi digitalnog bankarstva. Navedeni koraci jamče mehanizam snažne autentikacije;
- zaključiti ugovor o pružanju usluga certificiranja, izdati i aktivirati kvalificirane certifikate za elektronički potpis i potpisati ga elektroničkim potpisom unošenjem OTP-a generiranog putem TOKENA s pomoću PIN-a;
- dodatne kontrole zahtijevaju dodatan OTP koji Krajnji korisnik prima putem SMS poruke poslane na njegov certificirani broj mobilnog telefona;
- potpis Banke potvrđuje aktiviranje usluge udaljenog elektroničkog potpisa.

Poslovnice/organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom ili Digitalne akvizicije:

- pristupiti Digitalnoj akviziciji ili osobno posjetiti prostorije Banke;
- ako je potrebno, potvrditi pravila koja su regulirana ugovorom o pružanju usluga certificiranja;
- ako je potrebno, provjeriti i potvrditi točnost svojih osobnih podataka s ciljem aktiviranja kvalificiranog certifikata za elektronički potpis;
- zatražiti izdavanje i aktivaciju certifikata. Ako Korisnik zatraži aktiviranje certifikata putem kanala poslovnice / organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom, prije potpisivanja ugovora o pružanju usluga certificiranja stvorit će se odgovarajući obrazac za podnošenje zahtjeva;
- primiti OTP putem SMS poruke poslane na svoj certificirani broj mobilnog telefona. Korisnik ne treba unijeti sigurnosni PIN u slučaju identifikacije licem u lice i video identifikacije. Podnositelj zahtjeva također može skenirati svoju debitnu karticu u poslovnici radi obavljanja prvog koraka autorizacije s pomoću čitača kartica;
- pročitati ugovor o pružanju usluga certificiranja, preuzeti kvalificirane certifikate za elektronički potpis i potpisati

ga elektroničkim potpisom unošenjem OTP-a. Ugovor o pružanju usluga certificiranja također se može potpisati i vlastoručnim potpisom;

- potpis Banke potvrđuje aktiviranje usluge udaljenog elektroničkog potpisa.

Dodatna dokumentacija koja se odnosi na uslugu udaljenog kvalificiranog potpisa bit će dostupna Korisniku prije sklapanja ugovora o pružanju usluga certificiranja povezanog s uslugama elektroničkog potpisa.

4.4.3 Aktivacija usluge udaljenog elektroničkog potpisa i potpisivanje ugovora od strane Korisnika Poslovnog subjekta

Kako bi aktivirao uslugu udaljenog elektroničkog potpisa i potpisao ugovor o pružanju usluga certificiranja, Podnositelj zahtjeva i Nositelj moraju poduzeti sljedeće proceduralne korake na različitim kanalima.

Kako bi potpisao ugovor o pružanju usluga certificiranja putem usluga daljinskog digitalnog bankarstva, Nositelj (neovisno o tome je li ujedno i Podnositelj zahtjeva) mora obaviti sljedeće proceduralne korake:

- pribaviti odobrenje Poslovnog subjekta ako Nositelj nije ujedno i Poslovni subjekt;
- pristupiti usluzi digitalnog bankarstva koristeći se autentikacijskim postupcima koje je definirala Banka;
- potvrditi pravila koja su regulirana ugovorom o pružanju usluga certificiranja;
- ako je potrebno, provjeriti i potvrditi točnost svojih osobnih podataka s ciljem aktiviranja kvalificiranog certifikata za elektronički potpis;
- zatražiti izdavanje i aktivaciju certifikata;
- generirati OTP unošenjem PIN-a u TOKEN, ovisno o korištenoj usluzi digitalnog bankarstva. Navedeni koraci jamče mehanizam snažne autentikacije;
- pročitati ugovor o usluzi certificiranja, preuzeti kvalificirane certifikate za elektronički potpis i potpisati ga elektroničkim potpisom unošenjem OTP-a generiranog putem TOKENA s pomoću PIN-a. Ugovor o pružanju usluga certificiranja također se može potpisati i vlastoručnim potpisom;
- dodatne kontrole zahtijevaju dodatan OTP koji krajnji korisnik Nositelj prima putem SMS poruke poslane na njegov certificirani broj mobilnog telefona;
- potpis Banke potvrđuje aktiviranje usluge udaljenog elektroničkog potpisa.

Kako bi potpisao ugovor o pružanju usluga certificiranja putem usluga daljinskog digitalnog bankarstva u slučaju kada Podnositelj zahtjeva nije ujedno i Nositelj, Podnositelj zahtjeva mora poduzeti sljedeće proceduralne korake:

- pristupiti usluzi digitalnog bankarstva koristeći se autentikacijskim postupcima koje je definirala Banka;
- potvrditi pravila koja su regulirana ugovorom o pružanju usluga certificiranja;
- generirati OTP unošenjem PIN-a u TOKEN, ovisno o korištenoj usluzi digitalnog bankarstva. Navedeni koraci jamče mehanizam snažne autentikacije;
- pročitati ugovor o usluzi certificiranja i potpisati ga elektroničkim potpisom unošenjem OTP-a generiranog putem TOKENA s pomoću PIN-a;
- dodatne kontrole zahtijevaju dodatan OTP koji Krajnji korisnik prima putem SMS poruke poslane na njegov certificirani broj mobilnog telefona.

Kako bi potpisao ugovor o pružanju usluga certificiranja u poslovnici/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom, Nositelj (neovisno o tome je li ujedno i Podnositelj zahtjeva) mora poduzeti sljedeće proceduralne korake:

- pribaviti odobrenje Poslovnog subjekta ako Nositelj nije ujedno i Poslovni subjekt;
- osobno posjetiti prostorije Banke;

- potvrditi pravila koja su regulirana ugovorom o pružanju usluga certificiranja;
- ako je potrebno, provjeriti i potvrditi točnost svojih osobnih podataka s ciljem aktiviranja kvalificiranog certifikata za elektronički potpis;
- zatražiti izdavanje i aktivaciju certifikata;
- pročitati ugovor o pružanju usluge certificiranja i potpisati ga elektroničkim ili vlastoručnim potpisom;
- U slučaju elektroničkog potpisa:
  - Nositelj prima OTP putem SMS poruke na svoj certificirani broj mobilnog telefona. Nositelj ne treba unijeti sigurnosni PIN u slučaju identifikacije licem u lice;
  - Nositelj upisuje kvalificirani certifikat za elektronički potpis i potpisuje ga elektronički unošenjem OTP-a;
- potpis Banke potvrđuje aktiviranje usluge udaljenog elektroničkog potpisa.

Kako bi potpisao ugovor o pružanju usluga certificiranja u poslovnici/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom u slučaju kada Podnositelj zahtjeva nije ujedno i Nositelj, Podnositelj zahtjeva mora obaviti sljedeće proceduralne korake:

- osobno posjetiti prostorije Banke;
- potvrditi pravila koja reguliraju ugovor o pružanju usluga certificiranja;
- pročitati ugovor o pružanju usluge certificiranja i potpisati ga elektroničkim ili vlastoručnim potpisom.

Dodatna dokumentacija koja se odnosi na uslugu udaljenog elektroničkog potpisa bit će dostupna klijentu prije sklapanja ugovora o pružanju usluga certificiranja povezanog s uslugama elektroničkog potpisa.

U slučaju da se ugovor o pružanju usluga certificiranja u poslovnici/organizacijskom dijelu Banke nadležnom za vođenje poslovnog odnosa s klijentom vlastoručno potpisuje, upis kvalificiranog certifikata za elektronički potpis može se izvršiti putem interneta tj. usluge digitalnog bankarstva Banke. Nositelj tada mora obaviti sljedeće proceduralne korake za aktiviranje usluge udaljenog elektroničkog potpisa:

- pristupiti usluzi digitalnog bankarstva koristeći se autentikacijskim postupcima koje je definirala Banka;
- ako je potrebno, provjeriti i potvrditi točnost svojih osobnih podataka s ciljem aktiviranja kvalificiranog certifikata za elektronički potpis;
- generirati OTP unošenjem PIN-a u TOKEN, ovisno o korištenoj usluzi digitalnog bankarstva. Navedeni koraci jamče mehanizam snažne autorizacije;
- upisati kvalificirani certifikat za elektronički potpis unošenjem OTP-a generiranog putem TOKENA s pomoću PIN-a;
- dodatne kontrole zahtijevaju dodatan OTP koji Krajnji korisnik prima putem SMS poruke poslane na njegov certificirani broj mobilnog telefona.

4.4.4 Izdavanje kvalificiranih certifikata za elektronički potpis

Kvalificirani certifikati za elektronički potpis izdaju se nakon generiranja para ključeva kako je prethodno naznačeno.

Postupak izdavanja kvalificiranih certifikata za elektronički potpis u cijelosti je transparentan Podnositelju zahtjeva koji u ovoj fazi ne ostvaruje interakciju s Certifikacijskim autoritetom.

Sukladno važećim zakonskim propisima, Certifikacijski autoritet dužan je zahtjev za izdavanje kvalificiranog certifikata za elektronički potpis čuvati najmanje 20 (dvadeset) godina od datuma izdavanja svakog kvalificiranog certifikata za elektronički potpis. Elektronički se čuvaju i svi tragovi potrebni kako bi se tijekom vremena dokazalo izvršenje ovog posla.

4.5 Postupak opoziva kvalificiranih certifikata za elektronički potpis

Sukladno [DPCM-u], kvalificirani certifikat za elektronički potpis opoziva se na zahtjev sljedećih strana:

- Nositelja;
- Poslovnog subjekta;
- Certifikacijskog autoriteta;
- Registracijskog autoriteta.

4.5.1 Zahtjev za opoziv koji podnosi Nositelj

Nositelj može podnijeti zahtjev za opoziv kvalificiranog certifikata za elektronički potpis tako da osobno posjeti poslovnicu/organizacijski dio Banke nadležan za vođenje poslovnog odnosa s klijentom. Nakon podnošenja zahtjeva za opoziv pokreće se automatski mehanizam za opoziv kvalificiranog certifikata za elektronički potpis na način koji je transparentan za Nositelja.

U slučaju da Nositelj jednostrano otkaže ugovor o pružanju usluga certificiranja koji je sklopljen s Bankom, Registracijski autoritet dužan je bez odlaganja obavijestiti Certifikacijski autoritet koji pristupa opozivu predmetnog kvalificiranog certifikata za elektronički potpis.

Nakon opoziva, Nositelj više ne može potpisivati dokumente s pomoću ključeva koji su mu prethodno dodijeljeni, a svi dokumenti koje je Nositelj potpisao prije opoziva kvalificiranog certifikata za elektronički potpis i dalje vrijede.

U pogledu valjanosti opoziva certifikata, opoziv je valjan od datuma na koji Banka zaprimi obavijest o opozivu.

4.5.2 Zahtjev za opoziv koji podnosi Poslovni subjekt

Poslovni subjekt može putem poslovnice/organizacijskog dijela Banke nadležnog za vođenje poslovnog odnosa s klijentom podnijeti zahtjev za opoziv kvalificiranog certifikata za elektronički potpis Nositelja usluge udaljenog elektroničkog potpisa u ime istog Poslovnog subjekta.

Nakon podnošenja zahtjeva za opoziv pokreće se automatski mehanizam za opoziv kvalificiranog certifikata za elektronički potpis na način koji je transparentan za Nositelja.

U slučaju da Poslovni subjekt jednostrano otkaže ugovor o pružanju usluga certificiranja koji je sklopljen s Bankom, Registracijski autoritet dužan je bez odlaganja obavijestiti Certifikacijski autoritet koji pristupa opozivu predmetnog kvalificiranog certifikata za elektronički potpis.

Nakon opoziva, Nositelj više ne može potpisivati dokumente s pomoću ključeva koji su mu prethodno dodijeljeni, a svi dokumenti koje je Nositelj potpisao prije opoziva kvalificiranog certifikata za elektronički potpis i dalje vrijede.

U pogledu valjanosti opoziva certifikata, opoziv je valjan od datuma na koji Banka zaprimi obavijest o opozivu.

4.5.3 Opoziv koji je podnio Certifikacijski autoritet ili Registracijski autoritet

Osim u opravdano hitnim slučajevima, Certifikacijski autoritet ili Registracijski autoritet koji namjerava opozvati kvalificirani certifikat za elektronički potpis dužan je unaprijed obavijestiti Nositelja/Poslovnog subjekta uz navođenje obrazloženja opoziva.

Registracijski autoritet dužan je bez odlaganja obavijestiti Certifikacijski autoritet o potrebi za opozivom kvalificiranog certifikata za elektronički potpis.

Certifikacijski autoritet dužan je opozvati certifikat kada:

- to Nositelj izričito zatraži;
- to izričito zatraži Poslovni subjekt u čije je ime Nositelj nabavio certifikat;
- ustanovi da su podaci Nositelja u evidenciji certifikata netočni ili nepotpuni;
- zaprimi službenu obavijest o smrti Nositelja;
- zaprimi službenu obavijest o gubitku poslovne sposobnosti Nositelja;
- Poslovni subjekt prestane postojati;
- dođe do otkaza ugovora o pružanju usluga certificiranja;
- utvrdi da se Nositelj služio netočnim podacima za izdavanje certifikata.

4.5.4 Okončanje postupka opoziva kvalificiranog certifikata za elektronički potpis

Po okončanju postupka opoziva kvalificiranog certifikata za elektronički potpis izrađuje se novi CRL koji se zatim objavljuje u odgovarajućem direktoriju putem internetske veze.

CRL se objavljuje sukladno točki 4.9.2. Nadalje, izvršeni opoziv kvalificiranog certifikata za elektronički potpis bilježi se u kontrolnoj datoteci zapisnika.

4.6 Postupak suspenzije kvalificiranih certifikata za elektronički potpis

Sukladno [DPCM-u], kvalificirani certifikat za elektronički potpis suspendira se na zahtjev sljedećih strana:

- Certifikacijskog autoriteta;
- Registracijskog autoriteta.

Osim u opravdano hitnim slučajevima, Certifikacijski autoritet ili Registracijski autoritet koji namjerava suspendirati kvalificirani certifikat za elektronički potpis dužan je unaprijed obavijestiti Nositelja/Poslovnog subjekta uz navođenje razloga suspenzije.

4.7 Postupak u slučaju gubitka PIN-a i OTP uređaja (TOKENA)

Nositelj se za autentikaciju može koristiti OTP uređajem kao jednom od autentikacijskih metoda

U slučaju gubitka ili krađe OTP uređaja, Nositelj mora postupiti u skladu s odredbama ugovora o usluzi digitalnog bankarstva. Postupak u slučaju gubitka PIN-a istovjetan je postupku u slučaju gubitka OTP uređaja.

4.8 Postupak zamjene ključeva

4.8.1 Zamjena Nositeljevih potpisnih ključeva

Certifikacijski autoritet određuje istek kvalificiranog certifikata za elektronički potpis i razdoblje valjanosti ključeva na temelju duljine ključeva i usluga za koje se ti ključevi koriste u skladu s [DPCM-om].

Razdoblje valjanosti ključeva podudara se s razdobljem valjanosti odgovarajućeg kvalificiranog certifikata za elektronički potpis, a to je 3 (tri) godine.

Zahtjev za izdavanje novog kvalificiranog certifikata za elektronički potpis može se podnijeti isključivo ako je certifikat istekao ili opozvan.

Nositelj nikada ne smije istovremeno imati 2 (dva) aktivna kvalificirana certifikata za elektronički potpis za isti Poslovni subjekt.

4.8.2 Zamjena certifikacijskih ključeva

Zamjenu certifikacijskih ključeva obavlja Certifikacijski autoritet u skladu s važećim zakonima i propisima.

4.9 Upravljanje direktorijem kvalificiranih certifikata za elektronički potpis

4.9.1 Direktorij kvalificiranih certifikata za elektronički potpis

Svi važeći kvalificirani certifikati za elektronički potpis koje je izdao Certifikacijski autoritet pohranjeni su u „registru certifikata".

- Javni direktorij sadrži sljedeće informacije:certifikati za ključeve Certifikacijskog autoriteta;
- certifikati koji se odnose na ugovore o certifikaciji;
- certifikati za AgID-ove potpisne ključeve;
- lista opozvanih kvalificiranih certifikata za elektronički potpis.

Lista opozvanih certifikata za elektronički potpis također se objavljuje putem protokola HTTP http://crl2.ca.intesa-sanpaolo.com/FirmaQualificata/CRL20.crl i

http://crlcl.ca2.intesasanpaolo.com/qc/CRL$$.crl

Certifikacijski autoritet koristi pouzdane sustave za upravljanje direktorijem kvalificiranih certifikata za elektronički potpis i javnim direktorijem, kao i metode kojima osigurava da:

- isključivo ovlaštene osobe mogu unositi podatke i vršiti promjene;
- se može provjeriti autentičnost informacija;
- su certifikati dostupni za javni uvid u mjeri u kojoj to dozvoljava Nositelj;
- je operater svjestan svih događaja koji dovode u pitanje sigurnosne zahtjeve.

4.9.2 Objavljivanje kvalificiranih certifikata za elektronički potpis i CRL-a

Kvalificirani certifikati za elektronički potpis objavljuju se u skladu s postupcima iz čl. 34. [DPCM-a].

CRL se sastavlja i objavljuje u javnom direktoriju svakih sat vremena, osim u slučaju tehničkih smetnji izvan kontrole Certifikacijskog autoriteta.

Pristup javnom direktoriju omogućen je putem javne internetske mreže na adresi navedenoj u ekstenziji distribucijske točke CRL-a u kvalificiranom certifikatu za elektronički potpis.

4.9.3 Reproduciranje direktorija kvalificiranih certifikata za elektronički potpis na različitim web-lokacijama

Certifikacijski autoritet kopira direktorij certifikata na niz web-lokacija i osigurava usklađenost i cjelovitost kopija u skladu s [DPCM-om].

Dodatne pojedinosti možete pronaći u odlomku 4.13.

4.10 Postupci zaštite osobnih podataka

Informacije o Nositelju koje pribavi Certifikacijski autoritet prilikom obavljanja usluga izdavanja kvalificiranih certifikata za elektronički potpis smatraju se povjerljivima, osim u slučaju da je dana pisana suglasnost Nositelja, te se ne smiju objavljivati, uz iznimku informacija izričito predviđenih za javno korištenje (npr. javni ključ, datum opoziva

kvalificiranog certifikata za elektronički potpis). Sukladno ovom Operativnom priručniku za uslugu udaljenog elektroničkog potpisa, Certifikacijski autoritet ne obrađuje „posebne kategorije osobnih podataka" kako su definirane u uredbi GDPR.

Aktivnosti u dijelu identifikacije i zaštite podataka sukladne su nacionalnim zakonima banke koja obavlja djelatnosti registracijskog autoriteta. Točnije, trajanje pohrane certifikata i svih povezanih dokumenata i informacija propisano je talijanskim pravom pa je trajanje pohrane u skladu s talijanskim zakonom.

Navedene osobne podatke obrađuje Certifikacijski autoritet u skladu s uredbom GDPR.

4.11 Postupak organiziranja datoteke kontrolnih zapisa

Certifikacijski autoritet automatski ili vlastoručno upisuje u datoteku kontrolnih zapisa događaje iz čl. 36. [DPCM-a]. Upisuju se barem sljedeći događaji:

- izdavanje kvalificiranih certifikata za elektronički potpis;
- opoziv kvalificiranih certifikata za elektronički potpis uz navođenje datuma i vremena objave CRL-a;
- početak i završetak radne sesije sustava za generiranje kvalificiranih certifikata za elektronički potpis;
- personalizacija potpisnih uređaja;
- ulazak u sigurnu sobu certifikacijskog sustava i izlazak iz iste.

Certifikacijski autoritet upravlja datotekom kontrolnih zapisa u skladu s čl. 41. (2) [DPCM-a].

4.12 Postupak upravljanja sigurnosnim kopijama podataka

Certifikacijski autoritet izradio je i proveo plan osiguranja kontinuiteta usluge koja se obavlja u skladu s ovim Operativnim priručnikom za uslugu udaljenog elektroničkog potpisa, a glavne radnje koje se obavljaju sukladno odgovarajućim postupcima opisane su u nastavku.

4.12.1 Postupak stvaranja sigurnosnih kopija podataka

Svakodnevno se za podatke, aplikacije, kontrolne datoteke zapisnika i ostale datoteke izrađuju sigurnosne kopije potrebne kako bi se u cijelosti vratili kritični procesori sustava upravljanja kvalificiranim certifikatima za elektronički potpis. U smislu tih procesora, izrada sigurnosnih kopija obavlja se daljinski, a tim postupkom upravlja poseban centralizirani sustav koji ispunjava sljedeće zahtjeve:

- minimizira potrebu za ljudskom intervencijom i pristupanjem tehničkim prostorijama;
- pojednostavljuje raspoređivanje poslova stvaranja sigurnosnih kopija i njihove revizije;
- povećava pouzdanost poslova stvaranja sigurnosnih kopija.

4.13 Postupak upravljanja nezgodama i katastrofalnim događajima

U nastavku je naveden opći opis tih postupaka.

4.13.1 Kvarovi računala

Sva računala koja se koriste za pružanje usluge izdavanja kvalificiranih certifikata za elektronički potpis pokrivena su ugovorom o održavanju temeljem kojeg se u slučaju kvara jamči reaktivacija računala u roku od 24 (dvadeset četiri) sata.

4.13.2 Nedostaci softvera

U slučaju nedostataka (gubitka ili oštećenja) programa ili podataka koji se ne mogu na drugi način vratiti, isti će se vratiti iz pohranjenih sigurnosno kopiranih podataka.

4.13.3 Kvar potpisnog uređaja Certifikacijskog autoriteta

U slučaju kvara potpisnog uređaja Certifikacijskog autoriteta, privatni ključ ponovo se uspostavlja na novom potpisnom uređaju počevši od segmenata prethodno generiranih ključeva, a po provedbi posebnog postupka koji zahtijeva zajedničku intervenciju više operatera. Ključni segmenti sačuvani su u šifriranom formatu i u različitim kontejnerima pod nadzorom različitih voditelja.

Napomena: ključni segmenti ne predstavljaju „kopiju" certifikacijskog ključa ([DPCM]) i mogu se koristiti isključivo za vraćanje cijelog ključa sukladno prethodno opisanom postupku.

U slučaju da vraćanje certifikacijskog ključa nije moguće, provodi se postupak predviđen za nedostatke certifikacijskog ključa (pogledajte sljedeći odlomak).

4.13.4 Nedostaci certifikacijskog ključa

U slučaju nedostataka u vezi s povjerljivošću privatnog certifikacijskog ključa, Certifikacijski autoritet je dužan:

- opozvati certifikat povezan s neispravnim privatnim ključem;
- opoziv prijaviti AgID-u u roku od 24 (dvadeset četiri) sata od opoziva;
- obavijestiti Nositelje o svim kvalificiranim certifikatima za elektronički potpis koji su potpisani privatnim ključem koji pripada opozvanom paru;
- opozvati sve kvalificirane certifikate za elektronički potpis potpisane neispravnim ključem;
- izdati nove kvalificirane certifikate za elektronički potpis s pomoću novog privatnog ključa.

4.13.5 Ugroženost glavne lokacije

U slučaju nedostupnosti prostora, zgrade ili sustava u cjelini uslijed bilo kakve katastrofe (požar, poplava, urušavanje i sl.) aktivira se plan oporavka od katastrofe, a taj se plan primjenjuje na sve radne resurse društva Intesa Sanpaolo i na resurse treće strane koja nudi uslugu izdavanja vremenskog žiga.

5. PRESTANAK PRUŽANJA USLUGE IZDAVANJA KVALIFICIRANIH CERTIFIKATA ZA ELEKTRONIČKI POTPIS

5.1 Pojedinosti o prestanku pružanja usluge izdavanja kvalificiranih certifikata za elektronički potpis

U slučaju prestanka pružanja usluge kvalificiranog davatelja usluga povjerenja AgID-u se mora 60 (šezdeset) dana unaprijed dostaviti posebno priopćenje u kojem su naznačeni novi Certifikacijski autoritet, ako je određen zamjenski Certifikacijski autoritet, te voditelj registra certifikata i pripadajuće dokumentacije.

Istovremeno s priopćenjem koje se šalje AgID-u, svi Nositelji moraju biti obaviješteni o prestanku obavljanja predmetnih poslova.

Ako se ne odredi zamjenski Certifikacijski autoritet, u priopćenju se mora jasno navesti da će biti opozvani svi kva-

lificirani certifikati za elektronički potpis koji još nisu istekli u trenutku prestanka pružanja usluge. Ti će kvalificirani certifikati za elektronički potpis prilikom opoziva biti uvršteni na listu opozvanih certifikata.

Dodatne pojedinosti u vezi s prestankom pružanja usluge možete pronaći u Planu prestanka pružanja usluge koji je pripremilo društvo Intesa Sanpaolo.

6. UPRAVLJANJE VREMENSKIM OZNAKAMA

6.1 Usluga izdavanja vremenskih žigova

Ova se točka odnosi na čl. 40. (3), točka p [DPCM-a].

Certifikacijski autoritet osigurava pružanje usluge izdavanja vremenskih žigova u skladu s [DPCM-om], korištenjem usluga certifikacijskog autoriteta koji ispunjava uvjete za poslovanje u državama gdje se banke nalaze. Opis postupaka u vezi s davanjem zahtjeva za izdavanje vremenskog žiga i stjecanje istoga u skladu s važećim zakonima i propisima možete pronaći u operativnom priručniku pružatelja te usluge.

6.2 Točnost vremenske oznake

Sustav upravljanja vremenskim oznakama dohvaća podatak o vremenu iz radijskog prijamnika sinkroniziranog sa signalom koji emitira Nacionalni elektrotehnički institut „Galileo Ferraris" (NEI).

TSA-ov poslužitelj prilikom generiranja vremenskog žiga dohvaća datum/vrijeme iz sistemskog sata usklađenog s točnim vremenom UTC (Koordinirano univerzalno vrijeme) putem sinkronizacijskog signala primljenog od vanjskog prijamnika koji prepoznaje kvalitetu signala koji emitira mreža GPS satelita. Vremenski signal dobiven na taj način usklađen je s odstupanjima točnosti predviđenim važećim zakonima i propisima.

7. POSTUPAK VERIFIKACIJE ELEKTRONIČKOG POTPISA

Ova se točka odnosi na čl. 40. (3), točka r [DPCM-a].

7.1 Aplikacija za verifikaciju

Unutar područja „Dokumenti" direktnih kanala kod banaka Nositelj ima mogućnost uvida u svoje elektronički potpisane dokumente. Ti se dokumenti spremaju u PDF formatu, a ovisno o direktnom kanalu kojeg je Nositelj odabrao (internetski, mobilni), Nositelju na raspolaganju stoji aplikacija koja mu omogućuje verifikaciju stavljenog elektroničkog potpisa.

Nositelj također može primiti elektronički potpisane dokumente putem e-pošte.

Sukladno čl. 42. (2) [DPCM-a], verifikacijski sustavi raspoloživi Nositelju interoperabilni su s dokumentima koji se potpisuju elektroničkim potpisom koji izdaje Certifikacijski autoritet.

7.2 Format dokumenata

Dokumenti koji se dostavljaju Nositelju putem izravnih kanala banaka sukladni su s važećim zakonima i propisima; posebice se ističe da dokumenti u elektroničkom obliku ne mogu sadržavati *„makro naredbe, izvršne kodove ii druge elemente koji mogu aktivirati funkcije putem kojih se mogu mijenjati sadržane radnje, činjenice ili podaci"*.

7.3 Upozorenja u vezi s CRL-om

Nositelj i Poslovni subjekt prilikom pregledavanja moraju uzeti u obzir tehnička vremena potrebna za ažuriranje informacija sadržanih u CRL-u.

Ta su tehnička vremena posebno potrebna u slučaju da Nositelj, Poslovni subjekt, Registracijski autoritet ili Certifikacijski autoritet namjeravaju opozvati ili reaktivirati kvalificirani certifikat za elektronički potpis, kao i u slučaju kad Certifikacijski autoritet provodi tehničke/administrativne postupke u vezi sa zahtjevom za opoziv i pripadajućim ažuriranjem CRL-a.

Prilikom potpisivanja dokumenta s pomoću kvalificiranog certifikata za elektronički potpis provjerava se CRL lista kako bi se osiguralo da odgovarajući kvalificirani certifikat za elektronički potpis nije opozvan.

8. RADNI POSTUPAK ZA GENERIRANJE ELEKTRONIČKIH POTPISA

Ova se točka odnosi na čl. 40. (3), točka s [DPCM-a].

Karakteristike usluge ne obuhvaćaju isporuku potpisne aplikacije koja se instalira na uređaj Nositelja (osobno računalo, pametni telefon i sl.); sve funkcije koje Nositelju omogućuju potpisivanje jednog ili više elektroničkih dokumenata izravno su obuhvaćene odgovarajućom odredbom ugovora o usluzi digitalnog bankarstva i/ili ugovora o pružanju usluga certificiranja Banke.

Elektronički potpisi stvoreni putem usluge digitalnog bankarstva ispunjavaju zahtjeve predviđene za potpisne algoritme iz čl. 4. (2) [DPCM-a].