PODIJELI DOŽIVLJAJ.

KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

ID broj :	174
Vrsta propisa (skraćenica):	CD
Broj verzije:	1.0
Dokument OID:	1.3.6.1.4.1.56393.2.1.2.1
Odgovorni sektor:	Sektor za razvoj servisa i digitalnu transformaciju
Datum donošenja/usvajanja:	06/09/2021
Datum stupanja na snagu:	08/09/2021
Validnost:	Neodređeno
Broj aneksa/priloga:	1

Praktična pravila rada sistema elektronske identifikacije (CTrust eID CPS)

	Ime i prezime	Sektor	Pozicija
Odgovorni podnosilac – član Menadžment komiteta / kao Podnosilac:	Dušan Banović	Sektor za razvoj servisa i digitalnu transformaciju	Direktor Sektora za razvoj servisa i digitalnu transformaciju
Pripremili Eksperti:	Tanja Bokan	Sektor za razvoj servisa i digitalnu transformaciju	Rukovodilac odjeljenja za digitalnu transformaciju
	Ivan Stanković	Sektor Tehnike	Vođa službe za IT infrastrukturu i IT/NT bezbjednost
	Jovana Novaković		Glavni specijalista za regulatorna pitanja i odnose sa Vladom
	Biljana Papović	Sektor za razvoj servisa i digitalnu transformaciju	Vođa službe za unapređenje i automatizaciju poslovnih procesa
	Jelena Đođić	Sektor za razvoj servisa i digitalnu transformaciju	Specijalista za unapređenje korisničkih procesa i parametara kvaliteta
	Dragomir Stevanović – S&T Crna Gora d.o.o.		
	Slobodan Pavićević – S&T Crna Gora d.o.o.		

Revidirano:			
Odobrenje pravne usklađenosti:	Pavle Đurović	Sektor za korporativne i pravne poslove	Direktor Sektora za korporativne i pravne poslove i Sekretar Društva

Interne reference:

- Kompanijska direktiva o pripremi i usvajanju internih propisa
- Obavezujuća korporativna pravila za zaštitu privatnosti
- Kompanijska direktiva o sigurnosti
- Kompanijska direktiva o kontrolnom setu sigurnosti
- Politika pružanja kvalifikovanih elektronskih usluga povjerenja (CTrust Certificate Policy – CTrust CP)

Eksterne reference:

OSNOVNI ZAKON

[1] Zakon o elektronskoj identifikaciji i elektronskom potpisu

PRAVILNICI

[2] Pravilnik o minimalnim tehničkim standardima i pratećim procedurama u odnosu na koje se određuje stepen sigurnosti sistema elektronske identifikacije
[3] Pravilnik o tehničkim i operativnim zahtjevima koji se odnose na čvor - mjesto priključenja sistema elektronske identifikacije i procesu uspostavljanja okvira za interoperabilnost sistema elektronske identifikacije
[4] Pravilnik o okviru za interoperabilnost sistema elektronske identifikacije

OSTALI ZAKONI

[5] Zakon o zaštiti podataka o ličnosti

STANDARDI

[6] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation)
[7] ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management
[8] ISO 9001:2015 - Quality management systems - Requirements
[9] ETSI EN 319 401 V2.2.1. (2018-04) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[10] ETSI EN 319 411-1 V1.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[11] ETSI EN 319 411-2 V2.2.2. (2018-04) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[12] ETSI EN 319 412-1 V1.1.1. (2016-02) – Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 1: Overview and common data structures
[13] ETSI EN 319 403 V 2.2.2 (2015-08) - Electronic Signatures and Infrastructures (ESI);

	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
[14]	IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

ISTORIJA DOKUMENTA

Verzija	Datum stupanja na snagu propisa/izmjena	Kratak opis izmjena
1.0	08.09.2021.	Prva verzija dokumenta sa popunjenim poglavljima

SADRŽAJ:

1. UVOD

Crnogorski Telekom A.D. Podgorica (u daljem tekstu: CT) je uspostavio infrastrukturu i u okviru svoje organizacije oformio sistem za pružanje kvalifikovanih elektronskih usluga povjerenja (u daljem tekstu: CTrust).

Takođe je uspostavljen sistem elektronske identifikacije radi izdavanja sredstava elektronske identifikacije.

Ovim dokumentom definiše se način na koji CTrust ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su propisani, za sisteme elektronske identifikacije, Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim pravilnicima.

1.1. PREGLED OSNOVNIH PRETPOSTAVKI

Ovim dokumetnom opisani su bitni elementi sistema elektronske identifikacije i to:

- procedura za podnošenje zahtjeva i registracije korisnika;
- procedura za dokazivanje i provjeru identiteta pravnog i fizičkog lica;
- procedura za povezivanje pravnog i fizičkog lica;
- karakteristike i dizajn sredstva elektronske identifikacije:
  - CT sredstvo elektronske identifikacije koje je dizajnirano tako da koristi 2 autentifikaciona faktora: korisničko ime i lozinku kao faktor autentifikacije na osnovu znanja i One Time Password (OTP) koji se dobija putem eTrust autentifikator mobilne aplikacije, kao faktor autentifikacije na osnovu vlasništva tj. dinamički faktor autentifikacije;
- procedura za izdavanje, dostavu i aktivaciju sredstva elektronske identifikacije;
- procedura za suspenziju, opoziv i ponovnu aktivaciju sredstva elektronske identifikacije;
- procedura za obnovu i zamjenu sredstva elektronske identifikacije;
- mehanizam autentifikacije;
- upravljanje internim aktima, javno obavještavanje i informisanje korisnika;
- način upravljanja sigurnošću informacija;
- način vođenja evidencija;
- način ispunjenja zahtjeva povezanih sa prostorijama i zaposlenima;
- opis tehničkih kontrola koja se vrše nad sistemom;
- procedure kojima se vrše provjere usklađenosti i revizije.

1.1.1. OPSEG I NAMJENA

Ovaj dokument opisuje postupke i procedure koje primjenjuje CT tokom pružanja usluga izdavanja sredstava elektronske identifikacije.
Namjena ovog dokumenta je propisivanje postupaka koje sprovode učesnici navedeni u tački 1.3. ovog dokumenta.
Struktura ovog dokumenta zasniva se na standardizovanom dokumentu IETF RFC 3647, uz izvjesne modifikacije neophodne da bi se opisali zahtjevi za sistem i sredstva eID propisana Zakonom [1] i Pravilnikom [2].
CT utvrđuje i interna pravila rada (u daljem tekstu: interna pravila) u kojima su sadržani i detaljno opisani postupci i mjere koji se primjenjuju prilikom prijema zahtjeva za izdavanjem sredstva elektronske identifikacije, izdavanja sredstva elektronske identifikacije, upravljanja životnim vijekom sredstva elektronske identifikacije, upravljanja IT infrastrukturom i njenom zaštitom. Interna pravila su privatni dokumenti i predstavljaju poslovnu tajnu CT-a.

1.2. NAZIV DOKUMENTA I IDENTIFIKACIONI PODACI

CT-u je dodijeljen od strane IANA organizacije (Internet Assigned Number Authority) sljedeći OID: 1.3.6.1.4.1.56393.
Na osnovu tog OID-a CT je za potrebe sistema elektronske identifikacije dodijelio sljedeći OID: 1.3.6.1.4.1.56393.2.
U nastavku je naveden naziv ovog dokumenta i njegovi identifikacioni podaci.
Naziv: Praktična pravila rada sistema elektronske identifikacije (CTrust eID CPS)

Verzija: 1.0
Identifikaciona oznaka (OID) za ovaj dokument je: 1.3.6.1.4.1.56393.2.1.2.1
Internet adrese na kojoj je objavljen ovaj CPS dokument je: http://ca.ctrust.telekom.me/cpcps.

1.3. UČESNICI SISTEMA ELEKTRONSKE IDENTIFIKACIJE

Učesnici CTrust sistema elektronske identifikacije CT-a su:

- Upravljačko tijelo
- Operativno tijelo
- Registraciona tijela
- Korisnici
- Treća lica

1.3.1. UPRAVLJAČKO I OPERATIVNO TIJELO

1.3.1.1. UPRAVLJAČKO TIJELO CTRUST-A (CTRUST PMA ILI SAMO PMA)

CT organizuje upravljačko tijelo CTrust-a (eng. *Policy Managment Authority* – u daljem tekstu: CTrust PMA ili samo PMA) koje je odgovorno za obavljanje sljedećih aktivnosti:

- Izradu i održavanje ovog dokumenta;
- Izradu i održavanje ostalih javnih dokumenata koji su namijenjeni korisnicima, kao što su Ugovor sa krajnjim korisnikom (eng. *End-User Agreement*);
- Podnošenje praktičnih pravila rada na usvajanje izvršnom direktoru CT-a;
- Vrši nadzor i organizuje reviziju usklađenosti sistema elektronske identifikacije sa ovim dokumentom;
- Odgovorno je za izradu procjena procedura i praksi drugih sistema koji pružaju uslugu izrade sredstva elektronske identifikacije, a sa kojima se vrši međusobno povezivanje;
- Rješava potencijalne sporove nastale u domenu rada CTrust-a;
- I druge poslove upravljanja neophodne za funkcionisanje CTrust-a.

1.3.1.2. TIJELO ZA OPERATIVNE POSLOVE (CTRUST OA)

Tijelo za operativne poslove obavlja sljedeće aktivnosti:

- Instalacija, konfiguracija i održavanje IT sistema;
- Instalacija, konfiguracija i održavanje komunikacione mreže;
- Instalacija, konfiguracija i održavanje aplikacija sistema elektronske identifikacije;
- Upravljanje i nadzor infrastrukturom u skladu sa ovim dokumentom;
- Rješavanje sporova između krajnjih korisnika i registracionog tijela;
- I ostale operativne i tehničke poslove potrebne za funkcionisanje kompletne infrastrukture sistema za izradu sredstva elektronske identifikacije.

1.3.2. REGISTRACIONA TIJELA (REGISTRATION AUTHORITIES)

Poslove registracionog tijela za krajnje korisnike vrše Registraciona tijela CTrust-a i opisani su u nastavku dokumenta.

1.3.2.1. REGISTRACIONA TIJELA CTRUST-A (CTRUST RA)

Poslovnice CT-a predstavljaju registraciona tijela za podnošenje zahtjeva za elektronske usluge povjerenja. Zaposleni CT-a koji rade u poslovnicama u smislu ovog dokumenta predstavljaju službenike za registraciju.
Službenici za registraciju za potrebe izdavanja sredstva elektronske identifikacije obavljaju sljedeće aktivnosti:

- Vrše identifikaciju korisnika po važećim zakonskim procedurama i pravilima rada CT-a, a za potrebe pružanja usluge opisane ovim dokumentom;

- Primjenjuju interne procedure za provjeru službenih i ovjerenih dokumenata u cilju provjere identiteta korisnika i valjanosti njihovog zahtjeva, i preuzimaju službena i ovjerena dokumenta;
- Dostavljaju korisniku popunjen zahtjev za uslugu izdavanja sredstva elektronske identifikacije, da provjeri i potvrdi validnost podataka;
- Registruju fizičko ili pravno lice kojem se izdaje sredstvo elektronske identifikacije u sklopu procedure podnošenja zahtjeva;
- Dostavljaju krajnjem korisniku ugovor o korišćenju sredstva elektronske identifikacije, u skladu sa internim procedurama CT-a;
- Učestvuju u procesu suspenzije, opoziva i ponovne reaktivacije sredstva za elektronsku identifikaciju;
- Učestvuju u procesu obnove i zamjene sredstva za elektronsku identifikaciju;
- Obavljaju i druge potrebne poslove u skladu sa internim procedurama CT-a.

CTrust registraciona tijela djeluju u skladu sa praksom, procedurama i osnovnim dokumentima rada CTrust-a. Ne postoji ograničenje na broj registracionih tijela koja mogu biti pridružena CTrust infrastrukturi.

Registraciona tijela centralizovano vode evidenciju svih aktivnosti koje izvršavaju za potrebe CT-a.

1.3.3. NARUČIOCI I KORISNICI

Korisnici sredstva elektronske identifikacije koje izdaje CTrust su fizička lica, i pravna lica koja imaju prebivalište ili boravište odnosno sjedište u Crnoj Gori.
Naručioc (subscriber) može biti fizičko lice ili pravno lice. Uslugu upotrebljava korisnik (*subject*) čije se ime ili funkcija registruju kod prijave za izdavanje sredstva elektronske identifikacije.
Za uslugu definisanu ovim dokumentom naručilac je istovremeno i krajnji korisnik.
Punu odgovornost koja proističe iz upotrebe usluge snosi naručilac, bez obzira da li je naručilac fizičko ili pravno lice.

1.3.4. TREĆA LICA (RELYING PARTIES)

Treća lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, tijela državne uprave i dr.) koja se pouzdaju u izdato sredstvo elektronske identifikacije.

1.3.5. OSTALI UČESNICI

Ostali učesnici su pravna ili fizička lica koja, na neki način, doprinose ili učestvuju u obezbjeđivanju kvaliteta pružanja usluge elektronskog identiteta.

1.4. KOMPONENTE SISTEMA ELEKTRONSKE IDENTIFIKACIJE

1.4.1. SISTEMSKE KOMPONENTE

Glavne sistemske komponente sistema elektronske identifikacije su:

- Autentifikacioni i autorizacioni server - Authentication and Authorization Server

Authentication and Authorization Server upravlja svim sistemskim korisnicima i vrši dužnost autentifikacionog mehanizma sa sve vrste usluga. Sve komponente platforme koje poseduju web korisnički interfejs su integrisane sa Autentifikacionim serverom čime je ovoj komponenti povjerena autentifikacija i ona je odgovorna za pouzdano identifikovanje korisnika.

- Identity access management (IAM)

Identity access management (IAM) je softverska komponenta odgovorna za upravljanje korisničkim nalozima i zahtjevima za izdavanje certifikata za potrebe servisa udaljenog potpisa/pečata ili drugih udaljenih usluga. Ova komponenta sadrži funkcionalnosti kao što su kreiranje, izmjena i brisanje korisnika. Blisko sarađuje sa Back office-om, u nastojanju da

operaterima obezbijedi neophodne funkcionalnosti, kao što su odobravanje zahtjeva za izdavanje certifikata, verifikaciju korisničkog identiteta i dostavljanje zahtjeva za izdavanje certifikata do certifikacionog autoriteta.

- **Caligraphy Service Manager**

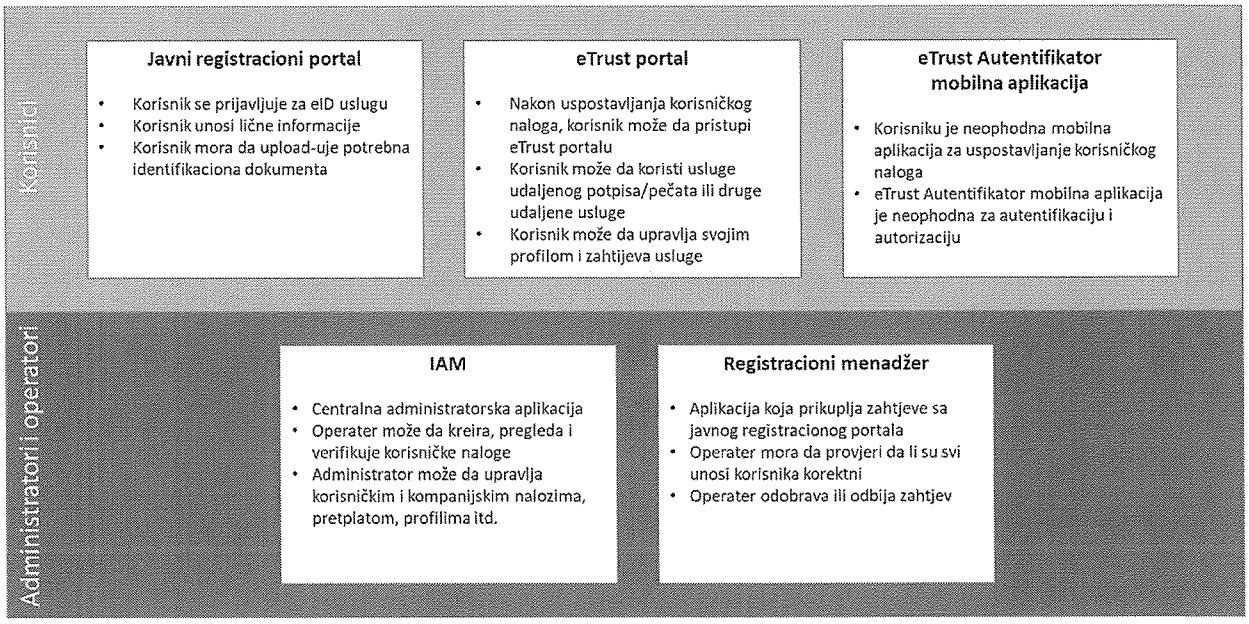
Caligraphy Service Manager je API gateway koji prikuplja sve korisničke zahtjeve i prevodi ih u odgovarajuće servisne zahtjeve. Ova komponenta predstavlja jedinstvenu tačku kontakta za sve vitalne funkcionalnosti koje sistem pruža krajnjim korisnicima.

- **Notification Manager**

Notification Manager je komponenta sistema odgovorna za prosljeđivanje sistemskih notifikacija krajnjim korisnicima. Ova komponenta se koristi za autentifikaciju korisnika koji pristupaju sistemu, kao i za autorizaciju digitalnih transakcija od strane korisnika preko mobilnog telefona, čime se postiže dodatni nivo sigurosti u identitet korisnika i volju korisnika da izvrši započetu operaciju.

1.4.2. APLIKATIVNE KOMPONENTE

Dijagram na slici 1. prikazuje glavne aplikacije koje se koriste u sistemu elektronske identifikacije u domenu dobijanja elektronskog identiteta korisnika, bilo da se radi o fizičkom ili pravnom licu.



Slika 1. – Aplikativne komponente usluge izdavanja eID sredstva

- Autentifikacioni Server – Centralni repozitorijum koji sadrži sve korisnike. Autentifikacioni server je odgovoran za mehanizam autentifikacije i omogućava nekoliko načina bezbjedne autentifikacije korisnicima.

- eTrust Autentifikator mobilna aplikacija – Mobilna aplikacija je važan bezbjednosni element sistema, koji pruža dodatni nivo bezbjednosti uzimajući učešće u mehanizmu autentifikacije i zahtijevajući od korisnika da autorizuje transakcije. eTrust Autentifikator mobilna aplikacija prima *push* notifikacije, obavještava korisnika i omogućava mu da autorizuje digitalnu transakciju.

- IAM – Identity and Access Management (IAM) je ključna komponenta koja čuva informacije o korisnicima i igra ulogu centralnog komunikacionog čvorišta za interakciju sa Back Office-om, PKI sistemom i ostalim sistemskim

komponentama koje čine jezgro sistema pružaoca usluga. IAM pohranjuje informacije o korisničkim nalozima i vodi računa o njihovoj pretplati, odnosno o upravljanju njihovim računima.

- Back office System – Back office je ključna operatorska komponenta za upravljanje korisničkim registracionim procesom. Ova komponenta obezbjeđuje operatorima sistema funkcije koje su neophodne za registraciju i upravljanje korisničkim nalozima. Osim ovoga, Back office nudi i funkcionalnosti odobravanja zahtjeva za izdavanje korisničkog certifikata, potpisivanje ugovora i verifikovanje identiteta korisnika.

1.5. ADMINISTRACIJA CPS DOKUMENTA

1.5.1. ORGANIZACIJA KOJA UPRAVLJA CPS DOKUMENTOM

CTrust PMA u ime CT-a periodično pregleda i ažurira ovaj dokument u skladu sa promjenama odredbi u zakonskoj regulativi ili drugim relevatnim situacijama.

1.5.2. KONTAKT OSOBA

Kontakt podaci za administraciju i sadržaj ovog dokumenta dati su u nastavku.
Poštanska adresa:

CTrust PMA: Crnogorski Telekom A.D.
Adresa: 81000 Podgorica, Moskovska br. 29.
E-mail: ctrust_pma@telekom.me

1.5.3. SUBJEKT KOJI UTVRĐUJE USAGLAŠENOST DOKUMENTA SA ZAKONOM

Nadležni organ shodno zakonu i propisima iz ove oblasti utvrđuje usaglašenost dokumenta sa zakonom. Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši nadležno Ministarstvo.
Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

1.5.4. PROCEDURA ODOBRAVANJA CPS DOKUMENTA

CPS dokument CT-a periodično se pregleda i ažurira po potrebi. Period pregleda i ažuriranja ovog dokumenta je minimalno jednom u dvije godine ili prilikom pripreme provjere usklađenosti.
Dokument se može pregledati i po potrebi ažurirati i češće ukoliko dođe do promjena u zakonskoj regulativi.
Na osnovu predloga CTrust PMA, CPS dokument odobrava izvršni direktor CT-a. Sve usvojene izmjene i dopune ovog dokumenta zvanično se dostavljaju bez odlaganja državnom organu nadležnom za ocjenu ispunjenosti uslova za vršenje usluga regulisanih Zakonom o elektronskoj identifikaciji i elektronskom potpisu.

1.6. DEFINICIJE I SKRAĆENICE

U ovom dokumentu pojedini izrazi imaju sljedeće značenje:

Pojam	Opis
Autentifikacija	Elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku.
Arhiva	Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili revizije.
Autorizacija	Procedura utvrđivanja prava koje neki autentifikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.
Certificate Practice Statement (CPS)	Javna praktična pravila i procedure koje certifikaciono tijelo primjenjuje u proceduri pružanja elektronske usluge.

Dinamička autentifikacija	Elektronski proces u kojem se upotrebljava kriptografija ili druge tehnike, kako bi se na zahtjev zainteresovane strane stvorio elektronski dokaz da subjekt kontroliše ili posjeduje identifikacione podatke, a koji se mijenja sa svakom autentifikacijom između subjekta i sistema koji provjerava identitet subjekta.
eID usluga	Usluga izdavanja sredstva elektronske identifikacije
eID sredstvo	Sredstvo elektronske identifikacije može biti skup podataka, računarska oprema (hardver) ili računarski program (softver) koji sadrže identifikacione podatke u elektronskom obliku ili povezuju fizičko lice, pravno lice ili organ vlasti sa tim podacima, a koji se koriste za autentifikaciju za uslugu u elektronskom obliku.
Faktor autentifikacije	Faktor za koji je potvrđeno da je povezan sa fizičkim licem, a može pripadati jednoj od sljedećih kategorija: faktor autentifikacije na osnovu vlasništva (faktor autentifikacije za koji subjekt mora dokazati da ga posjeduje), faktor autentifikacije na osnovu znanja (faktor autentifikacije za koji subjekt mora dokazati da ga poznaje), svojstveni faktor autentifikacije (faktor zasnovan na fizičkom obilježju fizičkog lica).
Identifikacija	Utvrđivanje da dato ime pojedinca odgovara realnom identitetu pojedinca.
Korisnički ugovor	Ugovor između krajnjeg korisnika i CT-a u cilju pružanja usluge elektronske identifikacije.
Korisnik/krajnji korisnik	Fizičko lice koje koristi uslugu elektronske identifikacije
Lični identifikacioni podaci	Skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica.
Organ vlasti	Državni organ, organ državne uprave, organ lokalne samouprave, odnosno lokalne uprave i pravno lice koje vrši javna ovlašćenja.
Registraciono tijelo (RA)	Tijelo odgovorno za identifikaciju i autentifikaciju korisnika, kao i kreiranje zahtjeva za izdavanje sredstva elektronske identifikacije. Često se i termin LRA (Local Registration Authority) koristi u istom kontekstu.
Repozitorijum	Web stranica i/ili direktorijum na kome su javno dostupni osnovni dokumenti rada CA, kao i eventualne druge informacije koje se odnose na pružanje elektronskih usluga povjerenja od strane datog CA (kao na primjer objavljivanje svih izdatih certifikata, itd.).
Certifikaciono tijelo izdavač certifikata (issuing CA)	U kontekstu određenog certifikata, certifikaciono tijelo – izdavalac certifikata je ono CA koje je izdalo (digitalno potpisalo) certifikat.
Certifikaciono tijelo	Pravno lice koje izdaje elektronske certifikate u skladu sa odredbama Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Treće lice	Treća lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove, tijela državne uprave i dr.) koja se pouzdaju u izdato sredstvo elektronske identifikacije.
eng. Policy Managment Authority	Upravljačko tijelo CTrust-a
Mobilna aplikacija (eTrust autentifikator)	Mobilna aplikacija koja je sastavni dio sredstva elektronske identifikacije koje izdaje CT
Interoperabilnost	Interoperabilnost je sposobnost dva ili više sistema elektronske identifikacije ili njihovih komponenti da razmjenjuju podatke i omoguće zajedničku upotrebu podataka i znanja.
Sistem elektronske identifikacije	Sistem elektronske identifikacije je sistem za izdavanje sredstava elektronske identifikacije fizičkim licima, pravnim licima, organima vlasti, odnosno fizičkim licima koja zastupaju pravna lica ili organe vlasti.
Čvor	Čvor je mjesto priključenja sistema elektronske identifikacije, ima mogućnost prepoznavanja i obrade, odnosno prosljeđivanja prenosa podataka na druge čvorove i povezivanja sa sistemima elektronske identifikacije drugih država.
Operater Čvora	Subjekt čija je obaveza da obezbijedi da čvor tačno i pouzdano obavlja funkciju mjesta priključenja.

Kvalifikovano sredstvo za izradu elektronskog potpisa/pečata - QSCD sredstvo	Kvalifikovano sredstvo za izradu elektronskog potpisa je sredstvo za izradu kvalifikovanog elektronskog potpisa/kvalifikovanog elektronskog pečata koje ispunjava posebne uslove propisane Zakonom o elektronskoj identifikaciji i elektronskom potpisu. Kvalifikovano sredstvo za izradu elektronskog potpisa/pečata mora da obezbijedi da: 1) se podaci za izradu kvalifikovanog elektronskog potpisa/pečata mogu pojaviti samo jedanput i da je ostvarena njihova sigurnost; 2) se podaci za izradu kvalifikovanog elektronskog potpisa/pečata ne mogu utvrditi iz tog potpisa/pečata; 3) kvalifikovani elektronski potpis/pečata bude zaštićen od falsifikovanja upotrebom trenutno dostupne tehnologije; 4) podatke za izradu kvalifikovanog elektronskog potpisa/pečata potpisnik odnosno autor može pouzdano zaštititi od neovlašćenog korišćenja.

Skraćenice koje se koriste u ovom dokumentu:

Skraćenica	Objašnjenje
CT	Crnogorski Telekom A.D. Podgorica
CTrust	Tijelo CT-a koje pruža elektronske usluge povjerenja/kvalifikovane elektronske usluge povjerenja
CA	Certification Authority – Certifikaciono tijelo
GP CA	General Purpose CA – Certifikaciono tijelo za opšte namjene
RP CA	Remote Purpose CA – Certifikaciono tijelo za udaljene usluge
OA	Operations Authority – Tijelo za operativne poslove
RA	Registration Authority – Registraciono tijelo
ID	Identification document – Identifikacioni dokument
OID	Object IDentifier
CSR	Certificate Signing Request – Zahtjev za potpisivanje certifikata
QSCD sredstvo	Qualified Signature Creation Device – Kvalifikovano sredstvo za izradu kvalifikovanog elektronskog potpisa/pečata
QSCD Modul	QSCD uređaj zajedno sa sistemom za upravljanje ključevima
RFC	Request For Comments – Publikacije Internet društva (ISOC) i njegovih povezanih tijela, najistaknutije Radne grupe za internet inženjering (IETF), glavnih tijela za tehnički razvoj i uspostavljanje standarda za Internet.
ETSI	European Telecommunication Standardization Institute – Evropski institut za standardizaciju telekomunikacija
CP	Certificate Policy – Politika pružanja kvalifikovanih elektronskih usluga povjerenja
CPS	Certificate Practice Statement – Praktična pravila rada certifikacionog tijela
PMA	Policy Managment Authority – Upravljačko tijelo CTrust-a
IAM	Identity Access Management – Aplikacija za centralizovano upravljanje korisnicima
TLS	Transport Layer Security – Kriptografski protokol koji omogućava sigurnu komunikaciju putem računarskih mreža

2. UPIS

2.1. PODNOŠENJE ZAHTJEVA I REGISTRACIJA KORISNIKA

Korisnik može podnijeti zahtjev na dva načina:

1. popunjavanjem online registracione forme,
2. dolaskom u CT poslovnicu.

Prilikom obrade zahtjeva isti se odbija ili odobrava. Tokom procesa obrade zahtjeva vrši se provjera identiteta.
Nakon odobrenja zahtjeva pokreće se proces izdavanja sredstva opisan u tački 3.2.
Zahtjev mogu podnijeti fizička lica ili pravna lica, koja imaju prebivalište ili boravište odnosno sjedište u Crnoj Gori.
Prilikom podnošenja zahtjeva podnosilac treba da se upozna sa uslovima koji su povezani sa upotrebom sredstva elektronske identifikacije i sa preporučenim sigurnosnim mjerama opreza koje su povezane sa sredstvima elektronske identifikacije na sajtu www.telekom.me/ctrust.

Takođe, prilikom podnošenja zahtjeva, prikuplja se sljedeći minimalni skup podataka:
1. Za fizičko lice:
   - ime i prezime,
   - datum rođenja,
   - identifikacioni broj;
2. Za pravno lice:
   - naziv kompanije odnosno skraćeni naziv kompanije,
   - PIB.

CTrust zadržava pravo da prikupi i dodatne podatke koji su od značaja za pružanje usluge (npr. telefonski broj, adresa, itd.)

2.1.1. PROCES OBRADE ZAHTJEVA I ODGOVORNOSTI

CTrust izdaje eID sredstvo tek nakon provjere identiteta krajnjih korisnika i uspješnog završetka procesa registracije. Tokom ovog procesa, osim izdavanja eID sredstva, CT korisniku, kao dodatnu povoljnost, izdaje i kvalifikovani certifikat u skladu sa dokumentom „Praktična pravila rada za izdavanje kvalifikovanih certifikata za kvalifikovani elektronski pečat i kvalifikovanih certifikata za kvalifikovani elektronski potpis (CTrust Certificate Practice Statement Q - CTrust CPS Q)". Glavni koraci u procesu obrade zahtjeva su:

- Krajnji korisnik popunjava obrazac za prijavu putem web aplikacije ili preko RA operatera;
- Po završetku popunjavanja obrasca krajnji korisnik prilaže valjan dokument za identifikaciju kao što je opisano u tačkama 2.2. – 2.4.;
- Krajnji korisnik prihvata uslove definisane u CTrust politici pružanja usluga i CTrust praktičnim pravilima rada potpisivanjem korisničkog ugovora (eng. *End-User Agreement*). Potpisivanje korisničkog ugovora može da se obavi svojeručno u poslovnici ili koristeći uslugu udaljenog kvalifikovanog elektronskog potpisa.
- Krajnji korisnik na osnovu uputstva ili instrukcija RA Operatora, preuzima eTrust autentifikator mobilnu aplikaciju, i istu instalira na mobilni uređaj. Korisnik može da download-uje i instalira eTrust autentifikator mobilnu aplikaciju i prije pristupanja procesu identifikacije. Krajnji korisnik mora imati instaliranu eTrust autentifikator mobilnu aplikaciju i podešen PIN za zaštitu iste prije pokretanja procesa izdavanja i aktivacije eID sredstva i izrade kvalifikovanog certifikata.
- Službenik za registraciju unosi podatke sa zahtjeva u RA aplikaciju. Zahtjev za izdavanje eID sredstva se zatim prosljeđuje drugom službeniku za registraciju na provjeru i odobrenje, a istovremeno se startuje proces aktivacije krajnjeg korisnika i eTrust autentifikator mobilne aplikacije.
- Sistem dostavlja krajnjem korisniku putem email-a link neophodan za aktivaciju naloga krajnjeg korisnika i aktivaciju eTrust autentifikator mobilne aplikacije. Link je aktivan 24 sata od trenutka prijema elektronskom poštom.
- Krajnji korisnik slijedi dostavljeni link i, u prvom koraku, skenira kamerom mobilnog telefona QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim krajnji korisnik generiše lozinku za korisnički nalog koji je u formi e-mail adrese krajnjeg korisnika. Ovim korakom se završava

aktivacija eTrust autentifikator mobilne aplikacije i naloga krajnjeg korisnika, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju.

2.2. PROVJERA IDENTITETA FIZIČKOG LICA

Fizičko lice i fizičko lice koje je ovlašćeno da djeluje u ime pravnog lica, će biti identifikovana licem u lice. Pojedinci moraju da se identifikuju koristeći jedan od sljedećih važećih identifikacionih dokumenata, izdatih od strane odgovarajućeg državnog organa:

- Lična karta
- Pasoš

CTrust ne provjerava podatke koji se ne nalaze na identifikacionom dokumentu (npr. e-mail adresa, broj telefona,...). Krajnji korisnik je odgovoran za tačnost podataka unesenih na Zahtjevu i Ovlašćenju, a koji se ne nalaze na identifikacionom dokumentu.
U cilju ispunjenja zahtjeva definisanih Pravilnikom [3] definiše se minimalni skup podataka o identitetu fizičkog lica koji se prikupljaju tokom procesa registracije i to:

- prezime koje fizičko lice koristi u pravnom prometu,
- ime koje fizičko lice koristi u pravnom prometu,
- datum rođenja,
- jedinstveni identifikator.

Minimalni skup može da sadrži jedan ili više sljedećih podataka:

- rođeno ime i prezime,
- mjesto rođenja,
- ime oca ili majke,
- pseudonim,
- adresu prebivališta,
- pol.

2.3. PROVJERA IDENTITETA PRAVNOG LICA

Pravno lice koje zahtijeva izradu sredstva elektronske identifikacije mora da obezbijedi dovoljno dokaza o svom identitetu.
Provjera identiteta pravnog lica može se vršiti koristeći jedan od sljedećih načina:

- Original ili ovjerena kopija zvaničnih dokumenata koji pružaju dokaz o identitetu pravnog lica – rješenje od PIB/PDV, odnosno izvod o registraciji iz CRPS-a, ne starije od šest mjeseci, odnosno za javne ustanove i nevladine organizacije i druge pravne subjekte, dokaz o registraciji od ovlašćenog nadležnog organa;
- Sačuvane informacije ako je bila provjera identiteta pravnog lica prethodno utvrđivana od strane CT-a.

Pravno lice podnosi zahtjev preko fizičkog lica koje mora imati važeće ovlašćenje da djeluje u ime pravnog lica. CTrust RA će provjeriti identitet ovlašćenog lica kao što je definisano u tački 2.2., i njegovo ovlašćenje da djeluje u ime pravnog lica kao što je definisano u tački 2.4.
U cilju ispunjenja zahtjeva definisanih Pravilnikom [3] definiše se minimalni skup podataka o identitetu pravnog lica koji se prikupljaju tokom procesa registracije i to:

- naziv pravnog lica koji se koristi u pravnom prometu,
- jedinstveni identifikator.

Minimalni skup može da sadrži jedan ili više sljedećih podataka:

- adresu pravnog lica,
- broj pravnog lica kao obveznika poreza na dodatu vrijednost,
- poreski identifikacioni broj.

Minimalni skup podataka o identitetu fizičkog lica koje zastupa pravno lice sadrži podatke iz tačke 2.1. Podaci se prenose u izvornom obliku, a po potrebi se prevode na latinično pismo.

2.4. PROVJERA OVLAŠĆENJA (POVEZIVANJE PRAVNOG I FIZIČKOG LICA)

Pojedinac koji zahtijeva sredstvo elektronske identifikacije pravnog lica mora da obezbijedi validnu dokumentaciju da je to lice ovlašćeno da u ime i za račun pravnog lica može da zahtijeva sredstvo elektronske identifikacije. Naziv pravnog lica koje će biti uključeno u certifikat mora biti identično Registrovanom punom ili skraćenom nazivu pravnog lica kako je u prezentiranim dokumentima.

CTrust RA službenik provjerava identičnost podataka o ovlašćenom fizičkom licu sa ovlašćenja i iz zahtjeva za izdavanje sredstva elektronske identifikacije. Ovlašćenje mora biti formirano na osnovu propisanog obrasca ovlašćenja CT-a, ovjereno pečatom i potpisom ovlašćenog zastupnika pravnog lica. Ovlašćeni zastupnik pravnog lica se provjerava uvidom u izvod iz CRPS-a, a njegov potpis sa potpisom iz kartona deponovanih potpisa ili uvidom u kopiju identifikacionog dokumenta.

3. UPRAVLJANJE SREDSTVIMA ELEKTRONSKE IDENTIFIKACIJE

3.1. KARAKTERISTIKE I DIZAJN SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

CT izdaje sredstvo elektronske identifikacije bazirano na korišćenju dva autentifikaciona faktora za povezivanje sa identifikacionim podacima korisnika i to jedan faktor autentifikacije na osnovu znanja tj. korisničko ime/lozinka – user name/password, a drugi faktor autentifikacije na osnovu vlasništva tj. dinamički faktor autentifikacije – *One Time Password* (OTP), koji se dobija putem eTrust autentifikator mobilne aplikacije.

Korisničko ime i lozinku određuje sam korisnik u procesu prijave i registracije za uslugu. Korisnik tokom popunjavanja obrasca prijave na registracionom portalu unosi svoju e-mail adresu, koja će služiti kao korisničko ime i na koju će davalac usluge, nakon provjere identiteta od strane službenika za registraciju, dostaviti link za aktivaciju korisničkog naloga. U procesu aktivacije korisnik sam generiše lozinku. Davalac usluge nema uticaja na kreiranje ovog parametara. Lozinka je, tokom svog životnog ciklusa, poznata samo korisniku. Korisničko ime i lozinka čuvaju se u bazi podataka davaoca usluge, na način da je lozinka u formi koja nije čitljiva (*salted hash* vrijednost), čime se obezbjeđuje da je ne može reprodukovati čak ni administrator sistema, ali da se, od strane davaoca usluge, može utvrditi da se to sredstvo upotrebljava samo pod kontrolom ili od strane lica kojem pripada. Politika za formiranje lozinki je u skladu sa najboljom praksom industrije.

Dinamički faktor autentifikacije dobija se tokom inicijalizacije eTrust autentifikator mobilne aplikacije. Korisnik tokom instalacije i aktivacije eTrust autentifikatora, skeniranjem QR koda pomoću svog mobilnog telefona, inicijalizuje sistem za isporuku vemenski bazirane jednokratne lozinke (eng. *One Time Password* – OTP). OTP se može smatrati dinamičkim faktorom autentifikacije na osnovu vlasništva, a s obzirom na to da se može koristiti samo uz korisničko ime i lozinku i da je dostupno samo korisniku na čijem je mobilnom telefonu inicirano, može se smatrati da se ovo sredstvo upotrebljava samo pod kontrolom ili od strane lica kojem pripada.

3.1.1. IDENTIFIKACIJA USLUGE IZRADE SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

Identifikaciona oznaka (OID) za uslugu izrade sredstva elektronske identifikacije po ovim Praktičnim pravilima je: 1.3.6.1.4.1.56393.2.1.1.1.

Davalac usluge će navedeni OID koristiti u aplikacijama koje koriste sredstvo elektronske identifikacije.

3.2. OBRADA ZAHTJEVA, IZDAVANJE, DOSTAVA I AKTIVACIJA SREDSTVA ZA ELEKTRONSKU IDENTIFIKACIJU

Nakon odobrenja podnijetog zahtjeva za izdavanjem eID sredstva iz poglavlja 2. ovog dokumenta pokreće se postupak izdavanja, dostave i aktivacije.

Sredstvo, bazirano na dvofaktorskoj autentifikaciji, sastoji se od korisničkog imena i lozinke i vremenski bazirane jednokratne lozinke (eng. *One Time Password* – OTP).

Korisničko ime i lozinku generiše krajnji korisnik u procesu registracije i aktivacje korisničkog naloga i, s obzirom na način generisanja, isporuka nije neophodna.

OTP se inicijalizuje tokom inicijalizacije mobilne aplikacije, skeniranjem QR koda pomoću korisničkog mobilnog telefona, te se može smatrati da je isporučeno na način koji osigurava isporuku lično fizičkom licu kojem je izdat.

3.2.1. PROCES OBRADE ZAHTJEVA ZA IZDAVANJEM EID SREDSTVA I ODGOVORNOSTI

CTrust izdaje eID sredstvo tek nakon provjere identiteta krajnjih korisnika i uspješnog završetka procesa registracije. Glavni koraci u procesu obrade zahtjeva su:

- Krajnji korisnik popunjava obrazac za prijavu putem web aplikacije ili preko RA operatera.
- Po završetku popunjavanja obrasca krajnji korisnik prilaže valjan dokument za identifikaciju kao što je opisano u 2.2.
- Krajnji korisnik prihvata uslove definisane u CTrust politici pružanja usluga i CTrust praktičnim pravilima rada potpisivanjem korisničkog ugovora (eng. *End-User Agreement*). Potpisivanje korisničkog ugovora može da se obavi svojeručno u poslovnici ili koristeći uslugu udaljenog kvalifikovanog elektronskog potpisa.
- Krajnji korisnik na osnovu uputstva ili instrukcija RA operatera, preuzima eTrust autentifikator mobilnu aplikaciju, i istu instalira na mobilni uređaj. Korisnik može da download-uje i instalira eTrust autentifikator mobilnu aplikaciju i prije pristupanja procesu identifikacije. Krajnji korisnik mora imati instaliranu eTrust autentifikator mobilnu aplikaciju i podešen PIN za zaštitu iste prije pokretanja procesa izrade kvalifikovanog certifikata.
- Službenik za registraciju unosi podatke sa zahtjeva u RA aplikaciju. Tokom procesa izdavanja eID sredstva korisniku se takođe izdaje i kvalifikovani certifikat za elektronsko potpisivanje. Zahtjev za izdavanje eID sredstva se zatim prosljeđuje drugom službeniku za registraciju na provjeru i odobrenje, a istovremeno se startuje proces registracije krajnjeg korisnika i eTrust autentifikator mobilne aplikacije.
- Sistem dostavlja krajnjem korisniku putem email-a link neophodan za registraciju krajnjeg korisnika i registraciju eTrust autentifikator mobilne aplikacije.
- Krajnji korisnik slijedi dostavljeni link i, u prvom koraku, skenira kamerom mobilnog telefona QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim krajnji korisnik generiše lozinku za korisnički nalog koji je u formi e-mail adrese krajnjeg korisnika. Ovim korakom se završava registracija eTrust autentifikator mobilne aplikacije i naloga krajnjeg korisnika, kao i postavljanje parametara za dvofaktorsku autentifikaciju (eng. *user name – password, OTP*).
- Kada izdavanje certifikata odobri službenik za registraciju pokreće se automatizovani proces generisanja odgovarajućeg certifikata krajnjeg korisnika.

3.2.2. POSTUPAK IDENTIFIKACIJE I AUTENTIFIKACIJE KRAJNJIH KORISNIKA

CTrust vrši identifikaciju i autentifikaciju kao što je definisano u tačkama 2.2. – 2.4.

3.2.3. ODOBRAVANJE ILI ODBIJANJE ZAHTJEVA ZA IZDAVANJE EID SREDSTVA

Zahtjev za izdavajem eID sredstva će biti odobren ako su kumulativno ispunjeni sljedeći uslovi:

- Podnosilac zahtjeva popunio obrazac zahtjeva za izdavanje i priložio važeće dokumente za identifikaciju u skladu sa tačkama 2.2. - 2.4.;
- Podnosilac zahtjeva ima odgovarajuće ovlašćenje (za pravno lice);
- Podaci na obrascu zahtjeva za izdavanje su potpuni;
- Identifikacija identiteta krajnjeg korisnika i provjera ovlašćenja (za pravno lice) je uspješna;

- Podnosilac zahtjeva potpisom korisničkog ugovora potvrđuje da je upoznat sa uslovima CTrust CP i CTrust CPS i da ih prihvata.

U slučaju da bilo koji od navedenih kriterijuma nije ispunjen ili ako postoji opravdana sumnja da podnosilac zahtjeva ne ispunjava uslove ovog dokumenta, korisničkog ugovora ili važećim propisima CTrust RA će odbiti zahtjev.

3.2.4. VRIJEME ZA OBRADU ZAHTJEVA

Inicijalna obrada zahtjeva za izdavanje eID sredstva počinje u toku prisustva podnosioca zahtjeva u poslovnicama CT-a, tj. obavezno se u dijelu inicijalne obrade mora obaviti provjera identiteta podnosioca zahtjeva. Nakon obavljene provjere identiteta u roku od 24h od prijema linka za registraciju, korisnik je u obavezi da završi registraciju eTrust autentifikator mobilne aplikacije i povezivanje iste sa kreiranim nalogom kao i da postavi parametre za dvofaktorsku autentifikaciju (eng. *user name – password, OTP*).

3.2.5. AKTIVNOSTI TOKOM PROCESA IZDAVANJA CERTIFIKATA

Nakon prijema validnog zahtjeva za izdavanjem eID sredstva u sklopu kojeg se obavlja i izdavanje certifikata za krajnje korisnike certifikaciono tijelo sprovodi proces izdavanja odgovarajućih certifikata na sljedeći način:

- Krajnji korisnik se obavještava da je njegov zahtjev za izradu certifikata odobren i zahtijeva se njegovo odobrenje (autorizacija) za izradu certifikata. Autorizacija korisnika je neophodna kako bi sistem mogao da njegovim privatnim ključem potpiše CSR.
- Nakon autorizacije od strane krajnjeg korisnika putem eTrust autentifikatora, pristupa se procesu generisanje para asimetričnih ključeva krajnjeg korisnika u QSCD sredstvu.
- Sistem dostavlja CSR CTrust RP CA certifikacionom tijelu, i izrada certifikata se realizuje u skladu sa definisanim profilom konkretnog certifikata koji se izdaje. Certifikat krajnjeg korisnika se potpisuje naprednim elektronskim potpisom, koristeći privatni ključ certifikacionog tijela, čime se sprečava falsifikovanje certifikata. CTrust RP CA certifikat krajnjeg korisnika smješta se na QSCD modul.
- Par asimetričnih ključeva i certifikat se smještaju na bezbjedan način u odgovarajuću bazu podataka QSCD modula. Na mobilnom uređaju korisnika se formira aktivacioni podatak opisan u poglavlju 4., neophodan za isključivu kontrolu privatnog ključa od strane krajnjeg korisnika.

3.2.6. OBAVJEŠTENJE KRAJNJIH KORISNIKA O IZDAVANJU SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

Krajnji korisnik se o izdavanju eID sredstva obavještava putem eTrust autentifikatora.

3.2.7. ISPORUKA I AKTIVACIJA SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

Sredstva elektronske identifikacije se isporučuju i aktiviraju na način opisan u tački 3.2.1. ovih Praktičnih pravila.

3.3. OPOZIV, SUSPENZIJA I PONOVNA AKTIVACIJA SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

3.3.1. OPOZIV EID SREDSTVA

Opoziv eID sredstva se radi u skladu sa pravilima opisanim u tačkama 3.3.1.1. – 3.3.1.6.

3.3.1.1. OKOLNOSTI ZA OPOZIV EID SREDSTVA

Po zahtjevu službenika za registraciju CTrust RA tijela, nadležnog državnog organa ili samog krajnjeg korisnika certifikaciono tijelo vrši opoziv izdatog sredstva elektronske identifikacije u sljedećim slučajevima:

- opoziv zahtijeva krajnji korisnik ili njegov ovlašćeni zastupnik;
- ako CT utvrdi da je podatak kojim se utvrđuje identitet lica pogrešan ili je izdat na osnovu pogrešnih podataka;
- ako CT primi obavještenje da je krajnji korisnik eID sredstva izgubio poslovnu sposobnost, umro ili prestao da postoji;

- ako CT utvrdi da su podaci korišteni u izradi eID sredstva ili informacioni sistem davaoca usluge izrade sredstva elektronske identifikacije ugroženi na način koji utiče na bezbjednost i pouzdanost sredstva;
- ako CT prestaje sa radom ili mu je rad zabranjen;
- ako CT primi sudsku odluku ill upravni akt koji se odnose na izdato eID sredstvo;
- postoje drugi pravni razlozi predviđeni internim aktima definisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu, i drugim propisima koji regulišu ovu oblast;
- ako CT utvrdi da krajnji korisnik krši odredbe ovog dokumenta.

3.3.1.2. KO MOŽE ZAHTIJEVATI OPOZIV EID SREDSTVA

Opoziv eID sredstva može biti zatražen od:

1. krajnjeg korisnika ili njegovog ovlašćenog zastupnika;
2. službenika za registraciju CTrust RA tijela uz odgovarajući dokaz da je ispunjen jedan od uslova za opoziv iz tačke 3.3.1.1.;
3. suda ili nadležnog organa državne uprave.

3.3.1.3. PROCEDURA OPOZIVA EID SREDSTVA

Opoziv sredstva eID vrši se opozivom korisničkog naloga, čime se raskida veza između eID sredstva i identifikacionih podataka korisnika na neograničeno vrijeme.
Opoziv sredstva povlači i opoziv certifikata koji je izdat korisniku tokom izrade eID sredstva.
U slučaju da je potrebno izršiti opoziv na zahtjev krajnjeg korisnika, ili ovlašćenog zastupnika isti je dužan da u najkraćem mogućem roku kontaktira službenika za registraciju CT-a radi dostavljanja zahtjeva za opoziv. Krajnji korisnik mora lično doći u poslovnicu CT-a da podnese zahtjev za opoziv lli da isti podnese online i potpiše kvalifikovanim elektronskim potpisom. U slučaju ovlašćenog zastupnika zahtjev se podnosi lično u CT poslovnici.
Identifikacija podnosioca zahtjeva za opoziv se radi kao što je definisano u tačkama 2.2. – 2.4.
Opozivom eID sredstva korisnik dobija e-mail/SMS obavještenje o opozivu sredstva koji proizvodi dejstvo odmah.

3.3.1.4. VRIJEME ZA PREDAJU ZAHTJEVA ZA OPOZIV EID SREDSTVA

Subjekt koji je postao svjestan okolnosti koje zahtijevaju opoziv eID sredstva mora zatražiti opoziv što je prije moguće i bez nepotrebnog odgađanja.

3.3.1.5. PERIOD VREMENA U KOJEM CT MORA DA OBRADI ZAHTJEV ZA OPOZIVOM EID SREDSTVA

Registraciono tijelo će odmah i bez odlaganja sprovesti postupak za opoziv, a najkasnije 1 radni dan po prijemu validnog zahtjeva.

3.3.1.6. ZAHTJEVI ZA PROVJEROM OPOZVANOSTI EID SREDSTVA OD STRANE TREĆIH LICA

Nije primjenjivo.

3.3.2. SUSPENZIJA EID SREDSTVA

Suspenzija eID sredstva se radi u skladu sa pravilima opisanim u tačkama 3.3.2.1. – 3.3.2.4.

3.3.2.1. OKOLNOSTI ZA SUSPENZIJU EID SREDSTVA

Po zahtjevu službenika za registraciju CTrust RA tijela, nadležnog državnog organa ili samog krajnjeg korisnika certifikaciono tijelo vrši suspenziju izdatog sredstva elektronske identifikacije u sljedećim slučajevima:

- suspenziju zahtijeva krajnji korisnik ili njegov ovlašćeni zastupnik;
- ako CT primi sudsku odluku ill upravni akt koji se odnose na izdato eID sredstvo;

- postoje drugi pravni razlozi predviđeni internim aktima definisanim Zakonom o elektronskoj identifikaciji i elektronskom potpisu, i drugim propisima koji regulišu ovu oblast.

3.3.2.2. KO MOŽE ZAHTIJEVATI SUSPENZIJU EID SREDSTVA

Suspenzija eID sredstva može biti zatražena od krajnjeg korisnika ili njegovog ovlašćenog zastupnika.

3.3.2.3. PROCEDURA SUSPENZIJE EID SREDSTVA

Suspenzija eID sredstva vrši se suspenzijom korisničkog naloga, čime se privremeno raskida veza između eID sredstva i identifikacionih podataka korisnika na ograničeno vrijeme.
U slučaju da je potrebno izvršiti suspenziju na zahtjev krajnjeg korisnika, ili ovlašćenog zastupnika isti je dužan da u najkraćem mogućem roku kontaktira službenika za registraciju CT-a radi dostavljanja zahtjeva za suspenzijom. Krajnji korisnik mora lično doći u poslovnicu CT-a da podnese zahtjev za suspenziju ili da isti podnese online i potpiše kvalifikovanim elektronskim potpisom. U slučaju ovlašćenog zastupnika zahtjev se podnosi lično u CT poslovnici uz važeće ovlašćenje ovjereno kod notara.
Identifikacija podnosioca zahtjeva za suspenziju se radi kao što je definisano u tačkama 2.2. – 2.4.
Suspenzijom eID sredstva korisnik dobija e-mail/SMS obavještenje o suspenziji sredstva koja proizvodi dejstvo odmah.

3.3.2.4. MAKSIMALNO TRAJANJE SUSPENZIJE EID SREDSTVA

Suspenzija eID sredstva se radi na osnovu zahtjeva korisnika. Suspenzija sredstva elektronske identifikacije vrši se suspendovanjem korisničkog naloga u sistemu za elektronsku identifikaciju CT-a, čime se raskida veza između eID sredstva i identifikacionih podataka korisnika do podnošenja zahtjeva korisnika za promjenom ovog stanja. Maksimalno trajanje suspenzije je 90 dana nakon čega se, ukoliko nije bilo zahtjeva za ponovno aktiviranje ili opoziv, eID sredstvo potencijalno opoziva od strane davaoca usluge. Korisnik dobija e-mail notifikaciju o svakoj promjeni stanja.

3.4. OBNOVA I ZAMJENA SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

Obnova se ne radi.
Zamjena eID sredstva se zasniva na važećem eID sredstvu i podrazumijeva reinstalaciju eTrust autentifikator aplikacije ili promjenu korisničkog imena.
U slučaju da korisnik ne posjeduje važeće eID sredstvo zamjena se ne obavlja već je korisnik dužan da podnese zahtjev za opoziv eID sredstva i izdavanje novog sredstva.

3.4.1. OKOLNOSTI POD KOJIMA SE MOŽE OBNOVITI ILI ZAMIJENITI SREDSTVO ELEKTRONSKE IDENTIFIKACIJE

Obnova nije primjenjiva.
Zamjena eID sredstva se može desiti usljed sljedećih okolnosti:

1. Korisnik ima potrebu da reinstalira eTrust autentifikator aplikaciju na postojećem telefonu;
2. Korisnik je promijenio mobilni telefon pa je potrebno napraviti instalaciju eTrust autentifikator aplikacije na novom telefonu i njenu personalizaciju;
3. Korisnik ima potrebu da promijeni korisničko ime.

3.4.2. KO MOŽE DA ZAHTIJEVA OBNOVU ILI ZAMJENU

Obnova nije primjenjiva.
Zamjenu eID sredstva može da zahtijeva korisnik.

3.4.3. PROVJERA IDENTITETA KOD OBNOVE

Nije primjenjivo.

3.4.4. PROVJERA IDENTITETA KOD ZAMJENE

Korisnik može samostalno obaviti zamjenu prijavom na eTrust portal čime je obavljena njegova provjera identiteta.

3.4.5. PROCES OBRADE ZAHTJEVA ZA OBNOVOM ILI ZAMJENOM

Za obnovu nije primjenjivo.
Kod reinstalacije mobilne aplikacije korisnik na instaliranoj eTust autentifikator aplikaciji izabere opciju resetuj nalog. U tom momentu se raskida veza sa identifikacionim podacima i generiše se novi e-mail sa personalizovanim linkom (24h). Zatim korisnik putem pomenutog linka završava proces zamjene skeniranjem QR koda putem instalirane aplikacije eTrust autentifikator i na taj način uspostavlja novu vezu sa svojim identifikacionim podacima. U slučaju da korisnik nema mogućnost da samostalno resetuje nalog može to da uradi dolaskom u CT poslovnicu. Nakon povjere identiteta od strane RA službenika isti pokreće resetovanje korisničkog naloga. U tom momentu korisnik dobija e-mail sa personalizovanim linkom i može sam da završi proces zamjene sredstva.
U slučaju promjene korisničkog imena, korisnik se prethodno loguje na eTrust portal i bira u sekciji nalog opciju „Uredi", gdje unosi novi nalog (e-mail adresa). Promjena korisničkog imena nije moguća u poslovnici CT-a.

3.4.6. OBAVJEŠTAVANJE KRAJNJIH KORISNIKA O IZDAVANJU OBNOVLJENOG ILI ZAMIJENJENOG EID SREDSTVA

Nije primjenjivo.

3.4.7. POSTUPAK POTVRDE PRIHVATANJA OBNOVLJENOG ILI ZAMIJENJENOG EID SREDSTVA

Kao što je opisano u tački 4.1.1.1.

3.4.8. OBJAVA OBNOVLJENOG ILI ZAMIJENJENOG EID SREDSTVA

Nije primjenjivo.

3.4.9. OBAVJEŠTAVANJE OSTALIH UČESNIKA O IZDAVANJU OBNOVLJENOG ILI ZAMIJENJENOG EID SREDSTVA

Ne obavještavaju se drugi učesnici.

4. AUTENTIFIKACIJA I PROSLJEĐIVANJE PODATAKA O IDENTITETU

Proces autentifikacije je integralni dio eID sistema i zasniva se na sljedećim bezbjednosnim parametrima:

- Autentifikacija sredstvom elektronske identifikacije, baziranom na korišćenju dva autentifikaciona faktora za povezivanje sa identifikacionim podacima korisnika, odvija se na način da se koristi jedan faktor autentifikacije na osnovu znanja tj. korisničko ime/lozinka – *user name/password*, a drugi faktor autentifikacije na osnovu vlasništva tj. dinamički faktor autentifikacije – *One Time Password* (OTP), koji se dobija putem eTrust autentifikator mobilne aplikacije.

Oba autentifikaciona faktora se provjeravaju od strane Autentifikacionog servera tokom prijave na sistem. Podaci o identitetu lica nijesu dio mehanizma autentifikacije.
Tokom autentifikacije korišćenjem korisničkog imena i lozinke, vrši se pouzdana provjera eID sredstva i njegova ispravnost, na način da se korisničko ime i lozinka provjeravaju prilikom logovanja na sistem. Podaci o identitetu lica nijesu dio mehanizma autentifikacije, a korisničko ime i lozinka čuvaju se u bazi podataka davaoca usluge, na način da je lozinka u formi koja nije čitljiva (*salted hash* vrijednost), čime se obezbjeđuje da je ne može reprodukovati čak ni administrator sistema, ali da se, od strane davaoca usluge, može utvrditi da se to sredstvo upotrebljava samo pod kontrolom ili od strane lica kojem pripada. Kompleksnošću lozinki koje sistem nameće krajnjem korisniku prilikom definisanja istih, se obezbjeđuje mala vjerovatnoća da će lozinka biti otkrivena pogađanjem.

Dinamički faktor autentifikacije se dobija tokom registrovanja mobilne aplikacije eTrust autentifikator, tako što se OTP generator inicijalizuje skeniranjem QR koda kamerom mobilnog telefona. Ovakav način autentifikacije obezbjeđuje razumno povjerenje u to da se eID sredstvo koristi pod kontrolom ili od strane lica kojem pripada, te da je obezbijeđeno od najčešće primjenjivanih napada.

4.1. SIGURNOSNE KONTROLE ZA PROVJERU EID SREDSTVA – AUTENTIFIKACIJA

Online autentifikacija predstavlja ključni dio sistema elektronskih usluga. eTrust portal zahtijeva autentifikaciju od klijenta. Korisnik može pristupiti uslugama tek nakon uspješno izvršenog procesa autentifikacije. Na ovaj način se obezbjeđuje da su informacije koje se razmjenjuju dostupne samo konkretnom autentifikovanom korisniku. Podržana su dva mehanizma bazirana na dvofaktorskoj (korisničko ime/lozinka i OTP) autentifikaciji.

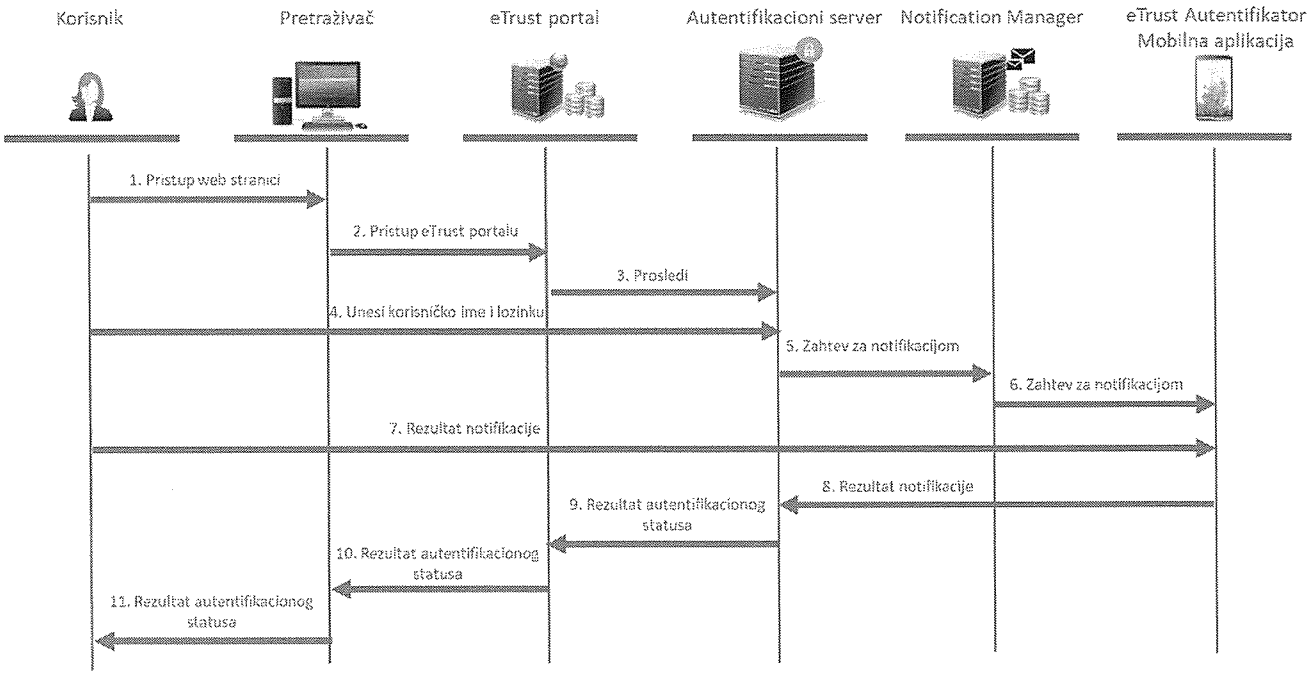
4.1.1.1. DVOFAKTORSKA (KORISNIČKO IME I LOZINKA, OTP) AUTENTIFIKACIJA

Sistem podržava dva tipa dvofaktorske autentifikacije. Oba tipa se baziraju na OTP generatoru i podrazumijevaju unos korisničkog imena i lozinke, kao i korišćenje eTrust autentifikator mobilne aplikacije.

Prva opcija je zasnovana na korišćenju mobilne notifikacije, gdje korisnik dobija notifikaciju na mobilnoj aplikaciji nakon unošenja korisničkog imena i lozinke na Autentifikacioni server. Korisnik mora da odobri notifikaciju sa telefona kako bi potvrdio akciju logovanja na sistem.

Druga opcija se zasniva na korišćenju OTP-a (*One Time Password*), gdje korisnik, nakon unosa korisničkog imena i lozinke, mora da pristupi OTP kodu na svojoj eTrust autentifikator mobilnoj aplikaciji i zatim taj kod unese direktno na web stranicu Autentifikacionog servera.

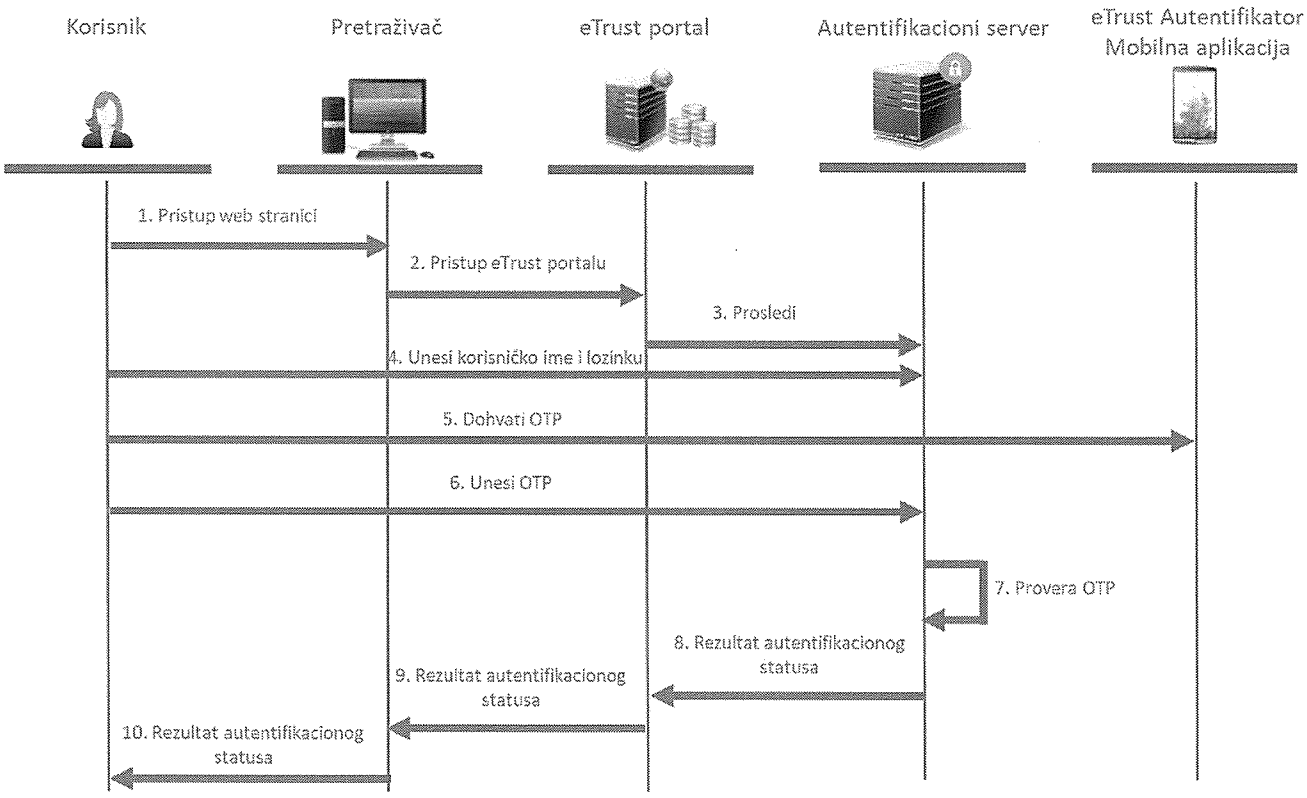
Mobilna notifikacija



Proces autentifikacije putem mobilne notifikacije se može opisati na sljedeći način:

1. Korisnik preko pretraživača pristupa eTrust portalu.
2. Ako ne postoji aktivan autentifikacioni token, onda eTrust portal prebacuje korisnika na Autentifikacioni server.
3. Korisnik unosi korisničko ime i lozinku na Autentifikacioni server.
4. Autentifikacioni server šalje zahtjev za notifikacijom do Notification Manager.
5. Notification Manager šalje notifikaciju ka eTrust Autentifikator mobilnoj aplikaciji.
6. eTrust Autentifikator mobilna aplikacija prikazuje notifikaciju korisniku koji bira da li da odobri ili odbaci zahtjev za logovanjem.
7. eTrust Autentifikator mobilna aplikacija šalje rezultat izbora korisnika do Autentifikacionog servera.
8. Autentifikacioni server šalje status rezultata ka eTrust portalu.
9. eTrust portal šalje status rezultata pretraživaču.
10. Web pretraživač prikaže poruku greške u slučaju da je korisnik odbio akciju na mobilnoj aplikaciji, ili vodi korisnika na željenu web stranu.

One Time Password (OTP)



Proces autentifikacije putem OTP se može opisati na sledeći način:

1. Korisnik preko pretraživača pristupa eTrust portalu.
2. Ako ne postoji aktivan autentifikacioni token, onda eTrust portal prebacuje korisnika na Autentifikacioni server.
3. Korisnik unosi korisničko ime i lozinku na Autentifikacioni server.
4. eTrust portal prikazuje web stranicu na kojoj korisnik može da unese svoj OTP kod. Korisnik treba da pristupi svojoj mobilnoj aplikaciji kako bi našao OTP kod.
5. Korisnik unosi OTP kod na Autentifikacioni server.
6. Autentifikacioni server provjerava da li je OTP kod ispravan.
7. Autentifikacioni server šalje status rezultata ka eTrust portalu.

8. eTrust portal šalje status rezultata pretraživaču.
9. Web pretraživač prikaže poruku greške u slučaju da je korisnik unio pogrešan OTP kod, ili vodi korisnika na željenu web stranu.

5. UPRAVLJANJE I ORGANIZACIJA

5.1. OBJAVLJIVANJE INTERNIH AKATA

5.1.1. REPOZITORIJUM

CT je odgovoran za rad repozitorijuma, objavu dokumenata i informacija na repozitorijumu. Repozitorijum čini javno dostupna web stranica CT-a. U okviru redovnog funkcionisanja repozitorijuma, on je dostupan za upotrebu 24 sata na dan, 7 dana u nedjelji.
U slučaju nedostupnosti repozitorijuma CT će preduzeti sve potrebne mjere i postupke da repozitorijum učini dostupnim u najkraćem mogućem roku.

5.1.2. OBJAVA INFORMACIJA O SISTEMU ELEKTRONSKE IDENTIFIKACIJE

Na repozitorijumu javno su objavljeni dokumenti i informacije o pružanju usluge izdavanja sredstva elektronske identifikacije (u daljem tekstu: eID usluga).
Repozitorijum se sastoji od dijela dostupnog na internet stranicama.

5.1.3. SADRŽAJ REPOZITORIJUMA

Na internet stranicama CTrust repozitorijuma objavljuju se:

- Dokument „Praktična pravila rada sistema elektronske identifikacije (CTrust eID CPS)";
- Prethodne verzije dokumenata;
- Uslovi i izjave o pružanju usluge izdavanja eID sredstva (eng. *Terms and conditions*);
- Obrasci zahtjeva za opoziv izdatog sredstva elektronske identifikacije;
- Obrasci zahtjeva za suspenziju izdatog sredstva elektronske identifikacije;
- Informacije o zakonskoj regulativi;
- Informacije o postojanju dokumenata važnih za poslovanje koji ne mogu biti u cjelosti ili uopšte objavljeni zbog osjetljivosti ili povjerljivosti sadržaja;
- Aktuelne lokacije poslovnica CT-a, koje predstavljaju lokacije registracionih tijela u smislu ovog dokumenta;
- Korisnička uputstva;
- Uputstva i potreban aplikativni softver za korišćenje sredstva elektronske identifikacije;
- Cjenovnik;
- Obavještenja krajnjim korisnicima i trećim licima u vezi s izrađenim sredstvima elektronske identifikacije;
- Ostale informacije vezane za rad CTrust-a.

Objavljeni sadržaj na internet stranicama dostupan je sa adrese http://www.telekom.me/ctrust na crnogorskom jeziku. CTrust PMA može pojedina dokumenta objaviti i na engleskom jeziku, ako za to ima potrebe.

U repozitorijumu se ne objavljuju povjerljivi podaci.

5.1.4. POSTUPCI OBJAVE SADRŽAJA I UPRAVLJANJA REPOZITORIJUMOM

Objavu dokumenata na repozitorijumu po odobrenju obavlja ovlašćeno lice zaduženo za upravljanje sadržajem internet dijela repozitorijuma.
Obavještenja krajnjim korisnicima, informacije o zakonskim aktima objavljuju se nakon početka primjene zakonskih akata u CTrust-u.

Objavu dokumenata uslova pružanja usluge izdavanja sredstva elektronske identifikacije, korisničkih uputstava, obrazaca zahtjeva, ugovora i ovlašćenja odobrava CTrust PMA. Objava ovih dokumenata se obavlja bez prethodne najave, a starije verzije dokumenata brišu se iz repozitorijuma.
Obavještenja i informacije mogu se objaviti na internet stranicama repozitorijuma i bez odobrenja CTrust PMA, ali CTrust PMA mora biti pravovremeno obaviješteno o svakoj objavi obavještenja i informacija.

5.1.5. UČESTALOST OBJAVLJIVANJA PODATAKA

CTrust PMA održava, ažurira, odobrava i objavljuje periodično po potrebi CPS za uslugu izdavanja eID sredstva.
Drugi dokumenti i ostale relevantne informacije objavljuju se po potrebi.

5.1.6. KONTROLA PRISTUPA REPOZITORIJUMU

Dokumenti i informacije objavljene na repozitorijumu su besplatne i javno dostupne svim učesnicima uspostavljene infrastrukture.
Repozitorijum ima uspostavljene kontrole pristupa u cilju sprečavanja neautorizovanog dodavanja, promjene ili brisanja informacija, zaštitu njihovog integriteta i autentičnosti. Pristup objavljenim dokumentima i informacijama na repozitorijumu omogućen je samo za čitanje.
Pravo dodavanja, promjene ili brisanja informacija na repozitorijumu imaju ovlašćena lica.

5.2. CJENOVNIK I OBAVJEŠTAVANJE KORISNIKA

5.2.1. CIJENE IZDAVANJA SREDSTVA ELEKTRONSKE IDENTIFIKACIJE

CT naplaćuje usluge izdavanja sredstva elektronske identifikacije u skladu sa cjenovnikom. Cijene ovih usluga biće objavljene na javnim internet stranicama repozitorijuma ili web stranici CT-a www.telekom.me.

5.2.2. CIJENE ZA DRUGE SERVISE

Nije primjenjivo.

5.2.3. POLITIKA REFUNDIRANJA

Troškovi se ne refundiraju.

5.2.4. FINANSIJSKA ODGOVORNOST

CT snosi finansijsku odgovornost za potencijalnu štetu koja može nastati korišćenjem izdatih srestava za elektronsku identifikaciju u skladu sa zakonima koji regulišu ovu oblast.

5.2.5. POKRIVANJE OSIGURANJA

CT dodatno osigurava imovinu polisom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija, i slično.

5.2.6. OSTALA SREDSTVA

Nije primjenjivo.

5.2.7. OSIGURANJE ILI GARANCIJSKO POKRIVANJE OD STRANE KRAJNJIH KORISNIKA I TREĆIH LICA

Krajnji korisnici usluge izdavanja eID sredstva i treća lica koja se pouzdaju u uslugu elektronske identifikacije isključivo su odgovorni da obezbijede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje usluga u okviru njihovih servisa ili aplikacija.

Krajnji korisnik eID sredstva dužan je da nadoknadi nastalu štetu koju bi CT mogao da ima kao rezultat nedozvoljenih radnji, kao što su:

- Lažno predstavljanje prilikom registracije krajnjeg korisnika;
- Bilo kog propusta krajnjeg korisnika za koji krajnji korisnik ne može dokazati da je propust nenamjerno učinjen;
- Ako krajnji korisnik ne obezbijedi korišćenje eID sredstva u skladu sa zakonom i ovim dokumentom;
- Ukoliko upotrebom eID sredstva krši bilo koji zakon koji je primjenjiv (na primjer ukoliko krši zakon o zaštiti intelektualne svojine);
- U svim drugim slučajevima koji su u suprotnosti sa zakonom, ovim dokumentom i drugim zakonskim aktima Crne Gore.

5.3. UPRAVLJANJE SIGURNOŠĆU INFORMACIJA

CT ima usvojenu kompanijsku direktivu za upravljanje bezbjednošću informacija i sertifikat ISO 27001 – sistem upravljanja bezbjednošću informacija.

Ovim poglavljem definisane su sve mjere, postupci i metodi, i druge tehničke bezbjednosne kontrole koje se primjenjuju prilikom upravljanja sigurnošću informacija. Tehničke kontrole uključuju životni ciklus sigurnosnih kontrola kao i operativne sigurnosne kontrole.

5.3.1. SIGURNOSNE KONTROLE RAČUNARA

5.3.1.1. SPECIFIČNI ZAHTJEVI ZA SIGURNOST RAČUNARA

CT primjenjuje mehanizme kontrole pristupa računarskim sistemima koji se koriste u okviru CTrust sistema. Računarska i komunikaciona oprema koja se koristi u okviru CTrust sistema fizički je obezbijeđena u prostorijama CT-a.
CT koristi i mehanizme logičke kontrole pristupa putem *firewall* uređaja.
Neautorizovan pristup opremi nije dozvoljen. Kritične softverske i hardverske komponente CTrust sistema mogu startovati samo dvije ili više ovlašćenih osoba koje posjeduju odgovarajuće smart kartice i koje znaju njihove PIN-ove ili odgovarajuće lozinke.

5.3.1.2. RANGIRANJE SIGURNOSTI RAČUNARA

Računari i operativni sistemi koje koristi CTrust sistem su komercijalni proizvodi koji su dodatno bezbjednosno ojačani.

5.3.2. ŽIVOTNI CIKLUS TEHNIČKIH SIGURNOSNIH KONTROLA

5.3.2.1. KONTROLE RAZVOJA SISTEMA

CT nadgleda i kontroliše razvoj sistema za izradu sredstava elektronske identifikacije. Softver koji se koristi u CTrust sistemu potiče iz pouzdanog izvora. Nove verzije softvera testiraju se kod proizvođača u fazi razvoja, a nakon toga i u CTrust sistemu u okviru testnog sajta. Nakon pozitivnih testova, vrši se implementacija softvera u produkcionom okruženju, u skladu sa internom procedurom upravljanja izmjenama na IT sistemima i aplikacijama CT-a.

5.3.2.2. KONTROLE UPRAVLJANJA SIGURNOŠĆU

CT nadgleda i kontroliše sigurnost i upravljanje sigurnošću sistema za izradu sredstva elektronske identifikacije.

5.3.2.3. ŽIVOTNI CIKLUS SIGURNOSNIH KONTROLA

CT sprovodi sva testiranja prije implementacije u okviru testnog sajta.

5.3.3. MREŽNE SIGURNOSNE KONTROLE

Sigurnost računarske mreže CTrust sistema zasnovana je na konceptu segmentacije mreže na mrežne zone različitih nivoa. Mrežne zone razgraničavaju se *firewall*-ovima koji propuštaju samo neophodan mrežni saobraćaj. Na sve sisteme locirane unutar jedne mrežne zone primjenjuju se iste sigurnosne mjere.
Mrežni segment na kom se nalaze radne stanice za administraciju *firewall*-om je odvojen od ostalih mrežnih segmenata i računara koji se nalaze u tim mrežnim segmentima.
Oprema za zaštitu računarske mreže bilježi tok saobraćaja i pokušaje pristupa servisima i javnim internet stranicama CTrust sistema. Samo ovlašćeno osoblje sa povjerljivim ulogama ima administratorska ovlašćenja za podešavanje i upravljanje opremom za zaštitu računarske mreže. Udaljeno podešavanje opreme za zaštitu računarske mreže je dozvoljeno pod strogo kontrolisanim uslovima.
Nepotrebne komunikacije, nalozi, portovi, protokoli i servisi su eksplicitno zabranjeni ili deaktivirani.
Interna računarska mreža CTrust sistema zaštićena je od neovlašćenog pristupa, uključujući pristup krajnjih korisnika i trećih lica.
Svi kritični sistemi smješteni su u sigurnoj zoni CT-a i raspoređeni su u više različitih sigurnosnih mrežnih zona.
Mrežne komponente CTrust sistema čuvaju se u fizički i logički sigurnom okruženju i usaglašenost njihove konfiguracije periodično se provjerava.

5.4. PRIVATNOST I ZAŠTITA LIČNIH PODATAKA

CT posvećuje pažnju zaštiti ličnih podataka koje prikuplja, skladišti i upotrebljava u cilju pružanja usluga iz opsega ovog dokumenta, te sa ličnim podacima postupa u skladu sa odgovarajućim zakonima. Podnošenjem zahtjeva za registraciju za korišćenje usluge elektonskog identiteta, korisnici daju saglasnost CT-u za korišćenje i obradu njihovih ličnih podataka prikupljenih u postupku registracije u skladu sa postojećom zakonskom regulativom, te čuvanje tih podataka u trajanju od najmanje 10 godina od prestanka važenja usluge na koju se ti podaci odnose.

5.4.1. PLAN PRIVATNOSTI

CT sprovodi mjere i postupke na zaštiti privatnosti i zaštiti ličnih podataka krajnjih korisnika usluge u skladu sa odgovarajućim zakonima.

5.4.2. INFORMACIJE KOJE SE TRETIRAJU KAO PRIVATNE

CT smatra privatnim sve informacije koje se odnose na krajnje korisnike eID usluge, osim onih informacija koje su sastavni dio izrađenog eID sredstva.

5.4.3. INFORMACIJE KOJE SE NE SMATRAJU PRIVATNIM

CT ne smatra privatnim samo one informacije na koje je krajnji korisnik dao saglasnost da se javno objave ili predaju trećem licu.

5.4.4. ODGOVORNOST ZA ZAŠTITU PRIVATNIH INFORMACIJA

CT je odgovoran za zaštitu privatnih informacija krajnjih korisnika u skladu sa internim propisima CT-a koji regulišu ovu oblast i pozitivnim propisima Crne Gore.

5.4.5. OTKRIVANJE INFORMACIJA SHODNO PRAVNIM I ADMINISTRATIVNIM PROCESIMA

CT je ovlašćen da koristi ili objavljuje lične podatke samo na osnovu saglasnosti krajnjih korisnika ili na zahtjev nadležnog organa.

5.4.6. OTKRIVANJE INFORMACIJE U SKLADU SA SUDSKIM ILI ADMINISTRATIVNIM PROCESOM

CT će ustupiti podatke sudu, tužilaštvu i drugim nadležnim državnim organima u slučajevima propisanim odgovarajućim zakonima.

5.4.7. OSTALE OKOLNOSTI KADA SE MOGU OTKRIVATI INFORMACIJE

CT će otkriti privatnu informaciju u ostalim okolnostima samo uz pismenu saglasnost krajnjeg korisnika.

5.4.8. PRAVA INTELEKTUALNOG VLASNIŠTVA

Sva prava intelektualnog vlasništva nad ovim dokumentom, zaštitnim znacima, eID sredstvom koje se izrađuje, repozitorijuma na kojima objavljuje informacije i svim dokumentima i informacijama koje su objavljene na repozitorijumima ostaju isključivo vlasništvo CT-a.

5.5. FIZIČKE BEZBJEDNOSNE KONTROLE

CT u svojim prostorijama primjenjuje odgovarajuće mehanizme fizičke zaštite prostorija i kontrole pristupa prostorijama CTrust sistema. Prostorije CTrust sistema čine bezbjedni prostor koji je podijeljen na više sigurnosnih zona u koje je dozvoljen pristup samo licima koje imaju odgovarajuće povjerljive uloge. Dozvoljen je pristup i drugim licima, ali samo uz prisustvo lica operativnog osoblja koja imaju odgovarajuće povjerljive uloge.

5.5.1. LOKACIJA I KONSTRUKCIJA SAJTA

Najvažnija oprema CTrust sistema se nalazi u posebnoj i zaštićenoj prostoriji, lociranoj u Data centru CT-a.
Prostorija CTrust sistema nalazi se u prostoru koji odgovara potrebama izvršenja operacija visoke bezbjednosti. Postoje označene zone sa fizičkom kontrolom pristupa i zaključane kancelarije sa odgovarajućim sefovima.

5.5.2. KONTROLA FIZIČKOG PRISTUPA

Pristup prostorijama CTrust sistema omogućen je primjenom sigurnosnih mehanizama fizičke kontrole pristupa u prostorije i iz jedne zone bezbjednosti u drugu zonu bezbjednosti, uključujući i zonu visoke bezbjednosti.
CTrust koristi za kontrolu fizičkog pristupa elektronske brave sa elektronskom karticom i čitačem otiska prsta.
Prostorija u kojoj su smješteni tehnički sistemi CTrust sistema je nadgledana 24 sata/7 dana nedjeljno:

- video nadzorom koji je povezan sa centralnim uređajem sistema u portirnici;
- fizičkom zaštitom na nivou poslovne zgrade CT-a u kojoj se nalazi Data centar, koju realizuje licencirana zaštitarska kuća.

5.5.3. ELEKTRIČNO NAPAJANJE I KLIMATIZACIJA

U prostorijama CTrust sistema izvedeno je električno napajanje u skladu sa svim standardima propisanim za električne instalacije i sigurno i kontinuirano napajanje električnom energijom opreme koju CTrust sistem koristi radi pružanja usluge izrade eID sredstva.
Sva oprema priključena je na jedinice za neprekidno napajanje.
Temperatura i vlažnost vazduha se u prostorijama održava u okviru unaprijed specificiranih intervala pomoću centralnog sistema klimatizacije Data centra CT-a, u skladu sa preporukama proizvođača računarske i druge opreme CTrust sistema, kao i u skladu sa principima bezbjednosti i zaštite zdravlja na radu.
Sistemi za napajanje električnom energijom i klimatizacije rade u redundantnom režimu rada.
Sve kritične komponente sistema su vezane na sistem za neprekidno napajanje (UPS) koji ima redundantne komponente.
UPS sistemi su vezani na mrežno napajanje i rezervno napajanje (agregat).

5.5.4. IZLOŽENOST POPLAVAMA I VREMENSKIM NEPOGODAMA

Prostorije CTrust sistema zaštićene su na odgovarajući način od poplava i vremenskih nepogoda.
Unutar prostorija nema vodovodnih instalacija, a oprema je smještena na povišenim podovima. Prostorija nije smještena u prizemlju i suterenu.

5.5.5. PREVENCIJA I ZAŠTITA OD POŽARA

CT primjenjuje sve potrebne mjere i postupke na prevenciji i zaštiti od požara.
Kompletan prostor Data centra CT-a je zaštićen sistemom za otkrivanje i automatsku dojavu požara tj. senzorima koji su povezani sa centralnim uređajem sistema u portirnici i sistemom obavještavanja na mobilni telefon rukovodioca službe za osiguranje i protivpožarnu zaštitu. U prostoriji CTrust sistema nalazi se i dodatni aparat za ručno gašenje požara.

5.5.6. SMJEŠTANJE MEDIJA

Svi mediji na kojima se nalaze podaci CTrust sistema, uključujući rezervne kopije sistema i softvera čuvaju se na bezbjedan način na dvije odvojene lokacije. Jedna lokacija je sef koji se nalazi u prostorijama CT-a. Druga lokacija je sef koji se nalazi na udaljenoj lokaciji u Podgorici.

5.5.7. ODLAGANJE NEPOTREBNIH MATERIJALA

Svi mediji i dokumentacija koji više nisu potrebni za rad CTrust sistema i predstavljaju otpad, prije odlaganja u smeće se fizički uništavaju odgovarajućom metodom. Papirni otpad se propušta kroz mašine za sječenje papira, a elektronski mediji se mogu mehanički uništiti ili koristeći poseban uređaj koji zadovoljava najstrože sigurnosne standarde iz ove oblasti (*degausser*).

5.5.8. SMJEŠTANJE KOPIJA MEDIJA NA UDALJENOJ LOKACIJI

Smještanje kopija medija realizuje se na drugoj lokaciji koja se nalazi u Podgorici, a koja ima uporediv nivo zaštite sa bezbjednom zonom na lokaciji CT-a.

5.5.9. ORGANIZACIONE MJERE ZAŠTITE

CT sprovodi kontrolu svojih zaposlenih radi obezbjeđivanja razumne sigurnosti, povjerljivosti i kompetencija zaposlenih. Osoblje CTrust sistema potpisuje izjavu da će se pridržavati pravne regulative u vezi zaštite podataka, kao i da će zadovoljiti sve postavljene zahtjeve u vezi sa povjerljivošću i svojim zaduženjima u okviru CTrust sistema.

5.5.10. POVJERLJIVE ULOGE

U okviru rada sistema za izradu eID sredstva osoblje može imati sljedeće povjerljive uloge:

- Sistem administrator ima sve neophodne privilegije i prava pristupa da:
  - Instalira i upravlja operativnim sistemima na kojima se koriste aplikacije za izradu eID sredstva;
  - Upravlja korisničkim nalozima na operativnom sistemu.
- CA Operator ima sve privilegije i prava pristupa da:
  - Kreira end entity-je (korisnike eID sredstva);
  - Kreira i izdaje eID sredstva.
- CA Revizor ima sve neophodne privilegije i prava da:
  - Vrši kontrolu audit logova.
- Database administrator ima sve neophodne privilegije i prava pristupa da:
  - Instalira i administrira bazu podataka za potrebe aplikacija za izradu eID sredstva.
- Službenik za registraciju je CA Operator i dodatno ima sve neophodne privilegije i prava pristupa da vrši:
  - Provjeru identiteta krajnjih korisnika;
  - Prijem, obradu i registraciju zahtjeva za potrebe izrade eID sredstva;
  - Prijem, obradu i registraciju zahtjeva za opoziv eID sredstva;
  - Potvrdu ispravnosti unesenih podataka krajnjih korisnika, odobravanje zahtjeva za izradu eID sredstva nakon uspješne potvrde ispravnosti unesenih podataka krajnjih korisnika, i pokretanje procesa za izdavanje ili opoziv eID sredstva.

Za potrebe uspostave sistema za izradu eID sredstva moguće je definisati i dodatne uloge.

5.5.11. IDENTIFIKACIJA I AUTENTIFIKACIJA OSOBA ZA POJEDINE ULOGE

Svaka uloga/dužnost definiše odgovarajuće zahtjeve u pogledu identifikacije i autentifikacije osobe koja obavlja datu ulogu/dužnost.
Za sve osobe koje imaju povjerljivu ulogu u sistemu za izradu eID sredstva CT-a vrši se bezbjednosna provjera lica.
Upravljanje korisničkim nalozima i kontrola autentifikacionih i autorizacionih parametara obavlja se centralizovano i pod kontrolom je sistem administratora. Svaka osoba sa povjerljivom ulogom ima korisnički nalog na Identity serveru i identifikuje se:

- aplikacijama certifikacionog tijela i aplikacijama sistema elektronske identifikacije – certifikatom za klijentsku autentifikaciju,
- operativnom sistemu - SSH ključem i kombinacijom korisničnog imena i lozinke.

Svaka operacija nad aplikacijama sistema za izradu eID sredstva zahtijeva da lice sa povjerljivom ulogom ima odgovarajuće privilegije za njihovo izvršavanje. Dijeljenje naloga i sredstava za autentifikaciju između osoblja je zabranjeno.
Osoblje izvršava samo one aktivnosti koje su autorizovane u okviru povjerljive uloge kroz ograničenja koje postavlja aplikacija, operativni sistem ili operativne procedure CTrust sistema.

5.5.12. ULOGE KOJE ZAHTIJEVAJU RAZDVAJANJE DUŽNOSTI

U cilju razdvajanja povjerljivih uloga u sistemu za izradu eID sredstva prava prijave na sisteme moraju biti dodijeljena u skladu sa tabelom 5.1.

PKI Uloga	Pristup operativnom sistemu	Pristup aplikaciji IAM	Pristup Registration manager aplikaciji
Sistem administrator	Da	Ne	Ne
CA Operator	Ne	Ne	Ne
CA Revizor	Ne	Da	Ne
Database administrator	Da	Ne	Ne
Službenik za registraciju	Ne	Da	Ne

Tabela 5.1: Prava prijave na sisteme

5.5.13. KADROVSKE BEZBJEDNOSNE KONTROLE

5.5.13.1. KVALIFIKACIJE, ISKUSTVO I PROVJERE

CT izvršava neophodne aktivnosti u cilju provjere biografije, kvalifikacija, kao i neophodnog iskustva u cilju realizacije u okviru konteksta kompetencije specifičnog posla. CT vrši sigurnosnu provjeru u skladu sa internim procedurama CT-a.
Zbog specifičnosti rada na poslovima pružanja usluge izrade eID sredstva, CT-u su potrebni ljudi koji su tehnološki i profesionalno kompetentni i koji imaju potrebna znanja. S tim u vezi CT vrši provjeru lica u skladu sa članom 34 Zakona o elektronskoj identifikaciji i elektronskom potpisu.

5.5.13.2. PROVJERA PRETHODNIH ANGAŽOVANJA

Provjera osoblja se vrši prema trenutno uspostavljenoj praksi u CT-u, a u skladu sa zakonom i propisima iz ove oblasti.

5.5.13.3. ZAHTJEVI ZA OBUKAMA

CT obezbjeđuje obuku za svoje zaposlene u cilju realizacije funkcija poslovanja.
Osoblje CTrust sistema prije početka obavljanja svojih poslova prolaze edukaciju u skladu sa poslovima koje će obavljati.
Zaposlenima s povjerljivim ulogama u radu na CTrust sistemima garantuje se obuka i usavršavanje u skladu sa njihovim povjerljivim ulogama.
Obuka i usavršavanje osoblja s povjerljivim ulogama u radu na CTrust sistemima obuhvata:

- Sigurnosni principi i mehanizmi;
- Svjesnost o sigurnosti;
- Obuka za korišćenje softvera na upotrebi;

- Zadaci povezani s povjerljivim ulogama koje će da obavljaju na sistemima za izradu eID sredstva;
- Postupci oporavka od nezgode i nastavka poslovanja.

Obuka i usavršavanje osoblja za registraciju u radu na CTrust sistemima uključuje:

- Osnovno znanje o sredstvima elektronske identifikacije;
- Načini registrovanja krajnjih korisnika;
- Uobičajene prijetnje u procesu provjere informacija;
- Rad u aplikacijama koje se koriste u registracionim tijelima;
- Svjesnost o sigurnosti;
- Zaštita ličnih podataka;
- Informacije s kojima je potrebno upoznati krajnje korisnike.

5.5.13.4. FREKVENCIJA I ZAHTJEVI ZA PONOVNU OBUKU

Obuka lica vrši se periodično i po potrebi radi održavanja potrebnog nivoa znanja zaposlenih za izvršavanje radnih zadataka.
Plan obrazovanja osoba se redovno revidira i u periodima koji nijesu duži od godinu dana.
Sprovođenje specijalizacije zaposlenih vrši se na godišnjem nivou u skladu sa planom obrazovanja.

5.5.13.5. SANKCIJE ZA NEOVLAŠĆENE AKTIVNOSTI

U slučaju neovlašćenih aktivnosti zaposleni podliježe odgovornosti za povrednu radne obaveze, a sankcije se određuju u okviru propisanog disciplinskog postupka CT-a.

5.5.13.6. ZAHTJEVI ZA SPOLJNE SARADNIKE

Spoljni saradnici predmet su istih provjera radi zaštite privatnosti i uslova povjerljivosti kao i zaposleni u CT-u koji obavljaju poslove u vezi sa CTrust sistemom.
Svi koji rade na ovaj način su obavezni potpisati sporazum o tajnosti (*non-disclosure agreement*).

5.5.13.7. DOKUMENTACIJA ZA POTREBE OSOBLJA

CT čini dostupnom svu dokumentaciju osoblju koja im je potrebna u obavljanju njihovih poslova u skladu sa njihovom povjerljivom ulogom i internim pravilima rada.

5.6. PROCEDURE UPRAVLJANJA RIZICIMA, ZAŠTITA KOMUNIKACIONIH KANALA I OSTALE TEHNIČKE KONTROLE

U procesu izrade eID sredstva se ne koristi kriptografski materijal.

Pod tehničkim kontrolama za upravljanje rizicima podrazumijevaju se:

- Procedure audit logovanja – uključuju logovanje događaja i reviziju sistema i implementirane su za svrhu održavanja bezbjednog okruženja;
- Procedure u slučaju incidenata i kršenja sigurnosti;
- Način zaštite od povjerljivosti, cjelovitosti i dostupnosti podataka opisan je u tački 5.6.11.

5.6.1. TIPOVI ZABILJEŽENIH DOGAĐAJA

CTrust sistem zapisuje događaje koji uključuju, ali nijesu ograničeni na operacije vezane za životni ciklus eID sredstva, pristup sistemu, kao i zahtjeve dostavljene sistemu.

5.6.2. FREKVENCIJA PROCESIRANJA LOGOVA

CTrust čuva audit logove u realnom vremenu, koji se kasnije procesiraju na dnevnom nivou i arhiviraju na sedmičnom nivou.

5.6.3. PERIOD ČUVANJA AUDIT LOGOVA

CTrust procesira i arhivira audit logove na sedmičnom nivou, koji se čuvaju u periodu od najmanje deset (10) godina od trenutka nastanka audit loga.

5.6.4. ZAŠTITA AUDIT LOGOVA

Audit logovi se samo mogu vidjeti od strane autorizovanog osoblja. Integritet audit loga koji nastaje iz softvera korišćenog za izradu eID sredstva zaštićen je primjenom odgovarajućih kriptografskih metoda.

5.6.5. PROCEDURE BACKUP-A AUDIT LOGOVA

CT implementira procedure backup-a audit logova.

5.6.6. SISTEM SAKUPLJANJA AUDIT LOGOVA

CT sakuplja i čuva audit logove u realnom vremenu.

5.6.7. OBAVJEŠTAVANJE LICA KOJE JE PROUZROKOVAO DOGAĐAJ

Lice koje je prouzrokovalo određeni audit događaj se ne obavještava o samoj audit aktivnosti.

5.6.8. PROCJENA RANJIVOSTI SISTEMA

CT periodično organizuje procjenu ranjivosti sistema.

5.6.9. ARHIVIRANJE ZAPISA/LOGOVA

Opšte odredbe koje se odnose na čuvanje logova različitih komponenti sistema za izradu eID sredstva definisane su ovim poglavljem.

5.6.9.1. TIPOVI ARHIVIRANIH ZAPISA

Zapisi koji se čuvaju:

- Zapisi o izdatim eID sredstvima;
- Informacije o podnešenim zahtjevima za izradu eID sredstva;
- I druga potrebna dokumentacija.

5.6.9.2. PERIOD ČUVANJA ARHIVE

Elektronski dnevnici čuvaju se najmanje deset (10) godina.
Ugovori sa krajnjim korisnicima, dokumentacija krajnjih korisnika i korespodencija trećih lica čuvaju se najmanje 10 godina.

5.6.9.3. ZAŠTITA ARHIVE

Podaci za arhive se prikupljaju u bezbjednoj zoni. Pristup bezbjednoj zoni je dozvoljen samo ovlašćenim osobama, kako je to definisano internim procedurama za pristup.
Za arhive operativnog sistema se upotrebljavaju zaštite koje omogućava sam operativni sistem.
Audit logovi aplikacija CTrust sistema su zaštićeni tehnologijom kriptografije javnih kriptografskih ključeva.

5.6.9.4. PROCEDURA PRAVLJENJA REZERVNIH KOPIJA ARHIVE

CTrust pravi rezervne kopije arhive periodično i čuva dvije odvojene kopije arhive. Jedna kopija arhive se čuva u sefu u CT-u, a druga u sefu na udaljenoj lokaciji koja se nalazi u Podgorici.

5.6.9.5. ZAHTJEVI ZA VREMENSKI PEČAT ARHIVIRANIH PODATAKA

Arhivirani podaci sadrže vrijeme dobijeno sa sistema na kojem su kreirani. To vrijeme nije elektronski vremenski pečat.

5.6.9.6. SISTEM SAKUPLJANJA ZAPISA

CTrust skuplja zapise i logove koji se arhiviraju po interno propisanoj proceduri.

5.6.9.7. PROCEDURE ZA PRISTUP I VERIFIKACIJU INFORMACIJA IZ ARHIVE

Pristup zapisima iz arhive imaju samo lica ovlašćena za pristup podacima iz arhive. Pristup podacima arhiviranim u siqurnim zonama imaju samo ovlašćena lica, uz dualnu kontrolu.
Verifikacija podataka iz arhive obavlja se provjerom njihovog integriteta.
Arhivirani podaci u elektronskom obliku se po potrebi upoređuju s pripadajućom kopijom.

5.6.10. KOMPROMITOVANJE I OPORAVAK SISTEMA POSLIJE NEPREDVIĐENIH SITUACIJA

5.6.10.1. PROCEDURE ZA POSTUPANJE U INCIDENTNIM I KOMPROMITUJUĆIM SITUACIJAMA

Internim pravilima rada definisane su procedure koje treba izvršiti pri rješavanju incidenata, kao i izvještavanje usljed potencijalne kompromitacije CTrust sistema.

5.6.10.2. RAČUNARSKI RESURSI, SOFTVER ILI PODACI KOJI SU OŠTEĆENI

CTrust definiše procedure oporavka koje se koriste ukoliko su računarski resursi, softver ili podaci neispravni ili se sumnja da su neispravni.

5.6.10.3. PROCEDURE KOJE SE SPROVODE KOD KOMPROMITACIJE SISTEMA

Procedure koje se sprovode kod kompromitacije sistema su propisane internim dokumentom „Plan prekida pružanja usluga CTrust sistema"

5.6.10.4. MOGUĆNOSTI KONTINUITETA POSLOVANJA NAKON KATASTROFE

Plan kontinuiteta poslovanja se implementira da osigura nastavak poslovanja nakon prirodne ili druge katastrofe.

5.6.11. ZAŠTITA POVJERLJIVOSTI, CJELOVITOSTI I DOSTUPNOSTI PODATAKA

Podaci o identitetu korisnika čuvaju se u bazi podataka davaoca usluge. Sigurnosne kopije baze podataka se vrše redovno i po utvrđenoj proceduri. Pristup podacima o identitetu korisnika posredstvom IAM aplikacije imaju samo zaposleni sa povjerljivim ulogama definisani u tabeli 5.1.

Autentifikacioni podaci korisnika (*password*) se čuvaju u formi koja nije čitljiva (*salted hash*) i nisu poznati ni davaocu usluga ni pouzdajućim stranama. Samo korisnik može da promijeni svoje autentifikacione podatke. Dinamička autentifikacija zahtijeva generisanje OTP koji se dobija na mobilnom uređaju korisnika, tako da se može pretpostaviti da je pod neposrednom kontrolom korisnika.

Komunikacioni kanal između korisnika i sistema zasnovan je na TLS protokolu.

Sve aktivnosti vezane za životni ciklus eID sredstva, pristup sistemu, kao i zahtjevi dostavljeni sistemu se bilježe u odgovarajućim audit logovima.
CT je sertifikovan po ISO 27001 standardu.

5.6.12. ZAVRŠETAK RADA

U slučaju planiranog prestanka pružanja usluge izrade eID sredstva, a u skladu sa „Planom prekida pružanja usluga CTrust sistema", poglavlje: „Prestanak poslovanja kvalifikovanog davaoca elektronskih usluga povjerenja", Crnogorski Telekom će učiniti sve razumne napore kako bi se minimizirao uticaj ukidanja usluge na poslovni proces krajnjih korisnika, naručilaca ili trećih lica.
CT će naročito:

- Obavijestiti sve krajnje korisnike i treća lica putem repozitorijuma i nadležni organ državne uprave najmanje šest mjeseci prije planiranog prestanka rada;
- Arhiviraće sve podatke u skladu sa periodom propisanim odgovarajućim zakonom od zadnjeg dana rada CTrust sistema.

5.7. PROVJERA USAGLAŠENOSTI I DRUGE PROCJENE

Provjera rada CTrust sistema regulisana je Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].
Upravni nadzor nad sprovođenjem Zakona o elektronskoj identifikaciji i elektronskom potpisu [1] vrši nadležno Ministarstvo.
Inspekcijski nadzor nad radom davalaca elektronskih usluga povjerenja i kvalifikovanih davalaca elektronskih usluga povjerenja i ispunjenošću uslova sistema elektronske identifikacije vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

5.7.1. FREKVENCIJA ILI OKOLNOSTI KADA SE VRŠI REVIZIJA

CTrust PMA će u skladu sa zakonom periodično organizovati internu provjeru i druge procjene usklađenosti sistema.
CTrust organizuje svoj rad u skladu sa relevantnim pravnim aktima koja regulišu rad davalaca elektronskih usluga povjerenja u Crnoj Gori, prije svega Zakona o elektronskoj identifikaciji i elektronskom potpisu i pravilnicima koji proizilaze iz istog, a odnose se na elektronske usluge povjerenja.
CTrust organizovaće bar jednom godišnje sopstvenu provjeru usaglašenosti ovog dokumenta i svog rada sa odgovarajućim propisima, a provjeru će izvršiti interni ili eksterni revizori.
Moguće je izvršiti i više od jedne interne revizije godišnje ukoliko je to zahtijevano od strane PMA ili je to posljedica nezadovoljavajućih rezultata prethodne revizije.

5.7.2. IDENTITET/KVALIFIKACIJE REVIZORA

Provjera saglasnosti rada sistema za izradu eID sredstva vrši se u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i odgovarajućim podzakonskim aktima.
CTrust takođe vrši redovne interne provjere usklađenosti svog rada pri čemu provjeru saglasnosti vrši interni revizor koji raspolaže adekvatnim revizorskim iskustvima i poznavanjem Zakona o elektronskoj identifikaciji i elektronskom potpisu.

5.7.3. ODNOS REVIZORA PREMA OCJENJIVANOM SUBJEKTU

Interni revizor na internoj provjeri saglasnosti ne ocjenjuje usaglašenost iz sopstvene oblasti odgovornosti, ukoliko ima neku od povjerljivih uloga u CTrust-u.
Eksterni revizor ne smije biti u konfliktu interesa.

5.7.4. TEME POKRIVENE U PROCESU PROCJENJIVANJA

Provjera usaglašenosti rada sistema za izradu eID sredstva obuhvata, ali se ne ograničava samo na sljedeće oblasti:

- Provjeru usaglašenosti ovog dokumenta i Zakona o elektronskoj identifikaciji i elektronskom potpisu;
- Kompletnost i tačnost dokumentacije;
- Organizacione procese, metode i procedure;
- Tehničke procese i procedure;
- Mjere iz oblasti informacione bezbjednosti;
- Mjere iz oblasti fizičke bezbjednosti;

Na zahtjev revizora CT pružiće pristup svim prostorima u kojima CTrust vrši izradu eID sredstva.

5.7.5. AKTIVNOSTI PREDUZETE U SLUČAJU NEUSAGLAŠENOSTI

CTrust uskladiće svoj rad sa preporukama i nalazima revizije.

5.7.6. OBJAVLJIVANJE REZULTATA

Izvještaji revizije dostavljaju se CTrust PMA.

6. INTEROPERABILNOST

Proces uspostavljanja okvira interoperabilnosti uspostavlja se primjenom evropske prakse i međunarodnih standarda:

- eIDAS Standard poruke;
- eIDAS Arhitektura interoperabilnosti;
- eIDAS Kripto uslovi za interoperabilnost na eIDAS;
- eIDAS Sigurnosni znak za označavanje jezika Profil svojstva.

CT će omogućiti interoperabilnost sistema za izradu eID sredstva sa drugim sistemima u skladu sa Zakonom i podzakonskim aktima koji regulišu ovu oblast.
Bitna komponenta sa kojom sistem elektronske identifikacije CTrust eID komunicira je Čvor – mjesto priključenja sistema elektronske identifikacije. CTrust eID sistem obezbjeđuje da:

- se dostavljaju metapodaci upravljanju čvorom u standardnom obliku prikladnom za automatsku obradu podataka, na siguran i pouzdan način. Sadrže najmanje sljedeće podatke:
  - podatak na osnovu koga se čvor identifikuje;
  - podatke na osnovu kojih se identifikuju povezani sistemi;
  - podatke na osnovu kojih se identifikuju poruke;
  - datum i vrijeme razmjene poruke.
- Automatsko preuzimanje podataka, u slučaju parametara koji se odnose na sigurnost;
- Čuvanje podataka pomoću kojih bi se, u slučaju incidenta, mogao rekonstruisati tok razmjene poruke radi utvrđivanja mjesta i vrste incidenta.

7. DRUGI POSLOVNI I PRAVNI ASPEKTI

7.1. TRAJANJE I PRESTANAK VAŽENJA

7.1.1. TRAJANJE

Ovaj dokument stupa na snagu danom donošenja. Dokument nema vremensko ograničenje.

7.1.2. PRESTANAK VAŽENJA

Dokument može biti stavljen van snage objavljivanjem nove verzije ovog dokumenta. U novoj verziji dokumenta biće naznačene obavljene izmjene i datum donošenja nove verzije dokumenta.

7.1.3. POSLJEDICE PRESTANKA VAŽENJA I NASTAVAK DJELOVANJA

Nakon prestanka važenja dokumenta, kao rezultata objavljivanja nove verzije dokumenta, eID sredstvo će se koristiti u skladu sa verzijom dokumeta koja je bila validna na dan izrade eID sredstva. U slučaju promjena okolnosti do nivoa kada ovo nije moguće, CT će obavijestiti krajnje korisnike na način definisan u tački 7.3.2., kao i treća lica preko javnih internet stranica, a na način definisan u tačkama 5.1.3. i 5.1.4.

7.2. POJEDINAČNA OBAVJEŠTENJA I KOMUNIKACIJA SA UČESNICIMA

CT nakon usvajanja dokumenta, distribuira isti kao i druge važeće akte/dokumente preko njegove javne internet stranice repozitorijuma.
Pogledati takođe tačku 7.3.2.

7.3. IZMJENE I DOPUNE

7.3.1. PROCEDURA ZA IZMJENU

Ovaj dokument mijenja se po potrebi. CTrust PMA može bez obavještavanja unositi tipografske ispravke, promjene kontakt podataka te druge manje ispravke koje bitno ne utiču na krajnje korisnike i treća lica. Svi učesnici mogu na kontakt adresu CTrust PMA definisanu u tački 1.5.2. ovog dokumenta poslati dopis s predlogom za ispravke grešaka, predlog dopuna ili izmjenu ovog dokumenta. U dopisu se navode kontakt podaci osobe koja je poslala predlog promjene. CTrust PMA može prihvatiti, prilagoditi ili odbiti predložene promjene nakon razmatranja istih. Izradu nove verzije ili izmjenu i dopunu postojeće verzije dokumenta odobrava i sprovodi CTrust PMA, a u skladu sa poslovnom regulativom CT-a i relevantnom zakonskom regulativom.

7.3.2. MEHANIZMI OBAVJEŠTAVANJA I VREMENSKI PERIODI

CTrust PMA može odlučiti da ne obavještava krajnje korisnike i treća lica u slučaju izmjena sa malim ili nikakvim uticajem. CTrust PMA u potpunosti odlučuje o tome da li izmjene imaju bilo kakav uticaj na krajnje korisnike i treća lica, na sopstvenu odgovornost.
Sve izmjene u ovom dokumentu biće objavljene na način koji je definisan u tački 1.5.
CTrust PMA će obavijestiti krajnje korisnike o promjenama koje imaju materijalnog uticaja na njih, putem e-maila i na javnim internet stranicama definisanim u tački 1.5.

7.3.3. OKOLNOSTI POD KOJIMA SE OID MORA IZMIJENITI

Donošenjem nove verzije dokumenta stvaraju se i okolnosti za definisanje nove OID vrijednosti predmetnog dokumenta.

7.4. PROCEDURE RJEŠAVANJA SPOROVA

Svi sporovi u vezi eID sredstva moraju se dostaviti na adresu iz tačke 1.5.2.
Sve sporove treba ako je moguće rješavati sporazumno. Ukoliko se dogovor ne može postići sporazumno, spor će se rješavati kod nadležnog suda u Crnoj Gori.

7.5. PRIMJENA ZAKONA

Ovaj dokument je u skladu sa Zakonom o elektronskoj identifikaciji i elektronskom potpisu i njegovim podzakonskim aktima.

7.6. USAGLAŠENOST SA PRIMJENLJIVIM ZAKONOM

Ovaj dokument je usaglašen sa:

- Zakonom o elektronskoj identifikaciji i elektronskom potpisu;
- Zakonom o zaštiti podataka o ličnosti;
- i drugim propisima i pravilnicima iz ove oblasti.

7.7. RAZNE ODREDBE

7.7.1. UGOVOR O PRUŽANJU USLUGE IZDAVANJA EID SREDSTVA

Ovaj dokument i opšti uslovi o izdavanju eID sredstva sadrže sve elemente koji definišu odnos između CT-a i krajnjih korisnika.

7.7.2. PRENOS PRAVA

Krajnjim korisnicima eID sredstva nije dozvoljeno da prava i obaveze koje proističu iz ovog dokumenta i opštih uslova prenesu u cjelosti ili parcijalno na druga lica po bilo kom osnovu.

7.7.3. KLAUZULA O VALJANOSTI

Nevaljanost jednog ili više djelova ovog dokumenta nemaju uticaj na valjanost ostalih odredbi ovog dokumenta ukoliko nemaju uticaj na materijalne odredbe (povjerenje u eID sredstvo i upotreba eID sredstva).

7.7.4. IZVRŠENJE (NADOKNADE ZA PRAVNOG ZASTUPNIKA I ODRICANJE OD PRAVA)

Nije primjenjivo.

7.7.5. VIŠA SILA

Višu silu predstavljaju vanredne okolnosti i nepredvidljive situacije kao što su prirodne katastrofe, nedostatak napajanja ili prekid telekomunikacionih veza, požar, zemljotres, nepredvidljivi IT incidenti kao što su napadi virusa ili napadi sa ciljem onemogućavanja servisa, greške u kriptografskim algoritmima i slično.
CT, krajnji korisnici ili treća lica neće biti odgovorni za bilo kakvu štetu koja je nastala usljed događaja kao rezultat više sile.

Dzina Tsybulskaja
Izvršni direktor

CRNOGORSKI TELEKOM A.D. PODGORICA

PRILOG 1

Struktura OID brojeva za dodjeljivanje Certificate Policy OID brojeva

Struktura CP OID		
NAZIV GRUPE	NAZIV GRANE OID-a	OID
Crnogorski Telekom PEN	Private enterprise number Crnogorski Telekom AD	CT-PEN
Organizaciona jedinica Crnogorskog Telekoma koja označava sistem elektronske identifikacije	OID grana dodijeljena organizacionoj jedinici nadležnoj za sistem elektronske identifikacije	OJCA = CT-PEN.2
Certificate Authority	OID grana koja označava konkretnu uslugu x=1 – Usluga izdavanja sredstava elektronske identifikacije	CAs = OJCAs.x
Certificate Policy	OID koji označava da li se sredstvo elektronske identifikacije izdaje za potrebe aplikacija ili krajnjih korisnika ili je u pitanju OID koji označava konkretni dokument davaoca elektronskih usluga povjerenja y=0 – sredstvo elektronske identifikacije za aplikacije y=1 – sredstvo elektronske identifikacije za korisnike y=2 – Praktična pravila rada sistema elektronske identifikacije (CTrust eID CPS)	CP = CAs.y
Certificate Policy	OID koji označava sredstvo elektronske identifikacije koji se izdaje ili OID koji označava verziju dokumenta davaoca usluga elektronske identifikacije	CP=CAs.y.N