KOMPANIJSKA DIREKTIVA

Crnogorski Telekom a.d. Podgorica

ID broj:	179
Vrsta propisa (skraćenica):	CD
Broj verzije:	1.1
Dokument OID:	1.3.6.1.4.1.56393.1.1.7.1
Odgovorni sektor:	Sektor za razvoj servisa i digitalnu transformaciju
Datum donošenja/usvajanja:	27/12/2022
Datum stupanja na snagu:	27/12/2022
Validnost:	Neodređeno
Broj aneksa/priloga:	0

Praktična pravila rada za pružanje kvalifikovane usluge elektronske preporučene dostave (CTrust eDelivery Certificate Practice Statement – CTrust eDelivery 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	Rukovodilac odjeljenja za cloud i virtuelnu infrastrukturu i sajber bezbjednost
	Jovana Novaković	Sektor za razvoj servisa i digitalnu transformaciju	Glavni specijalista za regulatorna pitanja i odnose sa Vladom
	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 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 bližim uslovima koje mora da ispunjava kvalifikovani davalac elektronskih usluga povjerenja [5] Pravilnik o bližim zahtjevima koje mora da ispunjava kvalifikovana usluga elektronske preporučene dostave Ostali zakoni [6] Zakon o zaštiti podataka o ličnosti Standardi [8] 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) [9] ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management [10] ISO 9001:2015 - Quality management systems - Requirements [11] ETSI EN 319 401 V2.2.1. (2018-04) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [12] ETSI EN 319 521 V1.0.0. (2018-05) – Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Electronic Registered Delivery Service Providers [13] IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework		

	[14] ETSI EN 319 522-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture [15] ETSI EN 319 522-2 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents [16] ETSI EN 319 522-3 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats

ISTORIJA DOKUMENTA

Verzija	Datum stupanja na snagu propisa/izmjena	Kratak opis izmjena
1.0	19.11.2022.	Prva verzija dokumenta sa popunjenim poglavljima.
1.1	27.12.2022.	Korekcije u poglavljima: 1.6. Definicije i skraćenice – pojašnjenje termina korisnik, krajnji korisnik i naručilac i usklađivanje cijelog dokumenta sa tim definicijama 2.1.1. Dopunjen opis procesa registracije zahtjeva za fizička i pravna lica 3.3. i 3.5. Usklađivanje sa članom 31 Zakona o elektronskoj identifikaciji i elektronskom potpisu

SADRŽAJ:

1. Uvod 7
1.1. Pregled osnovnih pretpostavki 7
1.1.1. Opseg i namjena 7
1.2. Naziv dokumenta i identifikacioni podaci 7
1.3. Učesnici sistema kvalifikovane usluge elektronske preporučene dostave 8
1.3.1. Upravljačko i operativno tijelo 8
1.3.1.1. Upravljačko tijelo CTrust-a (CTrust PMA ili samo PMA) 8
1.3.1.2. Tijelo za operativne poslove (CTrust OA) 8
1.3.2. Registraciona tijela (Registration Authorities) 8
1.3.2.1. Registraciona tijela CTrust-a (CTrust RA) 8
1.3.3. Naručioci i krajnji korisnici 9
1.3.4. Treća lica (Relying Parties) 9
1.3.5. Ostali učesnici 9
1.4. Komponente sistema kvalifikovane usluge elektronske preporučene dostave 9
1.4.1. Sistemske komponente 9
1.4.2. Aplikativne komponente 11
1.5. Administracija dokumenta 12
1.5.1. Organizacija koja upravlja dokumentom 12
1.5.2. Kontakt osoba 12
1.5.3. Subjekt koji utvrđuje usaglašenost dokumenta sa zakonom 12
1.5.4. Procedura odobravanja dokumenta 12
1.6. Definicije i skraćenice 12
2. Registracija korisnika 14
2.1. Podnošenje zahtjeva i registracija korisnika 14
2.1.1. Proces obrade zahtjeva i odgovornosti 15
2.1.1.1. Obrada zahtjeva za fizičko lice 15
2.1.1.2. Obrada zahtjeva za pravno lice 16
2.2. Provjera identiteta fizičkog lica 18
2.3. Provjera identiteta pravnog lica 18
3. Kvalifikovana usluga elektronske preporučene dostave 19
3.1. Identifikacija usluge 20
3.2. Procedura vršenja kvalifikovane usluge elektronske preporučene dostave 20
3.3. Integritet sadržaja poruke korisnika 21
3.4. Autentifikacija korisnika 21
3.4.1. Dvofaktorska (korisničko ime i lozinka, OTP) autentifikacija 21
3.5. Obezbjeđivanje kvalifikovanih elektronskih vremenskih pečata 23
3.6. Evidencija događaja 24
3.7. Interoperabilnost 25
4. Upravljanje i organizacija 25
4.1. Objavljivanje internih akata 25
4.1.1. Repozitorijum 25
4.1.2. Objava informacija o usluzi 25
4.1.3. Sadržaj repozitorijuma 25
4.1.4. Postupci objave sadržaja i upravljanja repozitorijumom 26
4.1.5. Učestalost objavljivanja podataka 26
4.1.6. Kontrola pristupa repozitorijumu 26
4.2. Cjenovnik i obavještavanje korisnika 26
4.2.1. Cijene pružanja kvalifikovane usluge elektronske preporučene dostave 26
4.2.2. Politika refundiranja 26

4.2.3. Finansijska odgovornost ... 26
4.2.4. Pokrivanje osiguranja ... 27
4.2.5. Ostala sredstva ... 27
4.2.6. Osiguranje ili garancijsko pokrivanje od strane naručilaca i trećih lica ... 27
4.3. Upravljanje sigurnošću informacija ... 27
4.3.1. Sigurnosne kontrole računara ... 27
4.3.1.1. Specifični zahtjevi za sigurnost računara ... 27
4.3.1.2. Rangiranje sigurnosti računara ... 27
4.3.2. Životni ciklus tehničkih sigurnosnih kontrola ... 28
4.3.2.1. Kontrole razvoja sistema ... 28
4.3.2.2. Kontrole upravljanja sigurnošću ... 28
4.3.2.3. Životni ciklus sigurnosnih kontrola ... 28
4.3.3. Mrežne sigurnosne kontrole ... 28
4.4. Privatnost i zaštita ličnih podataka ... 28
4.4.1. Plan privatnosti ... 28
4.4.2. Informacije koje se tretiraju kao privatne ... 28
4.4.3. Informacije koje se ne smatraju privatnim ... 29
4.4.4. Odgovornost za zaštitu privatnih informacija ... 29
4.4.5. Otkrivanje informacija shodno pravnim i administrativnim procesima ... 29
4.4.6. Otkrivanje informacije u skladu sa sudskim ili administrativnim procesom ... 29
4.4.7. Ostale okolnosti kada se mogu otkrivati informacije ... 29
4.4.8. Prava intelektualnog vlasništva ... 29
4.5. Fizičke bezbjednosne kontrole ... 29
4.5.1. Lokacija i konstrukcija sajta ... 29
4.5.2. Kontrola fizičkog pristupa ... 29
4.5.3. Električno napajanje i klimatizacija ... 29
4.5.4. Izloženost poplavama i vremenskim nepogodama ... 30
4.5.5. Prevencija i zaštita od požara ... 30
4.5.6. Smještanje medija ... 30
4.5.7. Odlaganje nepotrebnih materijala ... 30
4.5.8. Smještanje kopija medija na udaljenoj lokaciji ... 30
4.5.9. Organizacione mjere zaštite ... 30
4.5.10. Povjerljive uloge ... 30
4.5.11. Identifikacija i autentifikacija osoba za pojedine uloge ... 31
4.5.12. Uloge koje zahtijevaju razdvajanje dužnosti ... 31
4.5.13. Kadrovske bezbjednosne kontrole ... 31
4.5.13.1. Kvalifikacije, iskustvo i provjere ... 32
4.5.13.2. Provjera prethodnih angažovanja ... 32
4.5.13.3. Zahtjevi za obukama ... 32
4.5.13.4. Frekvencija i zahtjevi za ponovnu obuku ... 32
4.5.13.5. Sankcije za neovlašćene aktivnosti ... 32
4.5.13.6. Zahtjevi za spoljne saradnike ... 32
4.5.13.7. Dokumentacija za potrebe osoblja ... 33
4.6. Procedure upravljanja rizicima, zaštita komunikacionih kanala i ostale tehničke kontrole ... 33
4.6.1. Tipovi zabilježenih događaja ... 33
4.6.2. Frekvencija procesiranja logova ... 33
4.6.3. Period čuvanja audit logova ... 33
4.6.4. Zaštita audit logova ... 33
4.6.5. Procedure backup-a audit logova ... 33
4.6.6. Sistem sakupljanja audit logova ... 33
4.6.7. Obavještavanje lica koje je prouzrokovao događaj ... 33

4.6.8. Procjena ranjivosti sistema 33
4.6.9. Arhiviranje zapisa/logova 33
4.6.9.1. Tipovi arhiviranih zapisa 33
4.6.9.2. Period čuvanja arhive 34
4.6.9.3. Zaštita arhive 34
4.6.9.4. Procedura pravljenja rezervnih kopija arhive 34
4.6.9.5. Zahtjevi za vremenski pečat arhiviranih podataka 34
4.6.9.6. Sistem sakupljanja zapisa 34
4.6.9.7. Procedure za pristup i verifikaciju informacija iz arhive 34
4.6.10. Kompromitovanje i oporavak sistema poslije nepredviđenih situacija 34
4.6.10.1. Procedure za postupanje u incidentnim i kompromitujućim situacijama 34
4.6.10.2. Računarski resursi, softver ili podaci koji su oštećeni 34
4.6.10.3. Procedure koje se sprovode kod kompromitacije sistema 34
4.6.10.4. Mogućnosti kontinuiteta poslovanja nakon katastrofe 34
4.6.11. Zaštita povjerljivosti, cjelovitosti i dostupnosti podataka 35
4.6.12. Završetak rada 35
4.7. Provjera usaglašenosti i druge procjene 35
4.7.1. Frekvencija ili okolnosti kada se vrši revizija 35
4.7.2. Identitet/kvalifikacije revizora 36
4.7.3. Odnos revizora prema ocjenjivanom subjektu 36
4.7.4. Teme pokrivene u procesu procjenjivanja 36
4.7.5. Aktivnosti preduzete u slučaju neusaglašenosti 36
4.7.6. Objavljivanje rezultata 36
5. Drugi poslovni i pravni aspekti 36
5.1. Trajanje i prestanak važenja 36
5.1.1. Trajanje 36
5.1.2. Prestanak važenja 36
5.1.3. Posljedice prestanka važenja i nastavak djelovanja 37
5.2. Pojedinačna obavještenja i komunikacija sa učesnicima 37
5.3. Izmjene i dopune 37
5.3.1. Procedura za izmjenu 37
5.3.2. Mehanizmi obavještavanja i vremenski periodi 37
5.3.3. Okolnosti pod kojima se OID mora izmijeniti 37
5.4. Usaglašenost sa primjenljivim zakonom 37
5.5. Ostale odredbe 37
5.5.1. Ugovor o pružanju kvalifikovane usluge elektronske preporučene dostave 37
5.5.2. Prenos prava 38
5.5.3. Klauzula o valjanosti 38
5.5.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava) 38
5.5.5. Viša sila 38
5.6. Procedure rješavanja sporova 38

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).

U okviru CTrusta uspostavljen je i sistem za pružanje kvalifikovane usluge elektronske preporučene dostave (u daljem tekstu: eDelivery sistem) radi omogućavanja prenosa podataka pomoću elektronskih sredstava i pružanja dokaza o postupanju sa prenesenim podacima, uključujući dokaz o slanju i prijemu podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja ili bilo kakvih neovlašćenih prepravki.

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

1.1. Pregled osnovnih pretpostavki

Ovim dokumetnom opisani su bitni elementi sistema kvalifikovane usluge elektronske preporučene dostave i to:

- podnošenje zahtjeva i registracije krajnjih korisnika;
- dokazivanje i provjera identiteta fizičkog lica;
- dokazivanje i provjera identiteta pravnog lica;
- karakteristike i dizajn sistema za pružanje kvalifikovane usluge elektronske preporučene dostave;
- proces vršenja kvalifikovane usluge elektronske preporučene dostave;
- zaštita integriteta sadržaja elektronske preporučene dostave i obezbjeđivanje kvalifikovanih elektronskih vremenskih pečata;
- evidentiranje događaja prilikom vršenja kvalifikovane usluge elektronske preporučene dostave;
- interoperabilnost sistema za pružanje kvalifikovane usluge elektronske preporučene dostave;
- upravljanje internim aktima, javno obavještavanje i informisanje korisnika;
- način upravljanja sigurnošću informacija;
- način vođenja sistemskih evidencija;
- način ispunjenja zahtjeva povezanih sa prostorijama i zaposlenima;
- tehničke kontrole;
- provjera usklađenosti i revizije.

1.1.1. Opseg i namjena

Ovaj dokument opisuje postupke i procedure koje primjenjuje CT tokom pružanja kvalifikovane usluge elektronske preporučene dostave.
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 pružanje kvalifikovane usluge elektronske preporučene dostave propisani Zakonom [1] i Pravilnikom [5].
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 pružanja kvalifikovane usluge elektronske preporučene dostave i 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.
U nastavku je naveden naziv ovog dokumenta i njegovi identifikacioni podaci.
Naziv: Praktična pravila rada za pružanje kvalifikovane usluge elektronske preporučene dostave (CTrust eDelivery Certificate Practice Statement – CTrust eDelivery CPS)

Verzija: 1.1
Identifikaciona oznaka (OID) za ovaj dokument je: 1.3.6.1.4.1.56393.1.1.7.1
Internet adrese na kojoj je objavljen ovaj dokument je: http://ca.ctrust.telekom.me/cpcps.

1.3. Učesnici sistema kvalifikovane usluge elektronske preporučene dostave

Učesnici CTrust sistema kvalifikovane usluge elektronske preporučene dostave CT-a su:

- Upravljačko tijelo
- Operativno tijelo
- Registraciona tijela
- Naručioci i krajnji korisnici
- Treća lica
- Ostali učesnici

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 pravila rada na usvajanje izvršnom direktoru CT-a;
- Vršenje nadzor i organizuje reviziju usklađenosti pružanja kvalifikovane usluge elektronske preporučene dostave sa ovim dokumentom;
- Rješavanje potencijalnih sporova nastalih 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 za pružanje kvalifikovane usluge elektronske preporučene dostave;
- 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 za pružanje kvalifikovane usluge elektronske preporučene dostave.

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 pružanje kvalifikovanih elektronskih usluga povjerenja. Zaposleni CT-a koji rade u poslovnicama u smislu ovog dokumenta predstavljaju službenike za registraciju (RA operatere).

Registraciono tijelo može biti i eksterna organizacija (eksterni RA). U tom slučaju se odnosi i obaveze između CT-a i eksternog RA definišu zasebnim Ugovorom.
Službenici za registraciju obavljaju sljedeće aktivnosti:

- Vrše identifikaciju krajnjeg 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 krajnjeg korisnika i valjanosti njihovog zahtjeva, i preuzimaju službena i ovjerena dokumenta;
- Dostavljaju krajnjem korisniku popunjen zahtjev za pružanje kvalifikovane usluge elektronske preporučene dostave, da provjeri i potvrdi validnost podataka;
- Registruju fizičko ili pravno lice za kvalifikovanu uslugu elektronske preporučene dostave u sklopu procedure podnošenja zahtjeva;
- Dostavljaju krajnjem korisniku ugovor o korišćenju kvalifikovane usluge elektronske preporučene dostave, u skladu sa internim procedurama CT-a;
- 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 krajnji korisnici

Krajnji korisnici CTrust kvalifikovane usluge elektronske preporučene dostave su fizička lica koja imaju prebivalište ili boravište u Crnoj Gori i pravna lica registrovana u Crnoj Gori.
Naručilac *(subscriber)* može biti fizičko ili pravno lice. Kvalifikovanu uslugu elektronske preporučene dostave upotrebljava krajnji korisnik čije se ime ili funkcija registruju kod prijave za korišćenje kvalifikovane elektronske usluge povjerenja.
Kada kvalifikovanu uslugu elektronske preporučene dostave traži naručilac fizičko lice, tada je naručilac istovremeno i krajnji korisnik.
Kada kvalifikovanu uslugu elektronske preporučene dostave traži naručilac koji je pravno lice, tada naručilac daje pravo na upotrebu kvalifikovane usluge povjerenja krajnjem korisniku.
Punu odgovornost koja proističe iz upotrebe kvalifikovane usluge elektronske preporučene dostave 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, i dr.) koja se pouzdaju u CTrust kvalifikovanu uslugu elektronske preporučene dostave.

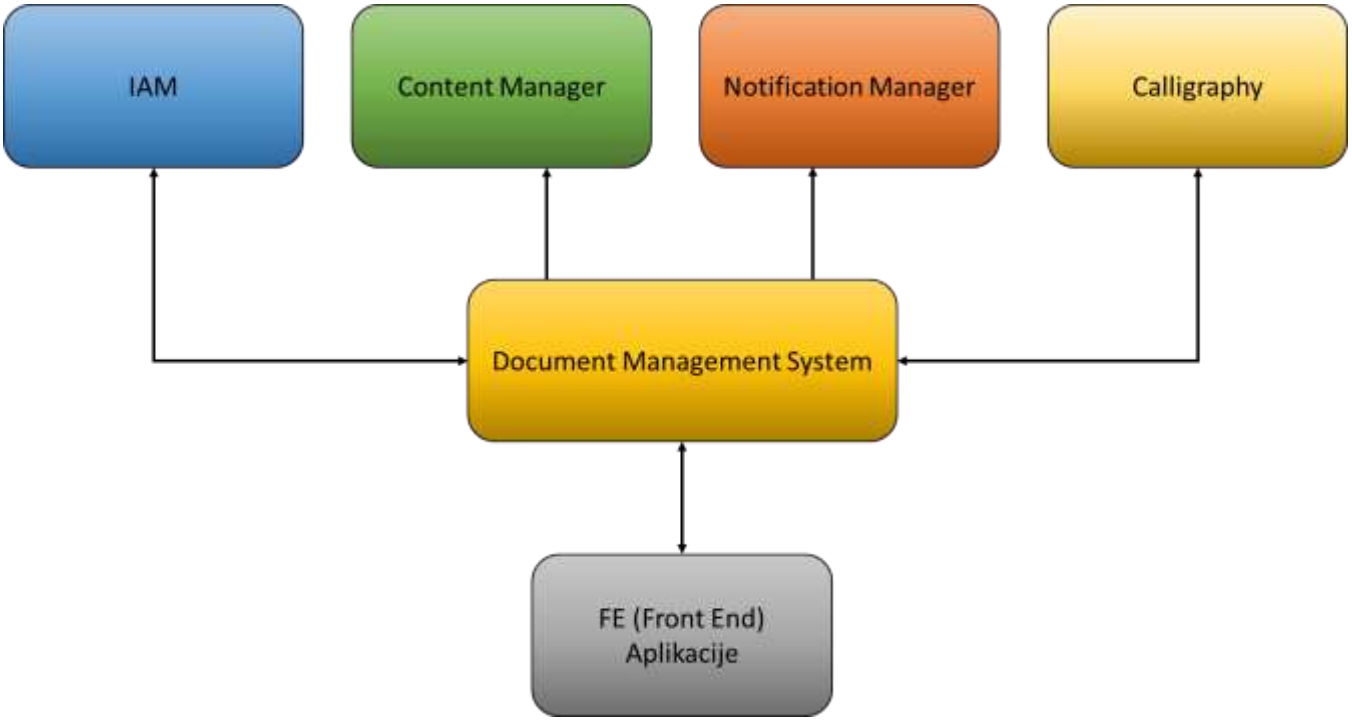
1.3.5. Ostali učesnici

Ostali učesnici su pravna ili fizička lica koja, na neki način, doprinose ili učestvuju u obezbjeđivanju kvaliteta pružanja kvalifikovane usluge elektronske preporučene dostave.

1.4. Komponente sistema kvalifikovane usluge elektronske preporučene dostave

1.4.1. Sistemske komponente

Sistemske komponente neophodne za korišćenje kvalifikovane usluge elektronske preporučene dostave prikazane su na slici 1.



Slika 1. – Sistemske komponente za korišćenje kvalifikovane usluge elektronske preporučene dostave

Glavne sistemske komponente eDelivery sistema su:

- **Identity access management (IAM)**

Identity access management (IAM) je softverska komponenta koja se koristi za upravljanje nalozima krajnjih korisnika. Ova komponenta sadrži funkcionalnosti kao što su kreiranje, izmjena i brisanje krajnjeg korisnika. Direktno komunicira sa Back office sistemom, u nastojanju da operaterima obezbijedi neophodne funkcionalnosti, prije svega verifikaciju korisničkog identiteta.

- **Content Manager (CM)**

Content Manager je modul koji se koristi za skladištenje binarnih podataka učitanih, potpisanih i pečatiranih dokumenata. CM koristi API metode za učitavanje i povlačenje binarnih podataka preko zadatih referenci.

- **Document Management System (DMS)**

Document Management System je modul čije su funkcionalnosti dostupne jedino preko CTrust portala, odakle krajnji korisnici mogu da kreiraju *workflow* za razmjenu dokumenata i izvršavaju različite vrste akcija u okviru *workflow*-a u kome participiraju.

- **Caligraphy Service Manager**

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

- **Notification Manager**

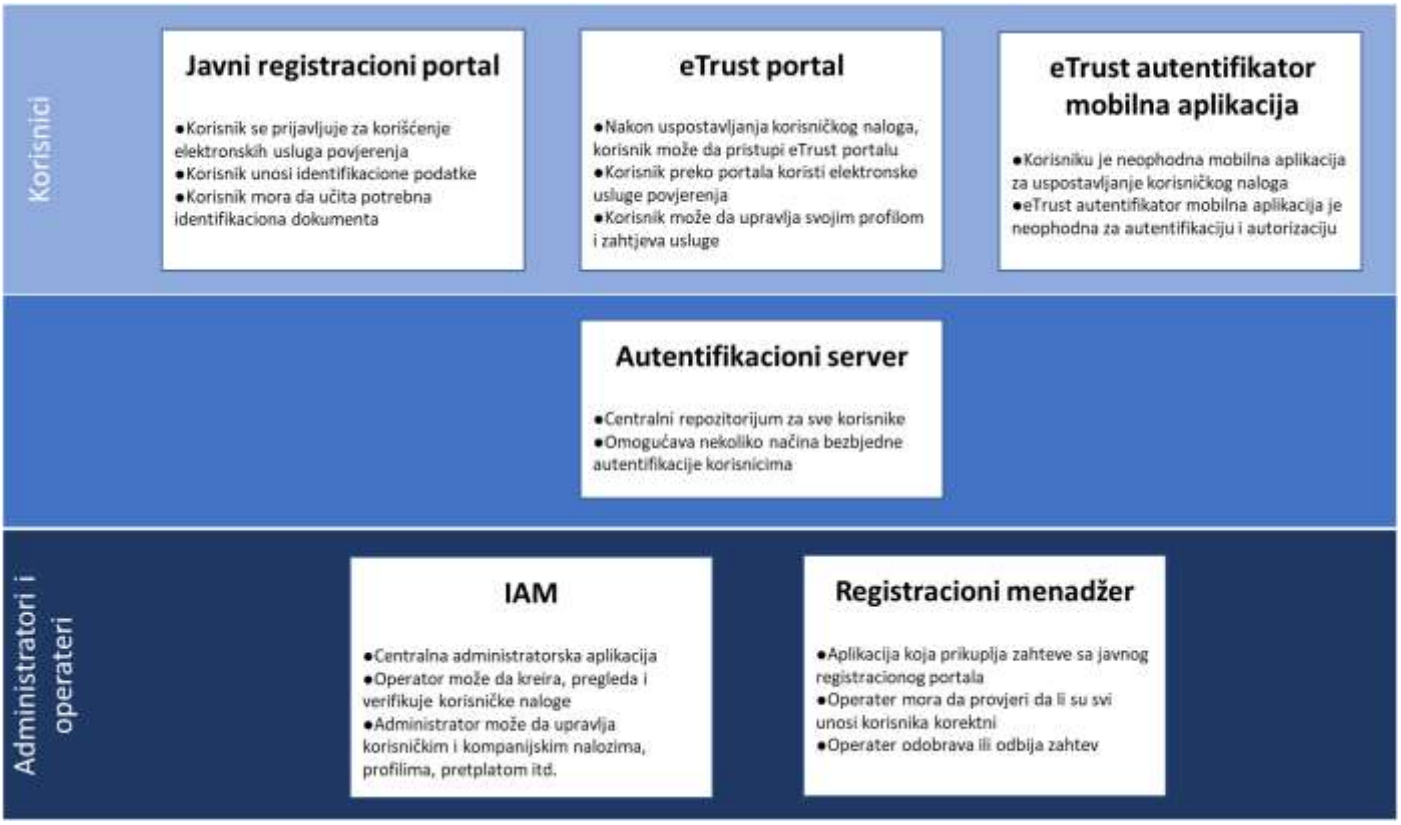
Notification Manager je komponenta sistema odgovorna za prosljeđivanje sistemskih notifikacija krajnjim korisnicima. Ova komponenta se koristi za autentifikaciju krajnjih korisnika koji pristupaju sistemu, kao i za autorizaciju digitalnih transakcija od strane krajnjih korisnika preko mobilnog telefona,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

- **FE (Front End) aplikacije**

FE aplikacije čine aplikativne komponente koje koriste krajnji korisnici, administratori i operateri sistema i one su detaljnije opisane u tački 1.4.2.

1.4.2. Aplikativne komponente

Dijagram na slici 2. prikazuje glavne aplikacije koje omogućavaju korišćenje kvalifikovane usluge elektronske preporučene dostave.



Slika 2. – Aplikativne komponente kvalifikovane usluge elektronske preporučene dostave

- Javni registracioni portal – Aplikativna komponenta kojom se krajnji korisnik prijavljuje za korišćenje kvalifikovanih elektronskih usluga povjerenja, unosi lične informacije i učitava potrebna identifikaciona dokumenta. Na osnovu uvida i provjere identifikacionih podataka, krajnjem korisniku se odobrava ili odbija zahtjev za korišćenje kvalifikovanih elektronskih usluga povjerenja.

- Autentifikacioni Server – Centralni repozitorijum koji sadrži sve krajnje korisnike. Autentifikacioni server predstavlja mehanizam autentifikacije i omogućava nekoliko načina bezbjedne autentifikacije krajnjim 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 krajnjeg korisnika da autorizuje transakcije. eTrust Autentifikator mobilna aplikacija prima *push* notifikacije, obavještava krajnjeg korisnika i omogućava mu da autorizuje digitalnu transakciju.

- eTrust portal – Aplikaciona komponenta pomoću koje krajnji korisnik upravlja svojim profilom i zahtijeva, odnosno koristi kvalifikovane elektronske usluge povjerenja. eTrust portal je dio Front Office-a i predstavlja centralno mjesto koje sadrži svu poslovnu logiku za korišćenje kvalifikovanih elektronskih usluga povjerenja.

- IAM – Identity and Access Management (IAM) – Ključna komponenta koja čuva informacije o krajnjim 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 nalozima krajnjih korisnika i vodi računa o njihovoj pretplati, odnosno o upravljanju njihovim računima.

- Registracioni menadžer – Ključna operatorska komponenta za upravljanje korisničkim registracionim procesom. Ova komponenta obezbjeđuje operatorima sistema funkcije koje su neophodne za registraciju i upravljanje nalozima krajnjih korisnika. Registracioni menadžer je dio Back office sistema, koji nudi i funkcionalnosti potpisivanja ugovora i verifikovanja identiteta krajnjih korisnika. Content Manager i Document Management System su, takođe, djelovi Back office-a i koriste se za omogućavanje kvalifikovane usluge elektronske preporučene dostave.

1.5. Administracija dokumenta

1.5.1. Organizacija koja upravlja dokumentom

CTrust PMA u ime CT-a periodično pregleda i ažurira ovaj dokument u skladu sa promjenama odredbi u zakonskoj regulativi ili drugim relevantnim 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 za pružanje kvalifikovane usluge elektronske preporučene dostave 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 dokumenta

Ovaj dokument CT-a se periodično 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, ovaj 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
Arhiva	Specifična baza podataka za čuvanje zapisa za određeni period vremena u cilju bezbjednosti, backup-a ili revizije.
Autentifikacija	Elektronski postupak koji omogućava potvrđivanje elektronske identifikacije fizičkog ili pravnog lica ili porijekla i integriteta podataka u elektronskom obliku.
Autorizacija	Procedura utvrđivanja prava koje neki autentifikovani korisnik ima za korišćenje odgovarajuće aplikacije ili servisa.
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.
eDelivery	Kvalifikovana usluga elektronske preporučene dostave
eng. Policy Managment Authority	Upravljačko tijelo CTrust-a
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.
Interoperabilnost	Interoperabilnost je sposobnost dva ili više sistema elektronske preporučene dostave ili njihovih komponenti da razmjenjuju podatke i omoguće zajedničku upotrebu podataka i znanja.
Korisnički ugovor	Ugovor između krajnjeg korisnika i CT-a u cilju pružanja kvalifikovane usluge elektronske preporučene dostave.
Korisnik	Fizičko ili pravno lice koje se oslanja na elektronsku identifikaciju ili elektronsku uslugu povjerenja.
Krajnji korisnik	Korisnik koji je pošiljalac/primalac elektronske preporučene dostave.
Kvalifikovana usluga elektronske preporučene dostave	Kvalifikovana usluga elektronske preporučene dostave je usluga koja omogućava prenos podataka pomoću elektronskih sredstava i pruža dokaz o postupanju sa prenesenim podacima, uključujući dokaz o slanju i prijemu podataka, čime se preneseni podaci štite od rizika gubitka, krađe, oštećenja ili bilo kakvih neovlašćenih prepravki i ispunjava uslove definisane članom 31 Zakona o elektronskoj identifikaciji i elektronskom potpisu.
Lični identifikacioni podaci	Skup podataka u elektronskom obliku koji omogućavaju da se utvrdi identitet fizičkog ili pravnog lica.
Mobilna aplikacija (eTrust autentifikator)	Mobilna aplikacija je važan bezbjednosni element sistema, koji pruža dodatni nivo bezbjednosti uzimajući učešće u mehanizmu autentifikacije i zahtijevajući od krajnjeg korisnika da autorizuje transakcije.
Naručilac	Naručilac može biti fizičko ili pravno lice koje snosi punu odgovornost koja proističe iz upotrebe elektronske usluge povjerenja.
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 registraciju zahtjeva za kvalifikovanu uslugu elektronske preporučene dostave. 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 davaoca usluge.

Treće lice	Treća lica su fizička lica i poslovni subjekti (kompanije, korporacije, ustanove i dr.) koja se pouzdaju u kvalifikovanu uslugu elektronske preporučene dostave.
Workflow	Redosljed industrijskih, administrativnih ili drugih procesa kroz koje dio posla prolazi od početka do završetka. Proces rada.

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/izdavanja sredstva elektronske identifikacije
OA	Operations Authority – Tijelo za operativne poslove
RA	Registration Authority – Registraciono tijelo
ID	Identification document – Identifikacioni dokument
OID	Object IDentifier
OTP	One Time Password – Lozinka koja se može iskoristiti samo jednom.
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
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
B	Basic Signature – Elektronski potpis koji se može verifikovati sve dok odgovarajući sertifikati nijesu opozvani ili istekli.
B-T	Signature with Time – Elektronski potpis koji dokazuje da je potpis postojao u datom trenutku vremena.
B-LT	Signature with Long-Term Validation Material – Elektronski potpis koji obezbjeđuje dugoročnu dostupnost materijala za verifikaciju tako što uključuje sav materijal ili reference na materijal potreban za verifikaciju potpisa.
B-LTA	Signature providing Long Term Availability and Integrity of Validation Material – Elektronski potpis koji cilja na dugoročnu dostupnost i integritet materijala za verifikaciju elektronskih potpisa i može pomoći da se izvrši verifikacija potpisa bez obzira na događaje koji ograničavaju njegovu validnost (npr. slabost kriptografskog algoritma koji je korišćen, isteklost verifikacionih podataka itd.).

2. Registracija korisnika

2.1. Podnošenje zahtjeva i registracija korisnika

Krajnji korisnik može podnijeti zahtjev na dva načina:

1. popunjavanjem online registracione forme (fizičko lice),
2. dolaskom u CT poslovnicu (fizičko lice, pravno lice).

Fizičko lice podnosi zahtjev lično, popunjavanjem online registracione forme ili dolaskom u CT poslovnicu, dok za pravno lice zahtjev podnosi ovlašćeno lice pravnog lica dolaskom u CT poslovnicu.
Prilikom obrade zahtjeva isti se odobrava ili odbija. Tokom procesa obrade zahtjeva vrši se provjera identiteta.

Zahtjev mogu podnijeti fizička lica koja imaju prebivalište ili boravište u Crnoj Gori i pravna lica registrovana u Crnoj Gori.
Prilikom podnošenja zahtjeva podnosilac treba da se upozna sa uslovima koji su povezani sa korišćenjem kvalifikovane usluge elektronske preporučene dostave i sa preporučenim sigurnosnim mjerama opreza 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 pravnog lica,
- PIB,
- sjedište pravnog lica.

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

2.1.1. Proces obrade zahtjeva i odgovornosti

CTrust pruža kvalifikovane elektronske usluge povjerenja tek nakon provjere identiteta krajnjih korisnika i uspješnog završetka procesa registracije. Da bi krajnji korisnik mogao da koristi uslugu kvalifikovane elektronske preporučene dostave potrebno je da ima kreiran nalog na eTrust sistemu (eTrust korisnički nalog). Glavni koraci u procesu obrade zahtjeva su opisani u tačkama 2.1.1.1. (za fizičko lice) i 2.1.1.2. (za pravno lice).

2.1.1.1. Obrada zahtjeva za fizičko lice

Korišćenje kvalifikovane usluge elektronske preporučene dostave od strane fizičkog lica podrazumijeva dodjelu eTrust korisničkog naloga za pristup sistemu fizičkom licu koje će imati pristup svom prijemnom/otpremnom sandučetu.

1) Ukoliko je zahtjev podnijet online:
- Krajnji korisnik popunjava obrazac za prijavu putem web aplikacije u sklopu kojeg prilaže i skenirana lična identifikaciona dokumenta koja su opisana u tački 2.2. i prihvata Ponudu i uslove korišćenja eTrust usluga (fizička i pravna lica).
- Ovako popunjen zahtjev se prosljeđuje službeniku za registraciju na provjeru i odobrenje.
- Nakon uvida u priloženu dokumentaciju i provjere tačnosti unesenih podataka iz on-line zahtjeva operater odobrava zahtjev.
- eTrust sistem na e-mail krajnjeg korisnika koji je unesen u zahtjevu šalje personalizovani link za podešavanje eTrust korisničkog naloga. Link je aktivan 24 sata od trenutka prijema elektronskom poštom. Preduslov za podešavanja eTrust korisničkog naloga je da krajnji korisnik ima instaliranu eTrust autentifikator mobilnu aplikaciju na mobilnom uređaju.
- Krajnji korisnik slijedi dostavljeni link i, u prvom koraku, pomoću eTrust autentifikator mobilne aplikacije skenira QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim krajnji korisnik generiše lozinku za eTrust korisnički nalog i isti aktivira putem eTrust autentifikator mobilne aplikacije. Ovim korakom se završava aktivacija eTrust autentifikator mobilne aplikacije i eTrust naloga krajnjeg korisnika, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju i krajnji korisnik se upućuje da se loguje na eTrust korisnički portal https://etrust.telekom.me.
- Krajnji korisnik se zatim upućuje u poslovnicu Crnogorskog Telekoma radi provjere identiteta.

- Kada RA operater uvidom u lična dokumenta krajnjeg korisnika uspješno provjeri identitet, i krajnji korisnik potpiše ugovor (svojeručno u poslovnici ili korišćenjem usluge udaljenog kvalifikovanog elektronskog potpisa) tada mu se aktivira usluga kvalifikovane elektronske preporučene dostave. Aktivacijom ove usluge korisnik logovanjem na eTrust portal pomoću dodijeljenog eTrust korisničkog naloga može pristupiti sandučetu za prijem i otpremu pošiljke.

2) Ukoliko je zahtjev podnesen preko RA operatera:

- Krajnji korisnik prilikom podnošenja zahtjeva za prijavu prihvata Ponudu i uslove korišćenja eTrust usluga (fizička i pravna lica).
- Prilikom predaje zahtjeva RA operateru krajnji korisnik prilaže valjan identifikacioni dokument kao što je opisano u tački 2.2. Potpisivanje ugovora se može obaviti svojeručno u poslovnici ili korišćenjem usluge udaljenog kvalifikovanog elektronskog potpisa.
- RA operater (službenik za registraciju) unosi korisničke podatke u eTrust sistem zajedno sa skeniranom priloženom dokumentacijom i provjeri identitet krajnjeg korisnika.
- RA operater aktivira uslugu kvalifikovane elektronske preporučene dostave pri čemu, nakon potvrde identiteta, takođe počinje i proces kreiranja eTrust korisničkog naloga
- eTrust sistem na e-mail krajnjeg korisnika koji je unesen u zahtjevu šalje personalizovani link za podešavanje eTrust korisničkog naloga. Link je aktivan 24 sata od trenutka prijema elektronskom poštom. Preduslov za podešavanje eTrust naloga je da krajnji korisnik ima instaliranu eTrust autentifikator mobilnu aplikaciju na mobilnom uređaju.
- Krajnji korisnik slijedi dostavljeni link i, u prvom koraku, pomoću eTrust autentifikator mobilne aplikacije skenira QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim krajnji korisnik generiše lozinku za eTrust korisnički nalog i isti aktivira putem eTrust autentifikator mobilne aplikacije. Ovim korakom se završava aktivacija eTrust autentifikator mobilne aplikacije i eTrust naloga krajnjeg korisnika, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju i krajnji korisnik se upućuje da se loguje na eTrust korisnički portal https://etrust.telekom.me.
- Logovanjem na eTrust korisnicki portal krajnji korisnik dobija pristup sandučetu za prijem i otpremu sadržaja putem kvalifikovane elektronske dostave.

2.1.1.2. Obrada zahtjeva za pravno lice

Korišćenje kvalifikovane usluge elektronske preporučene dostave od strane pravnog lica podrazumijeva da zaposleni posjeduje eTrust korisnički nalog za pristup sistemu i da pravno lice navede koji sve eTrust korisnički nalozi treba da imaju pristup prijemnom/otpremnom sandučetu pravnog lica.
Da bi pravno lice imalo definisano svoje prijemno/otpremno elektronsko sanduče, zahtjev se podnosi preko RA operatera po sljedećoj proceduri:

- Ovlašćeno lice pravnog lica podnosi zahtjev za prijavu i prihvata Ponudu i uslove korišćenja eTrust usluga.
- Prilikom predaje zahtjeva RA operateru ovlašćeno lice pravnog lica prilaže valjana identifikaciona dokumenta pravnog lica kao što je opisano u tački 2.3. Potpisivanje ugovora vrši ovlašćeno lice pravnog lica svojeručno u poslovnici ili korišćenjem usluge udaljenog elektronskog potpisa.
- RA operater (službenik za registraciju) unosi korisničke podatke u eTrust sistem zajedno sa skeniranom priloženom dokumentacijom i provjeri identitete pravnog lica i ovlašćenog lica pravnog lica i aktivira uslugu kvalifikovane elektronske preporučene dostave.
- RA operater može da dodijeli ovlašćenom licu pravnog lica ulogu administratora za to pravno lice, ukoliko je to definisano u zahtjevu. Prilikom dodjeljivanja uloge administratora, RA operater može definisati novog krajnjeg korisnika, ili izabrati jednog od postojećih, ukoliko je to lice već korisnik (posjeduje eTrust korisnički nalog) eTrust sistema.
- Nakon potvrde identiteta pravnog lica i administratora, započinje se proces kreiranja korisničkog naloga, ukoliko administrator nije već korisnik eTrust sistema.

- eTrust sistem na e-mail administratora koji je unesen u zahtjevu šalje personalizovani link za podešavanje eTrust korisničkog naloga. Link je aktivan 24 sata od trenutka prijema elektronskom poštom. Preduslov za podešavanja eTrust naloga je da administrator ima instaliranu eTrust autentifikator mobilnu aplikaciju na mobilnom uređaju.
- Administrator slijedi dostavljeni link i, u prvom koraku, pomoću eTrust autentifikator mobilne aplikacije skenira QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim administrator generiše lozinku za eTrust korisnički nalog i isti aktivira putem eTrust autentifikator mobilne aplikacije. Ovim korakom se završava aktivacija eTrust autentifikator mobilne aplikacije i eTrust naloga, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju i administrator se upućuje da se loguje na eTrust korisnički portal https://etrust.telekom.me.
- RA operater ili Administrator (ukoliko je definisan) kreira prijemno/otpremno sanduče pravnom licu, a može da doda i dodatne unutrašnje organizacione jedinice pravnog lica i kreira prijemne/otpremne sandučiće za njih. Kreiranje prijemnog/otpremnog sandučeta podrazumijeva:
    - definisanje naziva odjeljenja koje koristi to sanduče,
    - pridruživanje jedinstvene e-mail adrese tom odjeljenju (radi dobijanja notifikacija o elektronskoj preporučenoj dostavi) kao i
    - pridruživanje članova (zaposleni unutar kompanije) koji imaju pristup tom sandučetu. Članovi moraju imati već kreiran eTrust nalog kako bi mogli pristupiti sandučetu odgovarajućeg odjeljenja pravnog lica.

Ukoliko članovi nemaju kreiran korisnički nalog, dodjela istog se obavlja na sljedeći način:

- Zaposleni podnosi zahtjev za kreiranje eTrust korisničkog naloga online ili preko RA operatera.

1) Ukoliko je zahtjev podnijet online:

- Zaposleni popunjava obrazac za prijavu putem web aplikacije u sklopu kojeg prilaže i skenirana lična identifikaciona dokumenta koja su opisana u tački 2.2. i prihvata Ponudu i uslove korišćenja eTrust usluga (fizička i pravna lica).
- Ovako popunjen zahtjev se prosljeđuje službeniku za registraciju na provjeru i odobrenje.
- Nakon uvida u priloženu dokumentaciju i provjere tačnosti unesenih podataka iz on-line zahtjeva operater odobrava zahtjev.
- eTrust sistem na e-mail koji je unesen u zahtjevu šalje personalizovani link za podešavanje eTrust korisničkog naloga. Link je aktivan 24 sata od trenutka prijema elektronskom poštom. Preduslov za podešavanja eTrust korisničkog naloga je instaliranje eTrust autentifikator mobilne aplikacije na mobilnom uređaju.
- Zaposleni slijedi dostavljeni link i, u prvom koraku, pomoću eTrust autentifikator mobilne aplikacije skenira QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim generiše lozinku za eTrust korisnički nalog i isti aktivira putem eTrust autentifikator mobilne aplikacije. Ovim korakom se završava aktivacija eTrust autentifikator mobilne aplikacije i eTrust korisničkog naloga, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju.
- Zaposleni se zatim upućuje u poslovnicu Crnogorskog Telekoma radi provjere identiteta.
- Kada RA operater uvidom u lična dokumenta krajnjeg korisnika uspješno provjeri identitet tada je eTrust korisnički nalog spreman za korišćenje.

2) Ukoliko je zahtjev podnesen preko RA operatera:

- Zaposleni prilikom podnošenja zahtjeva za dobijanje eTust korisničkog naloga prihvata Ponudu i uslove korišćenja eTrust usluga (fizička i pravna lica).

- Prilikom predaje zahtjeva RA operateru prilaže se valjan identifikacioni dokument kao što je opisano u tački 2.2. Potpisivanje ugovora se može obaviti svojeručno u poslovnici ili korišćenjem usluge udaljenog kvalifikovanog elektronskog potpisa.
- RA operater (službenik za registraciju) unosi korisničke podatke u eTrust sistem zajedno sa skeniranom priloženom dokumentacijom i provjeri identitet krajnjeg korisnika.
- Nakon potvrđene provjere identiteta započinje se proces kreiranja eTrust korisničkog naloga.
- eTrust sistem na e-mail krajnjeg korisnika koji je unesen u zahtjevu šalje personalizovani link za podešavanje eTrust korisničkog naloga. Link je aktivan 24 sata od trenutka prijema elektronskom poštom. Preduslov za podešavanje eTrust naloga je da krajnji korisnik ima instaliranu eTrust autentifikator mobilnu aplikaciju na mobilnom uređaju.
- Krajnji korisnik slijedi dostavljeni link i, u prvom koraku, pomoću eTrust autentifikator mobilne aplikacije skenira QR kod dostavljen od strane web aplikacije na koju upućuje pomenuti link, kako bi se inicirao OTP generator. Zatim krajnji korisnik generiše lozinku za eTrust korisnički nalog i isti aktivira putem eTrust autentifikator mobilne aplikacije. Ovim korakom se završava aktivacija eTrust autentifikator mobilne aplikacije i eTrust naloga krajnjeg korisnika, kao i postavljanje parametara za dvofaktorsku (korisničko ime/lozinka, OTP) autentifikaciju i eTrust korisnički nalog je spreman za korišćenje.

2.2. Provjera identiteta fizičkog lica

Fizičko lice će biti identifikovano licem u lice. Pojedinci moraju da se identifikuju koristeći jedan od sljedećih važećih identifikacionih dokumenata, izdatih od strane odgovarajućeg državnog organa:

- Lična karta (u slučaju domaćeg državljanina);
- Pasoš (u slučaju stranog državljanina);
- Boravišna dozvola (u slučaju stranog državljanina).

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, 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:

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

2.3. Provjera identiteta pravnog lica

Ovlašćeno lice pravnog lica mora da dostavi identifikaciona dokumenta za pravno lice koje zastupa. U tu svrhu neophodno je dostaviti sljedeća dokumenta:

- Ovlašćenje za zastupanje pravnog lica;
- Original ili ovjerena kopija zvaničnih dokumenata koji pružaju dokaz o identitetu pravnog lica – rješenje, 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. Prihvata se i kopija rješenja, odnosno izvoda o registraciji iz CRPS-a, s tim što se u tom slučaju podaci moraju verifikovati kod ovlašćenog nadležnog organa koristeći postojeće servise u realnom vremenu, iz koga se mogu utvrditi:

- naziv pravnog lica,
- PIB,
- sjedište pravnog lica.

Ovlašćeno lice pravnog lica će biti identifikovano licem u lice koristeći jedan od sljedećih važećih identifikacionih dokumenata, izdatih od strane odgovarajućeg državnog organa:

- Lična karta (u slučaju domaćeg državljanina);
- Pasoš (u slučaju stranog državljanina);
- Boravišna dozvola (u slučaju stranog državljanina).

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, a koji se ne nalaze na identifikacionom dokumentu.

U cilju ispunjenja zahtjeva definisanih Pravilnikom [3] definiše se minimalni skup podataka o identitetu ovlašćenog 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:

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

3. Kvalifikovana usluga elektronske preporučene dostave

Kvalifikovana usluga elektronske preporučene dostave podliježe zakonskoj regulativi i standardima. Mapiranje relevantnijih zahtjeva sa opisima ispunjenosti istih dat je u tabeli Tabela 1.

Opis zahtjeva	**Regulatorni okvir**	**Opis ispunjenosti (poglavlja u dokumentu)**
Cjelovitost podataka	Član 30. Stav 1) tačka 1) [1] Član 31. Stav 1) tačka 4) [1]	3.3. Integritet sadržaja poruke korisnika
Slanje podataka od strane identifikovanog pošiljaoca	Član 30. Stav 1) tačka 2) [1] Član 31. Stav 1) tačka 2) [1] Član 2. i 4. [5]	3.2. Procedura vršenja kvalifikovane usluge elektronske preporučene dostave 3.4. Autentifikacija korisnika
Prijem podataka od strane identifikovanog primaoca	Član 30. Stav 1) tačka 3) [1] Član 31. Stav 1) tačka 3) [1] Član 2. 3. i 4. [5]	3.2. Procedura vršenja kvalifikovane usluge elektronske preporučene dostave 3.4. Autentifikacija korisnika

Tačnost datuma i vremena slanja i prijema podataka	Član 30. Stav 1) tačka 4) [1] Član 31. Stav 1) tačka 6) [1] Član 4. [5]	3.5. Obezbjeđivanje kvalifikovanih elektronskih vremenskih pečata
Dokaz o slanju i primanju podataka	Član 4. Stav 1) tačka 1) [5]	3.6. Evidencija događaja
Prikupljanje i čuvanje podataka	Član 4. Stav 1) tačka 2) [5]	3.6. Evidencija događaja

Tabela 1. Matrica kompatibilnosti regulatornih zahtjeva i opisa ispunjenosti istih

3.1. Identifikacija usluge

Identifikaciona oznaka (OID) za kvalifikovanu uslugu elektronske preporučene dostave po ovim Pravilima je: 1.3.6.1.4.1.56393.1.6.1.1

3.2. Procedura vršenja kvalifikovane usluge elektronske preporučene dostave

CTrust obezbjeđuje kvalifikovanu uslugu elektronske preporučene dostave samo svojim krajnjim korisnicima koji su registrovani za pomenutu uslugu. Na CTrust repozitorijumu (https://telekom.me/ctrust) se nalazi dokument – Korisničko uputstvo za korišćenje kvalifikovane usluge elektronske preporučene dostave.
Kvalifikovana usluga elektronske preporučene dostave vrši se preko sistema za upravljanje dokumentima (eng. *Document Management System* – DMS), u kome korisnik može da koristi i druge kvalifikovane elektronske usluge povjerenja (elektronsko potpisivanje, elektronsko pečatiranje, izrada elektronskog vremenskog pečata) uz kvalifikovanu uslugu elektronske preporučene dostave. Procedura pružanja kvalifikovane usluge elektronske preporučene dostave se odvija na sljedeći način:

- Krajnji korisnik se autentifikuje na eTrust portal dvofaktorskom autentifikacijom na način opisan u tački 3.4.
- Nakon autentifikacije, krajnji korisnik pristupa sistemu za upravljanje dokumentima na eTrust portalu, gdje bira opciju „Razmjena dokumenata“ u okviru koje se nalazi prijemno sanduče i drugi folderi u kojima može da pregleda sve dokumente vezane za kvalifikovanu uslugu elektronske preporučene dostave, odnosno da kroz filterske opcije (primljena, poslata, u pripremi, sve, notifikacije) selektuje dokument sa kojim je već radio. Ukoliko želi da pošalje novi dokument korišćenjem kvalifikovane usluge elektronske preporučene dostave, krajnji korisnik bira opciju „Dodaj dokument“.
- Izborom opcije “Dodaj dokument”, otvara se forma „Novi proces za dokument“ i bira opciju „eTrust preporučena dostava“ , koja vodi na formu za unos parametara procesa. Forma za unos parametara procesa sastoji se od sledećih cjelina:
  - Dokumenti, kojom se odabira i učitava dokument sa kojim će se raditi. Dokumenti moraju biti u .pdf formatu.
  - Učesnici, kojom se odabiraju učesnici u komunikaciji i njihove uloge, odnosno akcije koje mogu da odrade na dokumentu (elektronsko potpisivanje, elektronsko pečatiranje,...), rok do kada treba sprovesti akciju, podsjetnik, način i redosljed dostave. Učesnici moraju takođe da budu registrovani korisnici kvalifikovane usluge elektronske peporučene dostave čime se obezbjeđuje pouzdanost identiteta pošiljaoca i primaoca pošiljke.
  - Načina dostave, gdje krajnji korisnik može da odabere jedan od dva načina:
    - upotrebom kvalifikovane usluge elektronske preporučene dostave nakon svake akcije na dokumentu (što zahtijeva rad na samo jednom dokumentu i specificiranje redosljeda učesnika);
    - upotrebom kvalifikovane usluge elektronske preporučene dostave na kraju procesa obrade dokumenta, gdje se dostava vrši nakon svih željenih akcija nad dokumentom i nema ograničenja za broj dokumenata.
  - Podešavanje potpisa (ukoliko je izabrana akcija vezana za elektronsko potpisivanje ili elektronsko pečatiranje), gdje se može podesiti vrsta potpisa (B, B-T, B-LTA), kao i mjesto potpisa na dokumentu.

- Pregled, na kome se vide svi postavljeni parametri procesa.

Ukoliko je krajnji korisnik saglasan sa postavljenim parametrima, on bira opciju „Pokreni pošiljku“, čime se startuje *workflow*, koji ga dalje vodi kroz proces. *Workflow* vizuelno prikazuje status dokumenata nad kojima učesnici treba da izvrše zadate akcije, kao i status procesa.

3.3. Integritet sadržaja poruke korisnika

CTrust u okviru svakog dokaza o slanju i primanju sadržaja poruke korišćenjem kvalifikovane usluge elektronske preporučene dostave, navedenih u tački 3.6., šalje *hash* vrijednost poslatog/primljenog sadržaja poruke. Dokazi o slanju i primanju sadržaja poruke uključujući datum i vrijeme slanja, primanja i eventualne promjene podataka, obezbjeđuju se kvalifikovanim elektronskim pečatom kvalifikovanog davaoca elektronskih usluga povjerenja i ovjeravaju kvalifikovanim elektronskim vremenskim pečatom. Na ovaj način se onemogućava nedetektovana izmjena, odnosno obezbjeđuje integritet sadržaja poruke na prenosnom putu od jednog do drugog korisnika.

3.4. Autentifikacija korisnika

Proces autentifikacije je integralni dio vršenja kvalifikovane usluge elektronske preporučene dostave i zasniva se na sljedećim bezbjednosnim parametrima:

- Autentifikacija je bazirana na korišćenju dva autentifikaciona faktora za povezivanje sa identifikacionim podacima krajnjeg korisnika i 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 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 isti mogu upotrebljavati samo pod kontrolom ili od strane lica kojem pripadaju. 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 dinamički faktor autentifikacije koristi pod kontrolom ili od strane lica kojem pripada, te da je obezbijeđeno od najčešće primjenjivanih napada.

Online autentifikacija predstavlja ključni dio sistema kvalifikovanih elektronskih usluga povjerenja. eTrust portal zahtijeva autentifikaciju od korisnika. Krajnji 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 krajnjem korisniku. Podržana su dva mehanizma bazirana na dvofaktorskoj (korisničko ime/lozinka i OTP) autentifikaciji.

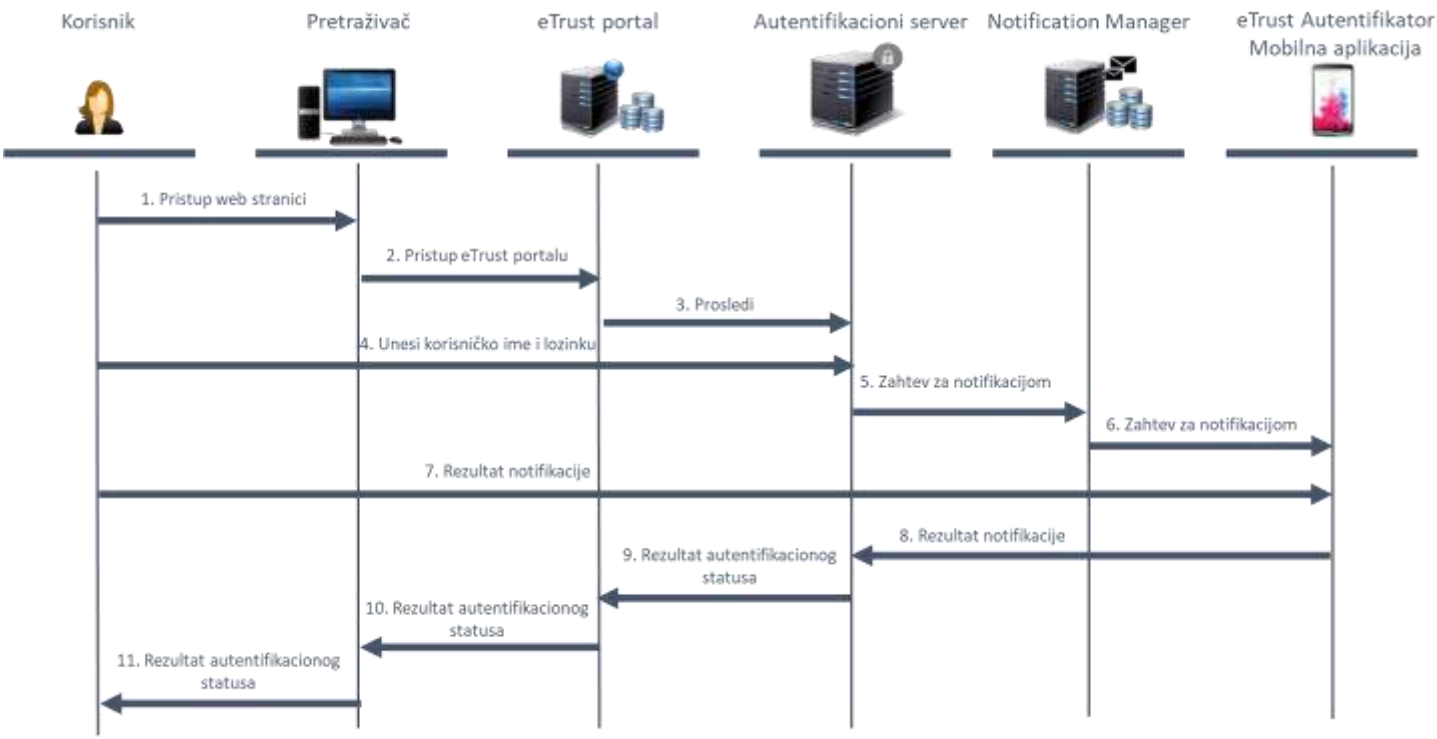
3.4.1. Dvofaktorska (korisničko ime i lozinka, OTP) autentifikacija

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 krajnji korisnik dobija notifikaciju na mobilnoj aplikaciji nakon unošenja korisničkog imena i lozinke na Autentifikacioni server. Krajnji 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 krajnji 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.

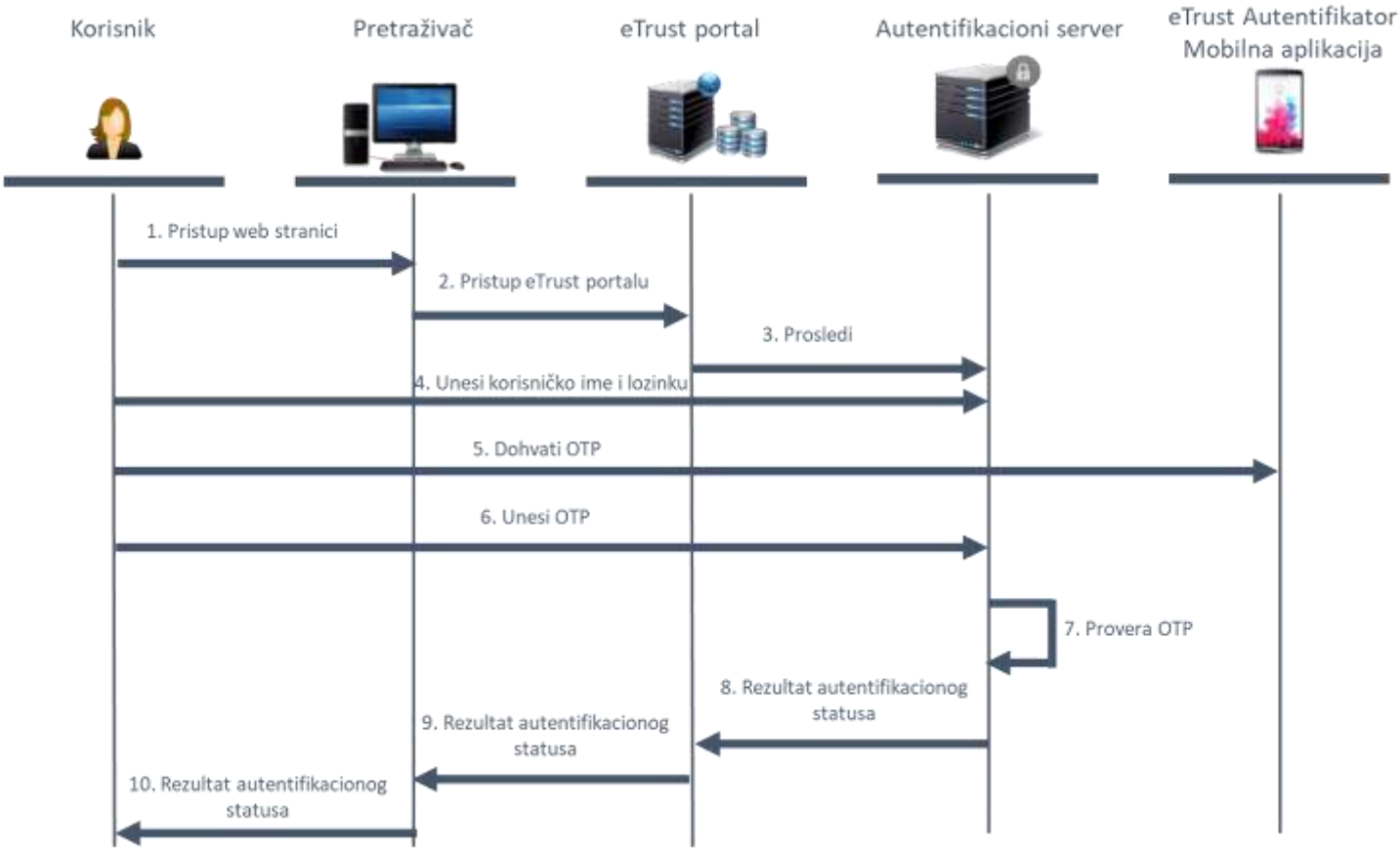
Mobilna notifikacija



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

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

One Time Password (OTP)



Proces autentifikacije putem OTP se može opisati na sljedeći način:

1. Krajnji korisnik preko web pretraživača pristupa eTrust portalu.
2. Ako ne postoji aktivan autentifikacioni token, onda eTrust portal prebacuje korisnika na Autentifikacioni server.
3. Krajnji korisnik unosi korisničko ime i lozinku na Autentifikacioni server.
4. eTrust portal prikazuje web stranicu na kojoj krajnji korisnik može da unese svoj OTP kod. Krajnji korisnik treba da pristupi svojoj mobilnoj aplikaciji kako bi našao OTP kod.
5. Krajnji 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 web pretraživaču.
9. Web pretraživač prikaže poruku greške u slučaju da je krajnji korisnik unio pogrešan OTP kod, ili vodi krajnjeg korisnika na željenu web stranu.

3.5. Obezbjeđivanje kvalifikovanih elektronskih vremenskih pečata

Vrijeme slanja, primanja, preuzimanja, i eventualne promjene podataka, obezbjeđuju se kvalifikovanim elektronskim pečatom kvalifikovanog davaoca elektronskih usluga povjerenja i ovjeravaju kvalifikovanim elektronskim vremenskim pečatom.
CTrust evidentira sve događaje tokom pružanja kvalifikovane usluge elektronske preporučene dostave. Evidentirani događaji navedeni su u tački 3.6.
CTrust zahtijeva slanje dokumenata u propisanom (pdf) formatu i ne vrši promjenu podataka za potrebe slanja ili primanja.

3.6. Evidencija događaja

CTrust razlikuje sljedeće tipove događaja, vezanih za kvalifikovanu uslugu elektronske preporučene dostave:

- Prihvatanje sadržaja elektronske preporučene dostave za slanje od strane davaoca usluga podrazumijeva da davalac usluga prima i prihvata sadržaj elektronske preporučene dostave od jednog krajnjeg korisnika kako bi ga otpremio nekom drugom krajnjem korisniku. Vrijeme prihvatanja predstavlja vrijeme kada je i zadnji bajt sadržaja elektronske peporučene dostave prihvaćen od strane davaoca usluge.
- Slanje sadržaja elektronske preporučene dostave predstavlja isporuku sadržaja elektronske preporučene dostave do prijemnog sandučeta krajnjeg korisnika kome je dostava namijenjena. Vrijeme slanja sadržaja elektronske preporučene dostave predstavlja vrijeme kada je posljednji bajt sadržaja elektronske preporučene dostave upućen sa sistema pružaoca usluge prema prijemnom sandučetu krajnjeg korisnika.
- Obavještenje krajnjem korisniku u vezi prijema elektronske preporučene dostave predstavlja obavještenje kojim se krajnji korisnik upoznaje da za njega postoji elektronska preporučena dostava, te da može da istu primi ili da je odbije. Vrijeme obavještenja je vrijeme kada je krajnjem korisniku sadržaj elektronske preporučene dostave isporučen u njegovo prijemno sanduče.
- Prijem sadržaja elektronske preporučene dostave podrazumijeva da je krajnjem korisniku, kome je dostava namijenjena, isporučen sadržaj elektronske preporučene dostave u njegovom prijemnom sandučetu i krajnji korisnik se eksplicitno izjasnio da li će istu da primi ili odbije. Vrijeme prijema je vrijeme eksplicitnog izjašnjavanja primaoca da prihvata/odbija sadržaj elektronske preporučene dostave.
- Preuzimanje sadržaja elektronske preporučene dostave predstavlja upoznavanje krajnjeg korisnika sa sadržajem elektronske preporučene dostave. Vrijeme preuzimanja je vrijeme kada je sadržaj elektronske preporučene dostave napustio sistem pružaoca usluge i uspješno je predat aplikaciji koju koristi primalac za prikaz sadržaja elektronske preporučene dostave.

CTrust izrađuje sljedeće dokaze o slanju, primanju i preuzimanju podataka prilikom pružanja kvalifikovane usluge elektronske preporučene dostave:

- Potvrdu o prihvatanju sadržaja elektronske proporučene dostave za slanje (od strane pružaoca usluge);
- Obavještenje krajnjem korisniku za prihvatanje elektronske preporučene dostave;
- Potvrdu o slanju sadržaja elektronske proporučene dostave;
- Potvrdu o prijemu sadržaja elektronske preporučene dostave;
- Potvrdu krajnjem korisniku da je rok za prijem sadržaja elektronske preporučene dostave istekao;
- Potvrdu o preuzimanju sadržaja elektronske proporučene dostave.

Svaka od navedenih potvrda mora da sadrži minimalno sljedeći skup podataka:

- Jedinstveni identifikator sadržaja elektronske preporučene dostave koji je dodijelio davalac kvalifikovane usluge elektronske preporučene dostave;
- Naziv davaoca kvalifikovane usluge elektronske preporučene dostave;
- Identifikaciona oznaka (OID) za kvalifikovanu uslugu elektronske preporučene dostave;
- Naziv sadržaja elektronske preporučene dostave;
- Kod i opis akcije koja je izvršena (prihvatanje pošiljke za slanje, slanje, prijem, preuzimanje)
- Metod koji je korišćen za autentifikaciju pošiljaoca i primaoca;
- Elektronske adrese pošiljaoca i primaoca;
- Podatak koji jedinstveno identifikuje sadržaj elektronske preporučene dostave (*hash*);
- Datum i vrijeme kada je akcija izvršena;
- Podatke o pošiljaocu i primaocu:
  1. za fizička lica
     - Ime,
     - Prezime,
     - Identifikacioni broj;

2. za pravna lica
   - Naziv,
   - PIB.

Rok za prijem sadržaja elektronske preporučene dostave je 15 dana od slanja sadržaja elektronske preporučene dostave. Nakon isteka tog roka sadržaj se više neće moći primiti.
CTrust zadržava pravo da u dokaze uvrsti i dodatne podatke, ukoliko su oni iz nekog razloga potrebni i ukoliko je njihovo objavljivanje u skladu sa zakonskom regulativom Crne Gore.
Primarni format potvrde je PDF format, a može biti i formatu XML.
Integritet svake od navedenih potvrda obezbjeđuju se kvalifikovanim elektronskim pečatom kvalifikovanog davaoca elektronskih usluga povjerenja i ovjeravaju kvalifikovanim elektronskim vremenskim pečatom.
CTrust čuva podatke o provjeri identiteta i nivou autentifikacije pošiljaoca i primaoca, kao i podatke o izvršenoj provjeri identiteta pošiljaoca, odnosno primaoca prije izvršene kvalifikovane usluge elektronske preporučene dostave.
Svi dokazi o slanju, primanju i preuzimanju podataka prilikom pružanja kvalifikovane usluge elektronske preporučene dostave se čuvaju u sistemu u periodu od najmanje 10 godina od vremena njihovog nastanka.
Sadržaj elektronske preporučene dostave se čuva na sistemu u periodu od najmanje 45 dana od vremena prihvatanja sadržaja elektronske proporučene dostave.

3.7. Interoperabilnost

CTrust pruža kvalifikovanu uslugu elektronske preporučene dostave samo svojim registrovanim korisnicima.

4. Upravljanje i organizacija

4.1. Objavljivanje internih akata

4.1.1. 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.

4.1.2. Objava informacija o usluzi

Na repozitorijumu su javno objavljeni dokumenti i informacije o pružanju kvalifikovane usluge elektronske preporučene dostave.
Repozitorijum se sastoji od dijela dostupnog na internet stranicama.

4.1.3. Sadržaj repozitorijuma

Na internet stranicama CTrust repozitorijuma objavljuju se:

- Dokument „Praktična pravila rada za pružanje kvalifikovane usluge elektronske preporučene dostave (CTrust eDelivery Certificate Practice Statement – CTrust eDelivery CPS)“;
- Prethodne verzije dokumenata;
- „Ponuda i uslovi korišćenja eTrust usluga (fizička i pravna lica)“ (eng. *Terms and conditions*);
- 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 za korišćenje kvalifikovane usluge elektronske preporučene dostave;
- Cjenovnik;
- Obavještenja krajnjim korisnicima i trećim licima u vezi s kvalifikovanom uslugom elektronske preporučene dostave;
- Ostale informacije vezane za rad CTrust-a.

Objavljeni sadržaj na internet stranicama dostupan je sa adrese https://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.

4.1.4. 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 kvalifikovane usluge elektronske preporučene dostave, 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.

4.1.5. Učestalost objavljivanja podataka

CTrust PMA održava, ažurira, odobrava i objavljuje periodično po potrebi „Praktična pravila rada za pružanje kvalifikovane usluge elektronske preporučene dostave (CTrust eDelivery Certificate Practice Statement – CTrust eDelivery CPS)“.
Drugi dokumenti i ostale relevantne informacije objavljuju se po potrebi.

4.1.6. 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.

4.2. Cjenovnik i obavještavanje korisnika

4.2.1. Cljene pružanja kvalifikovane usluge elektronske preporučene dostave

CT naplaćuje pružanje kvalifikovane usluge elektronske preporučene dostave u skladu sa cjenovnikom. Cijene ovih usluga biće objavljene na javnim internet stranicama repozitorijuma ili web stranici CT-a www.telekom.me.

4.2.2. Politika refundiranja

Troškovi se ne refundiraju.

4.2.3. Finansijska odgovornost

CT snosi finansijsku odgovornost za potencijalnu štetu koja može nastati korišćenjem kvalifikovane usluge elektronske preporučene dostave u skladu sa zakonima koji regulišu ovu oblast.

4.2.4. Pokrivanje osiguranja

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

4.2.5. Ostala sredstva

Nije primjenjivo.

4.2.6. Osiguranje ili garancijsko pokrivanje od strane naručilaca i trećih lica

Naručioci kvalifikovane usluge elektronske preporučene dostave i treća lica koja se pouzdaju u uslugu isključivo su odgovorni da obezbijede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje usluga u okviru njihovih servisa ili aplikacija.

Naručilac je dužan da nadoknadi nastalu štetu koju bi CT mogao da ima kao rezultat nedozvoljenih radnji, kao što su:

- Lažno predstavljanje prilikom registracije korisnika;
- Bilo kog propusta krajnjeg korisnika za koji krajnji korisnik ne može dokazati da je propust nenamjerno učinjen;
- Ako krajnji korisnik ne obezbijedi korišćenje usluge u skladu sa zakonom i ovim dokumentom;
- Ukoliko upotrebom usluge 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.

4.3. 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.

4.3.1. Sigurnosne kontrole računara

4.3.1.1. 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.

4.3.1.2. Rangiranje sigurnosti računara

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

4.3.2. Životni ciklus tehničkih sigurnosnih kontrola

4.3.2.1. Kontrole razvoja sistema

CT nadgleda i kontroliše razvoj sistema za pružanje kvalifikovane usluge elektronske preporučene dostave. 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.

4.3.2.2. Kontrole upravljanja sigurnošću

CT nadgleda i kontroliše sigurnost i upravljanje sigurnošću sistema za pružanje kvalifikovane usluge elektronske preporučene dostave.

4.3.2.3. Životni ciklus sigurnosnih kontrola

CT sprovodi sva testiranja prije implementacije u okviru testnog sajta.

4.3.3. 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.

4.4. 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 kvalifikovane usluge elektronske preporučene dostave, krajnji 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.

4.4.1. Plan privatnosti

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

4.4.2. Informacije koje se tretiraju kao privatne

CT smatra privatnim sve informacije koje se odnose na krajne korisnike kvalifikovane usluge elektronske preporučene dostave.

4.4.3. 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.

4.4.4. 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.

4.4.5. 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.

4.4.6. 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.

4.4.7. Ostale okolnosti kada se mogu otkrivati informacije

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

4.4.8. Prava intelektualnog vlasništva

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

4.5. 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.

4.5.1. 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.

4.5.2. 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.

4.5.3. 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 kvalifikovane usluge elektronske preporučene dostave.
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).

4.5.4. 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.

4.5.5. 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.

4.5.6. 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.

4.5.7. Odlaganje nepotrebnih materijala

Svi mediji i dokumentacija koji više nijesu 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*).

4.5.8. 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.

4.5.9. 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.

4.5.10. Povjerljive uloge

U okviru rada eDelivery sistema 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 realizaciju kvalifikovane usluge elektronske preporučene dostave;
  - Upravlja korisničkim nalozima na operativnom sistemu.
- CA Operator ima sve privilegije i prava pristupa da:
  - Kreira end entity-je (krajnje korisnike kvalifikovane usluge elektronske preporučene dostave);
- 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 pružanje kvalifikovane usluge elektronske preporučene dostave.
- 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 korišćenje kvalifikovane usluge elektronske preporučene dostave;
  - Potvrdu ispravnosti unesenih podataka krajnjih korisnika, odobravanje zahtjeva za korišćenje kvalifikovane usluge elektronske preporučene dostave nakon uspješne potvrde ispravnosti unesenih podataka krajnjih korisnika.

Za potrebe uspostave eDelivery sistema moguće je definisati i dodatne uloge.

4.5.11. 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 eDelivery sistemu 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 eDelivery sistema 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.

4.5.12. Uloge koje zahtijevaju razdvajanje dužnosti

U cilju razdvajanja povjerljivih uloga u eDelivery sistemu prava prijave na sisteme moraju biti dodijeljena u skladu sa tabelom 2.

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 2: Prava prijave na sisteme

4.5.13. Kadrovske bezbjednosne kontrole

4.5.13.1. 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 kvalifikovane usluge elektronske preporučene dostave, 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.

4.5.13.2. Provjera prethodnih angažovanja

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

4.5.13.3. 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 pružanje kvalifikovane usluge elektronske preporučene dostave;
- Postupci oporavka od nezgode i nastavka poslovanja.

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

- Osnovno znanje o kvalifikovanoj elektronskoj preporučenoj dostavi;
- 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.

4.5.13.4. 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.

4.5.13.5. 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.

4.5.13.6. 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*).

4.5.13.7. 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.

4.6. Procedure upravljanja rizicima, zaštita komunikacionih kanala i ostale tehničke kontrole

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 povjerljivosti, cjelovitosti i dostupnosti podataka opisan je u tački 4.6.11.

4.6.1. Tipovi zabilježenih događaja

CTrust sistem zapisuje događaje koji uključuju, ali nijesu ograničeni na evidencije opisane u tački 3.6., pristup sistemu, kao i zahtjeve dostavljene sistemu.

4.6.2. Frekvencija procesiranja logova

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

4.6.3. 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.

4.6.4. Zaštita audit logova

Audit logovi se samo mogu vidjeti od strane autorizovanog osoblja. Integritet audit loga koji nastaje iz softvera korišćenog za pružanje kvalifikovane usluge elektronske preporučene dostave zaštićen je primjenom odgovarajućih kriptografskih metoda.

4.6.5. Procedure backup-a audit logova

CT implementira procedure backup-a audit logova.

4.6.6. Sistem sakupljanja audit logova

CT sakuplja i čuva audit logove u realnom vremenu.

4.6.7. Obavještavanje lica koje je prouzrokovao događaj

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

4.6.8. Procjena ranjivosti sistema

CT periodično organizuje procjenu ranjivosti sistema.

4.6.9. Arhiviranje zapisa/logova

Opšte odredbe koje se odnose na čuvanje logova različitih komponenti sistema za pružanje kvalifikovane usluge elektronske preporučene dostave definisane su ovim poglavljem.

4.6.9.1. Tipovi arhiviranih zapisa

Zapisi koji se čuvaju:

- Zapisi definisani u tački 3.6.;
- Informacije o podnešenim zahtjevima za pružanje kvalifikovane usluge elektronske preporučene dostave;
- I druga potrebna dokumentacija.

4.6.9.2. 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.

4.6.9.3. 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.

4.6.9.4. 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.

4.6.9.5. Zahtjevi za vremenski pečat arhiviranih podataka

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

4.6.9.6. Sistem sakupljanja zapisa

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

4.6.9.7. 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 sigurnim 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.

4.6.10. Kompromitovanje i oporavak sistema poslije nepredviđenih situacija

4.6.10.1. 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.

4.6.10.2. 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.

4.6.10.3. Procedure koje se sprovode kod kompromitacije sistema

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

4.6.10.4. Mogućnosti kontinuiteta poslovanja nakon katastrofe

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

4.6.11. Zaštita povjerljivosti, cjelovitosti i dostupnosti podataka

Podaci o identitetu krajnjih korisnika čuvaju se u bazi podataka davaoca usluge. Sigurnosne kopije baze podataka se vrše redovno i po utvrđenoj proceduri. Pristup podacima o identitetu krajnjih korisnika posredstvom IAM aplikacije imaju samo zaposleni sa povjerljivim ulogama definisani u tabeli 2.

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

Hash vrijednost sadržaja elektronske preporučene dostave koje razmjenjuju korisnici nalazi se u svakoj potvrdi o slanju, primanju i preuzimanju podataka, a sve potvrde su elektronski pečatirane od strane davaoca usluga, što obezbjeđuje nemogućnost nedetektovane izmjene podataka.

Datum i vrijeme slanja, primanja, preuzimanja sadržaja elektronske preporučene dostave na potvrdama se ovjeravaju kvalifikovanim elektronskim vremenskim pečatom.

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

Sve aktivnosti vezane za kvalifikovanu uslugu elektronske preporučene dostave, pristup sistemu, kao i zahtjevi dostavljeni sistemu se bilježe u odgovarajućim audit logovima.

CT je sertifikovan po ISO 27001 standardu.

4.6.12. Završetak rada

U slučaju planiranog prestanka pružanja kvalifikovane usluge elektronske preporučene dostave, 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 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.

4.7. 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 za pružanje kvalifikovane usluge elektronske preporučene dostave vrši inspekcija za usluge informacionog društva, u skladu sa zakonom kojim se uređuje inspekcijski nadzor i Zakonom o elektronskoj identifikaciji i elektronskom potpisu [1].

4.7.1. 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 davaoca kvalifikovanih 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 kvalifikovane 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.

4.7.2. Identitet/kvalifikacije revizora

Provjera saglasnosti rada sistema za pružanje kvalifikovane usluge elektronske preporučene dostave 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.

4.7.3. 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.

4.7.4. Teme pokrivene u procesu procjenjivanja

Provjera usaglašenosti rada eDelivery sistema 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 pruža kvalifikovanu uslugu elektronske preporučene dostave.

4.7.5. Aktivnosti preduzete u slučaju neusaglašenosti

CTrust uskladiće svoj rad sa preporukama i nalazima revizije.

4.7.6. Objavljivanje rezultata

Izvještaji revizije dostavljaju se CTrust PMA.

5. Drugi poslovni i pravni aspekti

5.1. Trajanje i prestanak važenja

5.1.1. Trajanje

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

5.1.2. 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.

5.1.3. Posljedice prestanka važenja i nastavak djelovanja

Nakon prestanka važenja dokumenta, kao rezultata objavljivanja nove verzije dokumenta, kvalifikovana usluga elektronske preporučene dostave će se koristiti u skladu sa verzijom dokumenta koja je bila validna na dan registracije krajnjeg korisnika za pomenutu uslugu. U slučaju promjena okolnosti do nivoa kada ovo nije moguće, CT će obavijestiti krajnje korisnike na način definisan u tački 5.3.2.

5.2. 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 5.3.2.

5.3. Izmjene i dopune

5.3.1. 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.

5.3.2. 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.

5.3.3. Okolnosti pod kojima se OID mora izmijeniti

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

5.4. 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 iz ove oblasti.

5.5. Ostale odredbe

5.5.1. Ugovor o pružanju kvalifikovane usluge elektronske preporučene dostave

Ovaj dokument i „Ponuda i uslovi korišćenja eTrust usluga (fizička i pravna lica)“ i korisnički ugovor sadrže sve elemente koji definišu odnos između CT-a i krajnjih korisnika.
Obaveze koje krajnji korisnik prihvata prilikom potpisivanja korisničkog ugovora:

- Da koristi kvalifikovanu uslugu elektronske preporučene dostave samo za namjene određene u zakonske svrhe;

- Da će poštovati Praktična pravila rada;
- Da će čuvati lozinku za pristup u tajnosti kako bi se spriječilo otkrivanje i neovlašćeno korišćenje, te po tom osnovu snosi svaku odgovornost;
- U slučaju zloupotrebe ili sumnje u zloupotrebu bez odlaganja obavijesti davaoca usluge;
- Da obavijesti davaoca usluge o promjeni ličnih podataka;
- Pruži tačne i pouzdane podatke o svom identitetu, informacije o e-mail adresi (i da joj ima pristup) ili drugim podacima sadržanim u zahtjevu;
- Da obezbijedi internet konekciju radi pristupanja usluzi;
- U postupku provjere identiteta podnosioca zahtjeva isti bude fizički prisutan.

5.5.2. Prenos prava

Krajnjim korisnicima kvalifikovane usluge elektronske preporučene dostave 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.

5.5.3. Klauzula o valjanosti

Nevaljanost jednog ili više djelova ovog dokumenta nemaju uticaj na valjanost ostalih odredbi ovog dokumenta ukoliko nemaju uticaj na materijalne odredbe.

5.5.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava)

Nije primjenjivo.

5.5.5. 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.

5.6. Procedure rješavanja sporova

Svi sporovi u vezi pružanja kvalifikovane usluge elektronske preporučene dostave 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.

Stjepan Udovičić
Izvršni direktor