Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave

Velika Gorica, prosinac 2023.

Informacije o dokumentu

Naziv dokumenta	Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave
Verzija dokumenta	1.3
Status dokumenta	Važeći
Datum donošenja	15/12/2023
OID	**1.3.6.1.4.1.54777.1.1.2**
Tip dokumenta	CPS
Klasifikacija dokumenta	Javno
Vlasnik	HP-Hrvatska pošta d.d., Poštanska 9, 10410 Velika Gorica, OIB: 87311810356, MBS: 080266264 (trgovački sud u Zagrebu)
Kontakt	Ured za optimizaciju, Poštanska 9, 10410 Velika Gorica ePreporuka@posta.hr
Smještaj dokumenta	https://www.eposta.hr/info
Povezani CP	Politika pružanja kvalificirane usluge elektroničke preporučene dostave OID: 1.3.6.1.4.1.54777.1.1.1

Povijest izmjena

Verzija	Datum	Pripremio	Opis izmjene
1.0	01.10.2021.	Igor Ivaštanin	Inicijalna verzija
1.1	01.01.2022.	Igor Ivaštanin	Unesena dodatna pojašnjenja uvjeta pružanja usluge
1.2	20.03.2023.	Marina Zečević	Unesena dodatna pojašnjenja vezana za sinkronizaciju vremena
1.3.	15.12.2023.	Marina Zečević	Promjena organizacije nadležne za administraciju Pravila postupanja

1. Uvod

Dokumentom "Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave" (u nastavku teksta: Pravila postupanja) propisuju se pravila postupanja koje HP – Hrvatska pošta d.d., sa sjedištem u Velikoj Gorici, Poštanska 9, OIB: 87311810356, upisana u registar Trgovačkog suda u Zagrebu, MBS: 080266264, (u nastavku teksta: HP d.d.) primjenjuje u pružanju usluge kvalificirane elektroničke preporučene dostave, u skladu s Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ („electronic IDentification, Authentication and trust Services“, u nastavku teksta: Uredba eIDAS), Zakonom o provedbi eIDAS Uredbe, te podzakonskim aktima i standardizacijskim dokumentima ETSI EN 319 401, ETSI EN 319 521 i ETSI EN 319 522.

HP d.d. je implementirao infrastrukturu za pružanje usluge kvalificirane elektroničke preporučene dostave („qualified electronic registered delivery service“, u daljem tekstu: QERDS) za svoje korisnike.

Kvalificirani elektronički vremenski žig koji HP d.d. koristi u pružanju usluge, eksternaliziran je kod drugog kvalificiranog pružatelja usluga povjerenja koji se nalazi na EU Trusted listi i njime se naznačuju datum i vrijeme slanja, primanja poruka i eventualne promjene podataka.

HP d.d. koristi napredni ili kvalificirani elektronički pečat za pečatiranje poruka elektroničke preporučene dostave kod slanja i primanja poruka, koji se bazira na elektroničkom certifikatu (najmanje prema NCP politici) izdanom od kvalificiranog pružatelja usluga povjerenja i kojim se isključuje mogućnost nezapažene promjene podataka.

Kvalificirani elektronički vremenski žig i najmanje napredni elektronički pečat osigurat će integritet podataka i autentičnost izvora podataka.

Kvalificirane usluge povjerenja su regulirane Zakonom za provedbu Uredbe eIDAS i Uredbom eIDAS, te su ova Pravila postupanja usklađena s navedenom regulativom.

Obuhvat ovih Pravila postupanja je cjelokupna infrastruktura HP-a d.d. koja se koristi za pružanje usluge kvalificirane elektroničke preporučene dostave.

Pravila postupanja će biti objavljena na web stranici https://www.eposta.hr/info.

1.1. Referentna dokumentacija

Temeljni propisi

- Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ
- Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/2017)

- Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)
- Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)

Podredni propisi

- Provedbena uredba komisije (EU) 2015/1505 od 8. rujna 2015. o utvrđivanju tehničkih specifikacija i formata koji se odnose na pouzdane popise u skladu s člankom 22. stavkom 5. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu
- Provedbena uredba komisije (EU) 2016/650 od 25. travnja 2016. utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu
- Provedbena odluka komisije (EU) 2015/1506 od 8. rujna 2015. o utvrđivanju specifikacija koje se odnose na formate naprednih elektroničkih potpisa i naprednih pečata koje priznaju tijela javnog sektora u skladu s člankom 27. stavkom 5. i člankom 37. stavkom 5. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.
- Pravilnik o pružanju i korištenju usluga povjerenja (NN 60/2019)

Normizacijski dokumenti

- ISO/IEC 27001:2013 – Information technology – Security techinques – Information security management
- ISO/IEC 27002:2013 – Information technology – Security techinques – Code of practice for information security management
- ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management
- ETSI EN 319 102-1 V1.1.1. (2016-05) – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 401 V2.2.1. (2021-05) – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2. (2021-05) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2. (2021-05) – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust ServiceProviders issuing certificates; Part 2: Requirements for trust service providers issuing EU Qualified Certificates
- ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522-1 V1.1.1 (2018-09) Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture

1.2. Identifikacijski podaci i OID oznaka

Naziv dokumenta: Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave
OID: 1.3.6.1.4.1.54777.1.1.2
Verzija: 1.3
Datum: 15.12.2023.
Poveznica do dokumenta: https://www.eposta.hr/info

1.3. Administracija Pravila

1.3.1. Organizacija nadležna za administraciju Pravila postupanja

Organizacija nadležna za administraciju Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave:

HP – Hrvatska pošta d.d.
Ured za optimizaciju
Poštanska 9
10410 Velika Gorica
Republika Hrvatska
email: ePreporuka@posta.hr

1.3.2. Postupak donošenja Pravila postupanja

Svaka verzija Pravila postupanja na snazi je sve do trenutka stupanja na snagu nove verzije Pravila postupanja.

Inicijativu za donošenje i inicijativu za izmjene i dopune Pravila postupanja daje Ured za strategiju i razvoj, a izmjene će biti najavljene i izmijenjena Pravila postupanja će biti dostupna u javnom repozitoriju HP-a d.d.

Odgovorne osobe HP-a d.d. nadležne su za usvajanje Pravila postupanja te izmjena i dopuna navedenih Pravila.

HP d.d. provodi redovitu reviziju ovih Pravila postupanja jedanput godišnje.

1.4. Definicije i kratice

1.4.1. Definicije

Aplikacija za uslugu elektroničke preporučene dostave	Sustav sačinjen od hardvera i/ili softvera, koji omogućava pošiljatelju i primatelju sudjelovanje razmjeni podataka s pružateljem usluge elektroničke preporučene dostave

Dokazi usluge elektroničke preporučene dostave	Podaci generirani unutar sustava elektroničke preporučene dostave, koji dokazuju da se određeni događaj u sustavu dogodio u određenom vremenu
Isporuka pošiljke (engl. consignment)	Pružatelj usluge elektroničke preporučene dostave je isporučio korisnički sadržaj unutar eBox QERDS - a primatelja definiranog Općim uvjetima korištenja servisa ePošta.
Javni ključ	Kriptografski ključ nekog korisnika koji je javno dostupan, a zajedno s privatnim ključem omogućuje verifikaciju digitalnog potpisa ili kriptiranje podataka
Koordinirano svjetsko vrijeme (UTC)	Vremenska ljestvica koja se temelji na sekundi kako je definirana ITU-R preporukom TF.460-5. Za većinu primjena u praksi UTC je ekvivalentan srednjem sunčevom vremenu na nultom meridijanu (0°). Točnije, UTC je kompromis između vrlo stabilnog atomskog vremena (Temps Atomique International - TAI) i sunčevog vremena koje se izvodi iz nepravilne rotacije Zemlje (u odnosu na dogovoreno Greenwich srednje zvjezdano vrijeme - GMST).
Korisnički sadržaj	Originalni podaci proizvedeni od pošiljatelja, koji trebaju biti dostavljeni primatelju.
Korisnik	Fizička ili pravna osoba koja koristi usluge povjerenja.
Kvalificirani certifikat za elektronički potpis	Certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I Uredbe eIDAS.
Kvalificirani elektronički vremenski žig	Elektronički vremenski žig koji ispunjava sljedeće zahtjeve: (a) povezuje datum i vrijeme s podacima na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene promjene podataka; (b) temelji se na izvoru točnog vremena povezanim s koordiniranim svjetskim vremenom; i (c) potpisan je pomoću naprednog elektroničkog potpisa ili pečaćen pomoću naprednog elektroničkog pečata kvalificiranog pružatelja usluga povjerenja ili jednakovrijednom metodom.
Kvalificirani pružatelj usluga povjerenja	Pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status.
Kvalificirani pružatelj usluge elektroničke preporučene dostave	Pružatelj usluga povjerenja koji pruža kvalificiranu uslugu elektroničke preporučene dostave
Kvalificirana usluga elektroničke preporučene dostave	Usluga elektroničke preporučene dostave koja ispunjava zahtjeve utvrđene u članku 44. eIDAS Uredbe

Kriptografski modul	Element sustava certificiranja koji ima funkciju generiranja i/ili pohrane ključeva tijekom kriptografskih operacija (engl. *Hardware Security Module*).
Lista kvalificiranih pružatelja usluga	Pouzdani popis davatelja usluga certificiranja koje nadziru/akreditiraju države članice EU (engl. Trusted List)
Lista opozvanih certifikata	Lista opozvanih ili suspendiranih certifikata, a čija dostupnost pouzdajućim sudionicima ili drugim osobama ili sustavima mora biti osigurana (engl. *Certificate Revocation List*).
Napredni elektronički potpis	Elektronički potpis koji pouzdano jamči identitet korisnika i koji: ▪ je povezan isključivo s korisnikom; ▪ nedvojbeno identificira korisnika; ▪ nastaje korištenjem sredstava kojima korisnik može samostalno upravljati i koja su isključivo pod nadzorom korisnika; ▪ sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka.
Opoziv certifikata	Postupak obustave važenja certifikata prije njihova redovitog isteka.
Pouzdajuća strana	Fizička ili pravna osoba koja se oslanja na elektroničku identifikaciju ili uslugu povjerenja.
Povjerljive uloge	Uloge koje se dodjeljuju zaposlenicima i o kojima ovisi sigurnost rada davatelja usluga certificiranja. Povjerljive uloge (engl. Trusted Roles) i pripadne odgovornosti moraju biti jasno određene i opisane u opisu posla djelatnika
Pošiljka	Strukturirani podaci u elektroničkom obliku koje priprema pošiljatelj i namijenjeni su za elektroničku preporučenu dostavu, a sastoje se od korisničkog sadržaja i metapodataka (naziv primatelja, adresu primatelja i sl.).
Pošiljatelj (engl. sender)	Fizička ili pravna osoba koja šalje korisnički sadržaj.
Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave	Pravila postupanja kod pružanja usluge elektroničke preporučene dostave sukladno zahtjevima eIDAS uredbe.
Primatelj (engl. recepient)	Fizička ili pravna osoba na koju je adresiran korisnički sadržaj.
Privatni ključ	Kriptografski ključ nekog korisnika koji je poznat samo korisniku, a zajedno s javnim ključem omogućuje kreiranje digitalnog potpisa ili dekriptiranje podataka.
Pružatelj usluge elektroničke preporučene dostave	Pružatelj usluge povjerenja, koji pruža uslugu elektroničke preporučene dostave

Tijelo za ocjenu sukladnosti	Tijelo ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.
Uručenje pošiljke (engl. handover)	Nakon pouzdane autentifikacije primatelja, korisnički sadržaj je preuzet ili odbijen od primatelja kroz QERDS aplikaciju, ili je sa ili bez autentifikacije primatelja istekao predviđeni rok za uručenje.
Validacija potpisa	Proces verifikacije i potvrde da je elektronički potpis valjan.
Verifikacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.
Usluga elektroničke preporučene dostave	Elektronička usluga, koja omogućava prijenos podataka/pošiljke između pošiljatelja i primatelja, uz osiguravanje dokaza o slanju i primanju podataka i mjera zaštite za smanjenje rizika od gubitka, krađe, uništenja ili neovlaštene promjene podataka.

1.4.2. Kratice

ERDS	Electronic Registered Delivery Service
ERDSP	Electronic Registered Delivery Service Provider
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
NCP	Normalized Certificate Policy
OID	Object Identifier
PKI	Public Key Infrastructure
QERDS	Qualified Electronic Registered Delivery Service
QERDSP	Qualified Electronic Registered Delivery Service Provider
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature Creation Device
TLS	Transport Layer Security
TSP	Trust Service Provider

2. Politike i postupci

2.1. Politika za usluge povjerenja

Politika za usluge povjerenja je Politika pružanja kvalificirane usluge elektroničke preporučene dostave HP-a d.d.

2.2. Pravila postupanja za usluge povjerenja

Pravila su javno dostupna na web stranicama HP-a d.d. i redovito se ažuriraju.
Ova Pravila postupanja adresiraju:

a) način autentifikacije pošiljatelja i primatelja;
b) mjere zaštite za smanjenje rizika od gubitka, krađe, uništenja ili neovlaštene izmjene podataka;

c) ograničenja u korištenju kvalificirane usluge elektroničke preporučene dostave (npr. ograničenja u dostupnosti dokaza);
d) obveze pošiljatelja i primatelja;
e) obveze pouzdajućih strana;
f) informacije za koje događaje u sustavu elektroničke preporučene dostave će se izrađivati dokazi;
g) listu kvalificiranih pružatelja usluga povjerenja koji sudjeluju u pružanju ove usluge (nalaze se u prilogu I ovih Pravila)

Ključne stavke za korisnike nalaze se u Uvjetima pružanja kvalificirane usluge elektroničke preporučene dostave.

2.3. Uvjeti pružanja

Korisnici i HP d.d. zasnivaju ugovorni odnos za kvalificiranu uslugu elektroničke preporučene dostave (u daljnjem tekstu: Ugovor) na način određen Općim uvjetima korištenja servisa ePošta. Ugovor uključuje Zahtjev za korištenjem kvalificirane usluge elektroničke preporučene dostave, Obavijest o prihvatu, Uvjete pružanja kvalificirane usluge elektroničke preporučene dostave (u daljem tekstu: Uvjeti pružanja), sa svim ključnim stavkama kod pružanja usluge i sve druge sastavne dijelove navedene u Općim uvjetima korištenja servisa ePošta.

U postupku sklapanja Ugovora korisnik je upoznat sa svim ograničenjima u korištenju QERDS te obvezama svih strana uključenih u pružanje usluge.

HP d.d. će pohraniti potpisane Ugovore i Uvjete pružanja koji mogu biti i u elektroničkom obliku.

2.4. Politika informacijske sigurnosti

Principi informacijske sigurnosti su opisani u internom aktu Pravilnik o sigurnosti informacijskih sustava.

2.5. Obveze pružatelja QERDS

HP d.d., kao kvalificirani pružatelj usluge povjerenja, odgovoran je za:

- ispravnu identifikaciju korisnika kod ugovaranja usluge,
- pouzdanu autentifikaciju pošiljatelja i primatelja,
- pružanje usluge na siguran način uz osiguravanje autentičnosti, povjerljivosti i integriteta podataka,
- propisno zaštiti osobne podatke,
- provođenje interne i vanjske provjere sukladnosti,
- sukladnost svim propisanim obvezama.

Dodatno, HP d.d. pruža QERDS u skladu s Uredbom eIDAS, Zakonom o provedbi eIDAS Uredbe, te standardizacijskim dokumentima. HP d.d. je odgovoran za upotrebu pouzdane i vjerodostojne

informacijske infrastrukture, koja se koristi za implementaciju kvalificirane usluge elektroničke preporučene dostave.

2.5.1. Obveze korisnika

Korisnici će:

- navesti točne i potpune podatke u zahtjevu za ugovaranjem usluge,
- prihvatiti Uvjete pružanja usluge i druge s njima povezane dokumente,
- čuvati autentifikacijske elemente od gubitka, krađe, oštećenja ili neovlaštene upotrebe,
- dojaviti HP-u d.d. u slučaju nastupanja događaja koji su kompromitirali sigurnost autentifikacijskih elemenata ili u slučaju kada postoji sumnja da je takav događaj nastupio,
- suzdržati se od iskorištavanja eventualnih sigurnosnih propusta ili nepravilnosti u radu sustava HP-a d.d., koje će odmah po utvrđivanju dojaviti HP-u d.d., te
- suzdržati se od prenošenja svojih odgovornosti u radu s kvalificiranom uslugom elektroničke preporučene dostave na treće osobe.
- koristiti se uslugom na zakonit način, u skladu s njezinom dopuštenom svrhom te uz poštivanje primjenjivih propisa.

2.5.2. Obveze pouzdajuće strane

Razumno pouzdanje u kvalificiranu uslugu elektroničke preporučene dostave za pouzdajuću stranu je postignuto ako u trenutku korištenja:

- poduzima neophodne preventivne sigurnosne mjere,
- provjerava napredni/kvalificirani elektronički pečat i kvalificirani elektronički vremenski žig HP-a d.d. korištenjem vjerodostojnih sustava,
- koristi pouzdane aplikacije u sigurnom IT okruženju.

Pouzdajuća strana koja ne postupa sukladno ovim Pravilima postupanja i obvezama koje iz njih proizlaze je sama odgovorna za rizike kod pouzdavanja u napredni/kvalificirani elektronički pečat i kvalificirani elektronički vremenski žig HP-a d.d.

2.6. Ograničenje odgovornosti

Osim onog za što je HP d.d. izričito odgovoran navedeno u poglavlju 9. „Politika pružanja kvalificirane usluge elektroničke preporučene dostave“ i poglavlju 2.5. ovih Pravila, HP d.d. kao pružatelj kvalificirane usluge povjerenja ne odgovora ni za koju drugu obvezu ili odgovornost, posebno ne u slučaju ako bi do odgovornosti HP-a d.d. prema danim obvezama došlo zbog povrede obveza i odgovornosti drugih sudionika navedenih u poglavlju 9. navedenih Politika i poglavlju 2.5. ovih Pravila.

HP d.d. nije odgovoran za štetu, uključujući i neizravnu štetu ili gubitak prihoda, gubitak podataka ili drugih šteta povezanih s kvalificiranim uslugama povjerenja, uzrokovanih korištenjem elektroničke preporučene dostave drugih pružatelja usluga ili korištenjem QERDS HP-a d.d. drugačije od dozvoljenog u ovim Pravilima.

3. Osnovni koncept

3.1. Integritet i povjerljivost korisničkog sadržaja

HP d.d., kao kvalificirani pružatelj usluge povjerenja, pruža uslugu u skladu s Uredbom eIDAS, Zakonom o provedbi eIDAS Uredbe, te standardizacijskim dokumentima, osigurava dostupnost, integritet i povjerljivost korisničkog sadržaja i metapodataka, tijekom prijenosa i u pohrani.

Elektronički dokumenti se štite elektroničkim potpisom/pečatom, podržanim certifikatom izdanim po najmanje ETSI 319 411-1 NCP politici izdanim od kvalificiranog pružatelja usluga povjerenja (QTSP), generiranim na takav način da se onemogući neotkrivena izmjena podataka.

HP d.d. mora provjeravati ispravnost elektroničkog pečata i vremenskog žiga te kvalificiranost QTSP (EU Trust List) na način da periodično provjerava je li kvalificirani pružatelj usluge certificiranja i izdavanja vremenskih žigova na EU Trust listi. Provjera kvalificiranosti obavlja se upitom na EU listu povjerenja. Provjere elektroničkog potpisa i pečata te provjera kvalificiranog elektroničkog vremenskog žiga obavljaju se sukladno normi ETSI EN 319 102.

QERDS podržava potpisivanje pošiljki na dva načina:

- delegirani scenarij – potpis provodi pružatelj usluge,
- scenarij dodatne sigurnosti – potpis provodi pošiljatelj.

3.2. Identifikacija i autentifikacija korisnika

Identifikacija Fizičke osobe kod ugovaranja QERDS obavlja se na sljedeće načine:

1) Osobno kod operatera u poštanskom uredu uz predočenje osobne iskaznice ili putovnice.
2) Udaljenom elektroničkom registracijom, digitalnim potpisom podržanim osobnim certifikatom, koji prihvaća HP izdanim po politikama ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-n ili QCP-n-qscd.

Identifikacija Pravne osobe ili registrirane djelatnosti koju obavlja fizička osoba kod ugovaranja QERDS obavlja se na sljedeće načine:

1) Osobno od strane osobe ovlaštene za zastupanje pravne osobe, ili od strane fizičke osobe koja je nositelj registrirane djelatnosti kod prodajnog predstavnika, uz predočenje osobne iskaznice ili drugog identifikacijskog dokumenta te uz prikupljanje i provjeru podataka o pravnoj osobi ili o registriranoj djelatnosti (puno ime i pravni status, dokaz o postojanju i dokaz o osobi ovlaštenoj za zastupanje, npr. iz nadležnog registra (donošenjem izvatka ili ispisa elektroničkog zapisa iz registra i/ili on-line upitom u registar). U slučaju kada opunomoćena osoba ugovara uslugu za pravnu osobu ili za nositelja registrirane djelatnosti, potrebno je prikupiti i dokaz o punomoći, koji se prilaže uz sam ugovor i na kojem potpis osobe ovlaštene za zastupanje mora biti javnobilježnički ovjeren .
2) Udaljenom elektroničkom registracijom, digitalnim potpisom podržanim poslovnim certifikatom izdanim po politikama ETSI 319 411-1 NCP, ETSI 319 411-2 QCP-l ili QCP-l-qscd.

U svrhu utvrđivanja identiteta fizičkih osoba prikupljaju se sljedeće informacije i dokumenti:

a) Osnovne informacije o osobi subjektu certificiranja i(li) ovlaštenom predstavniku, koje uključuju:
- puno ime i prezime,
- vrsta i broj dokumenta kojim se dokazuje identitet
- OIB ili u slučaju da korisnik ne posjeduje OIB onda drugi nacionalni identifikacijski broj iz identifikacijskog dokumenta,
- adresa prebivališta
- datum rođenja.

b) Zahtijevaju se odgovarajući dokumenti za provjeru imena, identiteta i osnove za izdavanje certifikata.

c) Dokumenti koji se smatraju prihvatljivim dokazima identiteta za izdavanje certifikata fizičkim osobama su:
- osobna iskaznica,
- putovnica.

Nakon uspješne identifikacije, prikupljeni podaci se koriste za registraciju korisnika za QERDS. Registracijom je korisniku sustava dodijeljena sigurna adresa elektroničkog poštanskog sandučića (eBox QERDS). Po završetku registracije i korisnik može koristiti QERDS.

Autentifikacija Fizičke osobe i/ili Pravne osobe kod prijave u sustav za kvalificiranu uslugu provodi se dvofaktorskom autentifikacijom (korisničko ime, lozinka i OTP-jednokratna lozinka dostavljena putem aplikacije mPošta ili preko SMS-a).

Prilikom korištenja mobilne aplikacije za pristup kvalificiranoj usluzi elektroničke preporučene dostave koristiti se pouzdana autentifikacija. Korisnik se u istu prijavljuje svojim PIN brojem, što uz posjedovanje mobilnog uređaja, koje se dokazuje mobilnom aplikacijom ePošta, koja je na siguran način povezana s mobilnim uređajem, i to čini 2-faktorsku autentifikaciju.

Mobilna aplikacija provjerava unesen PIN te:
a) u slučaju tri pogrešna unosa, blokira se na 5 minuta;
b) u slučaju tri naredna pogrešna unosa nakon deblokade, blokira se na dodatnih 5 minuta;
c) u slučaju tri naredna pogrešna unosa nakon druge deblokade, deaktivira se i potrebna je njena ponovna aktivacija.

OTP se generira na serverskoj strani (slučajni broj od 6 znamenaka), na zahtjev korisnika iz mobilne aplikacije ePošta, veže se uz korisnika i vrijedi određeno predefinirano vrijeme. Ako korisnik nema mobilnu aplikaciju ePošta, prilikom prijave u sustav za kvalificiranu uslugu može zatražiti dostavu OTP-a putem SMS poruke.

Detaljan prikaz korištenja mobilne aplikacije ePošta i unos OTP-a generiranog u mobilnoj aplikaciji, prikazani su u dokumentu „eBox eDelivery, Izvedbena dokumentacija“.

3.3. Vremenska referenca

Datum i vrijeme slanja, prijma i bilo koje izmjene nad korisničkim sadržajem označeni su kvalificiranim elektroničkim vremenskim žigom. HP d.d. u ovoj implementaciji koristi eksternaliziranog pružatelja usluge kvalificiranog elektroničkog vremenskog žiga, koji se nalazi na EU Trusted List (europska lista povjerenja). Za navedenog pružatelja usluga se redovito provjerava EU Trusted List. Osim korisničkog sadržaja, kvalificiranim elektroničkim vremenskim žigom označavaju se i svi dokazi u QERDS sustavu (u daljem tekstu: QERDS dokazi).

3.4. Događaji i dokazi

Sustav osigurava QERDS dokaze o prijmu pošiljke, te o isporuci (engl. consignment) i/ili uručenju (engl. handover) pošiljke. QERDS dokazi se štite naprednim/kvalificiranim elektroničkim potpisom/pečatom, podržanim certifikatom izdanim po najmanje ETSI 319 411-1 NCP politici i kvalificiranim elektroničkim vremenskim žigom (PAdES Baseline razine LT ili LTA) generiranim od kvalificiranog pružatelja usluga povjerenja (QTSP).

Dokazi pruženi pošiljatelju identični su u internoj dostavi (blackbox model) i eksternoj dostavi (4-corner model). Pošiljatelju ih isporučuje njegov pružatelj ERDS (S-ERDS), a u eksternoj dostavi izvor dokaza je uglavnom pružatelj ERDS primatelja (R-ERDS). U sljedećoj tablici opisani su događaji kod kojih se pružaju dokazi za pošiljatelja.

Tablica 1. Dokazi za pošiljatelja

Događaj	**Tip događaja**	**Izvor dokaza**	**Pružanje dokaza**
Prijam pošiljke (engl. submission)	Prihvaćen prijam Odbijen prijam	S-ERDS	Obvezno se spremaju dokazi i dostupni su pošiljatelju kroz njegov pretinac.
Isporuka pošiljke u pretinac primatelja (engl. consignment)	Uspješna isporuka Neuspješna isporuka	S-ERDS (BB) R-ERDS (4C)	Obvezno se spremaju dokazi i dostupni su pošiljatelju kroz njegov pretinac.
Uručenje pošiljke primatelju (engl. handover)	Uspješno uručenje Odbijanje uručenja Isteklo vrijeme za uručenje	S-ERDS (BB) R-ERDS (4C)	Obvezno se spremaju dokazi za sve pošiljke, a dostupni su pošiljatelju kroz njegov pretinac samo za pošiljke s povratnicom. Šalje se obavijest s dokazom u pretinac pošiljatelja i na njegovu email adresu, samo za pošiljke s povratnicom. Za pošiljke bez povratnice dokazi o uručenju mogu biti dostupni pošiljatelju na zahtjev.

Osim dokaza za pošiljatelja, postoje i dokazi za pružatelje QERDS u eksternoj dostavi (4-corner model), a događaji kod kojih se isti pružaju opisani su u sljedećoj tablici.

Tablica 2. Dokazi za pružatelja ERDS

Događaj	**Tip događaja**	**Izvor dokaza**	**Pružanje dokaza**
Prijenos (engl. relay)	Prihvaćeno Odbijeno Neuspješno	prijenosni ERDS	Obvezno
Prijenos non-ERDS	Uspješno Neuspješno Primljeno od non-ERDS	prijenosni ERDS	Opcionalno

Semantika QERDS dokaza je u skladu s točkom 8. norme EN 319 522-2.

QERDS dokazi čuvaju se 10 (deset) godina.

Zapisi iz sustava spremaju se na siguran način da osiguraju povjerljivost, integritet i dostupnost podataka. Nije dozvoljeno mijenjanje podataka u zapisima/arhivi.
U zapisima se bilježi:

- Identifikacijske podatke korisnika i logirati i arhivirati sve događaje vezane uz verifikaciju inicijalne i daljnje identifikacije pošiljatelja i primatelja
- Autentifikacijske podatke korisnika
- Dokaz da je identitet pošiljatelja inicijalno provjeren
- Zapise rada ERDS sustava, Provjera identiteta i aktivnosti rada pošiljatelja, primatelja i komunikacije
- Dokaz provjere identiteta primatelja prije prijma ili uručenja pošiljke
- Sredstvo kojim se dokazuje da korisnički sadržaj nije mijenjan tijekom prijenosa
- Sažetak (engl. hash) cjelokupnog korisničkog sadržaja
- Vremenske žigove koji odgovaraju datumu i vremenu prijama, isporuke i uručenja pošiljke.

Dodatno se bilježe i sistemski zapisi:

- Aktivnosti zaposlenika s povjerljivim ulogama u sustavu usluga povjerenja
- Sve sigurnosne događaje, promjene sigurnosne politike, podizanje, zaustavljanje i pad sustava, hardverski problemi, promjene na vatrozidima i ruterima.

Zapisi i arhiva čuvaju se 10 (deset) godina, a dodatno zabilježeni sistemski zapisi 2 (dvije) godine i nakon toga nisu dostupni.

3.5. Interoperabilnost

Za potrebe usklađivanja usluge elektroničke preporučene dostave s eDelivery standardom, u sustav su dodane AP (Access point) i SML (Service Metadata Locator) komponente. SML komponenta je usluga u oblaku, koja je implementirana i održavana od strane odjela za informatiku EU komisije.

eDelivery koncept se temelji na tzv. modelu četiri čvora [engl. four-corner model]. Čvorovi jedan i četiri predstavljaju pozadinske sustave koji ne izmjenjuju poruke izravno nego putem AP komponenti pružatelja usluga predstavljenih čvorovima dva i tri. Pozadinski sustav kroz AP komponente izmjenjuju poruke kroz javnu mrežu na interoperabilni način.

Pružatelj usluge pošiljatelja poziva AP komponentu, koja osigurava pečatiranje pošiljke korištenjem naprednog/kvalificiranog elektroničkog pečata (sukladno ETSI EN 319 102), kvalificiranog vremenskog žiga i enkripciju javnim ključem pružatelja usluge primatelja.

Kod primitka pošiljke, pružatelj usluge primatelja dekriptira pošiljku sa svojim privatnim ključem, provjerava napredni/kvalificirani elektronički pečat javnim ključem pružatelja usluge pošiljatelja i vremenski žig sukladno ETSI normama EN 319 102 i EN 319 421.

Pružatelj usluge primatelja šalje potpisani ERDS dokaz o prijmu pošiljke prema pružatelju usluge pošiljatelja, koji je nakon toga dostupan pošiljatelju.

Kod slanja i prijma pošiljke radi se pouzdana autentifikacija pošiljatelja i primatelja uz uspostavu TLS protokola u prijenosu (enkripcija podataka u prijenosu).

4. Procjena rizika

Procjena rizika za pružanje QERDS obavlja se i dokumentira unutar zasebnog dokumenta „Procjena rizika kod pružanja kvalificirane usluge elektroničke preporučene dostave“.

5. QERDS upravljanje i operacije

5.1. Interna organizacija

U pogledu rizika od odgovornosti za štetu sukladno članku 13. eIDAS Uredbe, HP d.d. raspolaže dostatnim financijskim sredstvima i odgovarajućim osiguranjem od odgovornosti. HP d.d. raspolaže s dostatnim sredstvima i ima financijsku stabilnost za pružanje kvalificiranih usluga povjerenja. HP d.d. ima valjane ugovore sa svim vanjskim tvrtkama, koje su uključene u implementaciju i održavanje sustava za pružanje kvalificirane usluge elektroničke preporučene dostave. Kritične funkcije se provode bazirano na principu “dva para očiju” i pouzdanoj autentifikaciji.

5.2. Nadzor nad radom radnika

Povjerljive uloge predstavljaju osnovu povjerenja za pružanje kvalificirane usluge povjerenja, dodijeljene su autoriziranim i kompetentnim radnicima HP-a d.d. Svaka povjerljiva uloga ima jasno definirane zadatke, obveze i odgovornosti.

Povjerljive uloge uključuju uloge:

- Security Officer – povjerljiva uloga odgovorna za:
    - provođenje sigurnosnih pravila u sustavu za pružanje kvalificiranih usluga povjerenja
    - konfiguraciju pravila izrade dnevničkih i revizijskih zapisa

  - izradu i održavanje ovih Pravila, Politike certificiranja i ostalih dokumenata javno dostupnih
  - upravljanje kriptografskim ključevima
- System Administrator - povjerljiva uloga odgovorna za konfiguraciju i održavanje svih hardverskih i softverskih komponenti sustava za QERDS
- System Operator - povjerljiva uloga odgovorna za provođenje procedura izrade rezervnih kopija i oporavka, upravljanje korisničkim računima u sustavu te nadzor rada komponenti sustava QERDS
- System Auditor - povjerljiva uloga odgovorna za pregled revizijskih zapisa, izvještaja o radu sustava i provođenje internih revizija u sustavu prema ovim Pravilima i Politici pružanja QERDS
- Identity Verification Officer – osigurava da je proces provjere identiteta korisnika u skladu s definicijom u ovim Pravilima i
- Registration officer – povjerljiva uloga odgovorna za provođenje i nadzor procesa registracije korisnika.

Povjerljive uloge dodijeljene su radnicima HP-a d.d. posebnom Odlukom.
Radnicima kojima je dodijeljena uloga Security Officer može biti dodijeljena povjerljiva uloga Identity Verification Officer i nijedna druga.
Radnicima kojima je dodijeljena uloga System Administrator, može biti dodijeljena povjerljiva uloga System Operator i nijedna druga.
Radnicima kojima je dodijeljena uloga System Operator, može biti dodijeljena povjerljiva uloga System Administrator i nijedna druga.
Radnicima kojima je dodijeljena uloga System Auditor, mogu imati isključivo tu povjerljivu ulogu.
Radnicima kojima je dodijeljena uloga Identity Verification Officer može biti dodijeljena povjerljiva uloga Security Officer i nijedna druga.
Radnicima kojima je dodijeljena uloga Registration Officer, mogu imati isključivo tu povjerljivu ulogu.

Zadatke vezane uz pružanje QERDS provode isključivo autorizirani radnici, u dovoljnom broju, znanju, iskustvu i kvalifikacijama. Opisom poslova povjerljivih uloga definirana su obavezna odgovarajuća stručna znanja kandidata za rad s kriptografskim tehnologijama te stručna znanja iz zaštite računalnih sustava i informacijskih sustava. Radnici s povjerljivim ulogama u HP-u d.d. ne mogu biti u radnom ili drugom poslovnom odnosu s drugim pružateljima kvalificiranih usluga povjerenja.

Prije početka rada na poslovima povjerljivih uloga, HP d.d. provodi odgovarajuće provjere kandidata da bi procijenila njihovu sposobnost i pouzdanost u skladu s potrebama poslova povjerljivih uloga. Radnici koji obavljaju poslove povjerljivih uloga u HP-u d.d., kontinuirano se školuju i usavršavaju u skladu s potrebama njihovih povjerljivih uloga te raspolažu dokumentacijom potrebnom za obavljanje aktivnosti sukladno ovlaštenjima dodijeljene povjerljive uloge. Neovlašteni postupci od strane radnika HP-a d.d. s povjerljivim ulogama predstavljaju kršenje obveze iz radnog odnosa sukladno odredbama važeće zakonske regulative i internih pravilnika.

Vanjski partneri, odnosno osobe iz drugih poslovnih subjekata koji obavljaju poslove na temelju ugovora o poslovnoj suradnji, obavljaju svoje funkcije s istim obvezama kao i radnici HP-a d.d. koji izvršavaju funkcije u sustavu te odgovarajućim internim aktima. Obnavljanje obuke izvršitelja povjerljivih uloga iz sustava provodi se u skladu s planovima edukacije radnika HP-a d.d.

5.3. Upravljanje imovinom

Sve komponente sustava za pružanje QERDS jasno su identificirane, popisane i klasificirane prema sigurnosti i poslovnoj važnosti. Mediji koji sadrže arhivske i rezervne podatke sustava u elektroničkom obliku se čuvaju na odvojenoj štićenoj lokaciji s primjerenim sustavima tehničke i tjelesne zaštite. Mediji su primjereno zaštićeni od oštećenja, krađe i neautoriziranog pristupa. Podaci s odbačenih medija se uništavaju na siguran način, elektroničkim brisanjem ili fizičkim uništavanjem medija.

5.4. Kontrola pristupa

Svaka autorizacija pristupa dodjeljuje se kroz kontroliran proces. Principi minimalnih potrebnih prava i segregacija dužnosti se poštuju. Periodično se provjeravaju dodijeljena ovlaštenja. Slojeviti sustavi zaštite povezani s fizičkom i logičkom kontrolom pristupa osiguravaju sigurno odvijanje procesa usluge elektroničkog vremenskog žiga.
Primijenjene mjere zaštite su:

- fizička sigurnost okruženja,
- segregacija dužnosti,
- mrežna segmentacija korištenjem vatrozida,
- nadzor događaja u informacijskom sustavu,
- očvršćivanje konfiguracija komponenti informacijskog sustava.

Sustav za pružanje QERDS logički je odvojen od ostatka IT infrastrukture u HP-u d.d., koristi najmanje logički odvojene mrežne (preklopnike i vatrozide) i poslužiteljske (fizičke i virtualne) sustave te upravljačke konzole.

5.5. Kriptografske kontrole

Certifikat za kvalificirani elektronički pečat pošiljki i QERDS dokaza u sustavu visokog je nivoa sigurnosti prema ETSI 319 411-2 QCP-l-qscd politici, koji je spremljen na sigurnom kriptografskom uređaju (HSM). HP d.d. koristi kriptografske uređaje sukladno standardu FIPS PUB 140-2, level 3 i/ili CC EAL 4+.

Par ključeva za kvalificirani elektronički pečat pošiljki i QERDS dokaza generira se u štićenoj zoni na kriptografskom uređaju uz minimalno dualnu kontrolu ovlaštenih osoba.

Sigurnosne kopije privatnih ključeva se izrađuju u zaštićenoj zoni gdje pristup imaju isključivo ovlaštene osobe. Sigurnosne kopije privatnih ključeva izrađuju ovlaštene osobe i izvan kriptografskog modula (HSM) nalaze se isključivo u enkriptiranom obliku te se čuvaju u zaštićenim zonama na fizički odvojenim lokacijama. Izrađuje se minimalno potrebni broj sigurnosnih kopija ključeva samo za osiguranje kontinuiteta pružanja usluge.

Nakon isteka važenja privatnih potpisnih ključeva, sve kopije ključeva se uništavaju i ne mogu se koristiti.
Uslugu kvalificiranog elektroničkog vremenskog žiga HP d.d. je eksternalizirao kvalificiranom pružatelju usluga povjerenja i njegov status na EU Trusted List redovito provjerava.

5.6. Fizička zaštita opreme i prostora

Pristup u zaštićeni prostor gdje su smještene komponente sustava za pružanje QERDS dopušten je samo ovlaštenim osobama. U slučaju da pristup u ovaj prostor mora biti omogućen osobama zaposlenima kod vanjskih pružatelja usluga, boravak osoba zaposlenih kod vanjskih pružatelja usluga u zaštićenom prostoru mora biti stalno popraćen od zaposlenika HP-a d.d. Svaki ulazak i izlazak iz štićenog prostora se bilježi.
Tehnička i tjelesna zaštita uključuju:

- tjelesnu zaštitu – zaštitare i vatrogasce,
- sustav videonadzora,
- kontrolu prolaza,
- protuprovalni i
- protupožarni sustav.

Pristup i ulazak u zaštićeni prostor nadzire se 24 sata na dan, 7 dana u tjednu.

5.7. Zaštita operacija

HP d.d. ima implementiran sustav informacijske sigurnosti s odgovarajućim sigurnosnim kontrolama koje osiguravaju da su operativni i sigurnosni rizici u granici prihvatljivosti. Te kontrole su:

- Upravljanje operativnim i sigurnosnim rizicima, s ciljem identifikacije i procjene rizika i prepoznavanjem sigurnosnih kontrola za njihovo ublažavanje;
- Upravljanje incidentima, formalna procedura s opisanim koracima za rekaciju na incidente, s ciljem smanjivanja štete i povratka u normalne operacije;
- Upravljanje kontinuitetom poslovanja, kao odgovor na krizne situacije i katastrofe, uz redovito testiranje i ažuriranje Planova kontinuiteta poslovanja;
- Proces upravljanja ranjivostima i prijetnjama – identificirati ranjivosti i prijetnje, te poduzeti aktivnosti za njihovo rješavanje;
- Proces upravljanja promjenama, formalni proces koji osigurava održavanje nivo sigurnosti tijekom promjena u sustavu;
- Nadzor sigurnosnih događaja i informacija (SIEM) – rano otkrivanje neautoriziranog pristupa u informacijski sustav HP d.d.

5.8. Mrežna sigurnost

Sigurnost računalne mreže sustava za pružanje QERDS zasnovana je na konceptu odjeljivanja mreže na mrežne zone različitih razina uz pozicioniranje poslužitelja i ostalih uređaja u različite mrežne zone odvojene vatrozidom i kontrolom pristupa. Mrežne zone odjeljuju se vatrozidima koji propuštaju samo nužan mrežni promet.
Konfiguracijske procedure mrežne opreme osiguravaju:

- upravljanje promjenama,
- ograničavanje pristupa na minimalno potreban i
- prevenciju neautoriziranog pristupa.

Sigurnosne kontrole na mrežnom nivou bazirane su na vatrozidu i uspostavi sigurnog komunikacijskog protokola TLS (Transport Layer Security). Sav mrežni promet je identificiran i odobren. Dodatne sigurnosne kontrole implementirane u sustavu omogućavaju analizu mrežnog prometa i prevenciju upada u mrežu i širenje malware-a.

Periodično i nakon svake značajne promjene u sustavu provodi se penetracijski test mrežne infrastrukture.

5.9. Upravljanje incidentima

Preventivne mjere sigurnosti bazirane na rezultatima procjene rizika mogu smanjiti broj incidenata, međutim nije ih moguće u potpunosti eliminirati. Mogućnost pravovremene i odgovarajuće reakcije na incident je ključna za otkrivanje incidenata, ublažavanje utjecaja i povratka u stanje potpune funkcionalnosti usluga.
Ključni elementi upravljanja incidentima su:

- evaluacija događaja, incidenata i kriznih situacija,
- definiranje nivoa eskalacije,
- uloge u eskalaciji,
- postupci reakcije na incident.

Informacije o sigurnosnim događajima i incidentima su klasificirane.

5.10. Prikupljanje zapisa za QERDS interni servis

Sve komponente sustava za pružanje QERDS konfigurirane su na način da svi događaji relevantni za sigurnost rada sustava i transakcija provedenih na sustavu budu automatski zabilježeni u revizijski zapis. Poslužitelji za prikupljanje revizijskih zapisa nalaze se u štićenoj zoni HP-a d.d.
Sljedeće vrste događaja koje se odnose na pružanje usluge kvalificiranog elektroničkog vremenskog žiga bilježe se u revizijski zapis:

- svi sigurnosni događaji,
- promjene sigurnosne politike,
- podizanje sustava,
- zaustavljanje i pad sustava,
- hardverski problemi,
- promjene na vatrozidima i ruterima.

Vrijeme na svim poslužiteljima iz sustava za pružanje QERDS usluge je sinkronizirano prema UTC (Coordinated Universal Time) vremenu preko centralnog servisa za sinkronizaciju vremena. Uspješnost sinkronizacije vremena provjerava se najmanje jednom dnevno. Revizijski zapisi sustava za pružanje QERDS čuvaju se najmanje 24 (dvadesetčetiri) mjeseca i mogu se koristiti kao dokaz u sudskim postupcima te u slučaju prekida pružanja QERDS. Revizijski zapisi za pružanje QERDS se pregledavaju redovito na dnevnoj osnovi.

5.11. Upravljanje kontinuitetom poslovanja

Za podatke i ključni softver u sustavu za pružanje QERDS redovito se izrađuju rezervne kopije. Rezervne kopije podataka i ključnog softvera se pohranjuju unutar štićene zone HP-a d.d. Povratak podataka i ključnog softvera s rezervnih kopija se redovito testira.

Plan upravljanja kontinuitetom poslovanja za sustav za pružanje QERDS je procedura postupanja u slučaju kriza i kritičnih incidenata, i redovito se testira i ažurira. Kritični poslovni procesi i njihovi parametri oporavka se redovito ažuriraju.

U Plan upravljanja kontinuitetom uključen je i scenarij gubitka, oštećenja ili sumnje na kompromitiranje privatnih ključeva HP-a d.d. za napredni/kvalificirani elektronički pečat i kriptografskih uređaja gdje su spremljeni ti ključevi.

5.12. Prestanak rada QERDSP

O planiranom prestanku pružanja kvalificirane usluge povjerenja HP d.d. će:

- obavijestiti sve korisnike usluge, pouzdajuće strane i nacionalno nadležno tijelo najmanje tri (3) mjeseca prije planiranog prestanka pružanja kvalificiranih usluga povjerenja;
- uložiti napor da analizira mogućnost pružanja kvalificiranih usluga povjerenja kod drugog kvalificiranog pružatelja usluga povjerenja.

Detaljna procedura prestanka pružanje usluge povjerenja propisana je u internom dokumentu „Plan prestanka pružanja usluga povjerenja“.

U slučaju da HP d.d. ne može osigurati pružanje QERDS kod drugog kvalificiranog pružatelja usluga povjerenja, HP d.d. će opozvati certifikate za napredni/kvalificirani elektronički pečat i uništiti povezane privatne ključeve.

U slučaju prestanka obavljanja kvalificirane usluge povjerenja, HP d.d. će nastaviti održavati podatke korisnika koji su prikupljeni u postupku registracije te podatke nastale u radu sustava, koji su nužni za pružanje dokaza u sudskim, upravnim i drugim postupcima u skladu s važećim odredbama zakonske regulative ili će njihovo održavanje ugovoriti s drugim poslovnim subjektom.

5.13. Sukladnost

Nadzor pružanja kvalificiranih usluga povjerenja iz opsega ovih Pravila postupanja provodi nadležno nacionalno tijelo (Ministarstvo gospodarstva i održivog razvoja) sukladno odredbama Uredbe (EU) br. 910/2014 (eIDAS), provedbenih akata donesenih temeljem Uredbe (EU) br. 910/2014 i Zakona o provedbi Uredbe (EU) br. 910/2014.

Vanjske provjere sukladnosti provode se najmanje svake 2 (dvije) godine sukladno Uredbi eIDAS i standardu ETSI EN 319 403.

Redovni nadzor sustava upravljanja informacijskom sigurnosti s ciljem provjere usklađenosti s ISO/IEC 27001 normom vrši se najmanje svakih 12 (dvanaest) mjeseci.

Interne provjere sukladnosti provode se periodično najmanje jednom godišnje, prije pružanja novih kvalificiranih usluga povjerenja, i poslije značajnih promjena u sustavu za pružanje QERDS.
Predmeti ocjenjivanja sukladnosti obuhvaćaju sljedeća područja pružanja kvalificiranih usluga povjerenja:

- cjelovitost i točnost dokumentacije;
- implementiranost zahtjeva za kvalificirane usluge povjerenja;
- organizacijski procesi i procedure;
- tehničke procese i procedure;
- implementirane mjere informacijske sigurnosti;
- vjerodostojne sustave;
- fizičku sigurnost predmetnih lokacija.

Opis predmetnog ocjenjivanja sukladnosti definiran je planom ocjenjivanja sukladnosti.

HP d.d. je u skladu s objektivnim i razumnim mogućnostima softverske podrške te svojstvima i funkcionalnostima QERDS usluge, poduzeo odgovarajuće mjere kako bi se omogućila što veća razina mogućnosti opažanja, operabilnosti, razumljivosti i stabilnosti QERDS usluge, a sve kako bi ta usluga bila jednako dostupna svim korisnicima. Važno je napomenuti da HP d.d., osim digitalne QERDS usluge, omogućava pružanje jednakovrijedne zamjenske usluge preporučene dostave koja nije u digitalnom obliku.

6. Stupanje na snagu; početak primjene ovih uvjeta;

Ova Pravila na snagu stupaju danom donošenja, a primjenjuju se od 15. prosinca 2023. godine, čime prestaju važiti Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave od 20.03.2023. godine.

Broj: HP-19/1-038964/23

HP-Hrvatska pošta d.d.
Predsjednik Uprave

Ivan Čulo

Ivan Čulo
Digitalno potpisao: Ivan Čulo
Datum: 2023.12.15 10:11:17 +01'00'

Prilog I. Popis kvalificiranih pružatelja usluga povjerenja

HP d.d. koristi usluge sljedećih kvalificiranih pružatelja usluga povjerenja:

Kvalificirani elektronički vremenski žig

- Name

AKD d.o.o.

- Trade name

AKD d.o.o.

- Postal address

Savska cesta 31
10000 - HR

- Electronic address

helpdesk-kid@akd.hr

- Information URL

https://www.id.hr/hr

- Trusted List URL

https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/HR/2

- Identifikacijska oznaka

OID: 1.3.6.1.4.1.43999