Politika pružanja kvalificirane usluge elektroničke preporučene dostave

Velika Gorica, prosinac 2023.

Informacije o dokumentu

Naziv dokumenta	Politika pružanja kvalificirane usluge elektroničke preporučene dostave
Verzija dokumenta	1.2
Status dokumenta	Važeći
Datum donošenja	15/12/2023
OID	**1.3.6.1.4.1.54777.1.1.1**
Tip dokumenta	CP
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 CPS	Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave OID: **1.3.6.1.4.1.54777.1.1.2**

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	15.12.2023.	Marina Zečević	Promjena organizacije nadležne za administraciju Politike

1. Uvod

Dokumentom "Politika pružanja kvalificirane usluge elektroničke preporučene dostave" (u nastavku teksta: Politika) propisuju se uvjeti 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: eIDAS Uredba), 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 kvalificirane usluge 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 će osigurati integritet podataka i autentičnost izvora podataka.

Obuhvat ove Politike je cjelokupna infrastruktura HP-a d.d. koja se koristi za pružanje QERDS. Odredbe Politike primjenjuju se na sve sudionike sustava za pružanje QERDS, uključujući među ostalim HP d.d. kao pružatelja usluge, korisnike i pouzdajuće sudionike.

Struktura ovog dokumenta slijedi normizacijski dokument ETSI EN 319 411-1 V1.2.2. (2021-05), koristeći dijelove koji su primjenjivi na pružanje QERDS.

Detaljnija razrada odredaba Politike i odgovarajući postupci za njihovu primjenu propisani su u dokumentu „Pravila postupanja za pružanje kvalificirane usluge elektroničke preporučene dostave" (u daljem tekstu: Pravila postupanja).

Politika će biti objavljena na web stranicama HP-a d.d. na adresi: 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: Politika pružanja kvalificirane usluge elektroničke preporučene dostave
Verzija: 1.2
Datum: 15.12.2023.
Poveznica do dokumenta: https://www.eposta.hr/info

Jedinstveni OID (engl. Object Identifier) **1.3.6.1.4.1.54777** dodijeljen je HP-u d.d. Na osnovu njega HP d.d. dodjeljuje **1.3.6.1.4.1.54777.1.1.1** za ovu Politiku.

Način dodjeljivanja OID-a i pojašnjenje za znamenke nakon jedinstvenog OID-a:

- prva znamenka: 1 – dokumentacija,
- druga znamenka: 1 – krovna dokumentacija,
- treća znamenka: 1-CP, 2-CPS.

1.3. Subjekti i područje primjene usluge

Pružatelj kvalificirane usluge elektroničke preporučene dostave
HP d.d. pruža QERDS uz korištenje kvalificiranog vremenskog žiga i naprednog/kvalificiranog elektroničkog pečata za zaštitu integriteta korisničkog sadržaja i QERDS dokaza i njihovo povezivanje s točnim vremenom.

Korisnici
Korisnici QERDS su fizičke i pravne osobe koje prilikom ugovaranja QERDS prihvaćaju Uvjete pružanja kvalificirane usluge elektroničke preporučene dostave i ostale s njima povezane dokumente bitne za izvršavanje usluge. Korisnici QERDS mogu biti primatelji i pošiljatelji korisničkog sadržaja.

Pouzdajuće strane
Pouzdajuće strane u QERDS jesu vanjski pružatelji usluga, poslovni subjekti u poslovnom odnosu s HP-om d.d. koji prihvaćaju QERDS dokaze, a nisu korisnici. Pouzdajuće strane moraju provjeriti napredni/kvalificirani elektronički pečat, kvalificirani elektronički vremenski žig i certifikate te odgovarajuću listu opozvanih certifikata ili primjenjivati OCSP servis za provjeru certifikata koje koristi HP d.d. prije nego što prihvate informaciju sadržanu u QERDS dokazima.

Ostali sudionici

Ostali sudionici sustava za pružanje QERDS jesu pravne osobe koje ne pružaju i ne koriste se kvalificiranim uslugama povjerenja, ali sudjeluju u dijelovima procesa vezanima uz pružanje kvalificiranih usluga povjerenja. Ovoj grupi sudionika sustava pripadaju proizvođači i distributeri hardvera i softvera korištenih u sustavu za pružanje QERDS, proizvođači i distributeri HSM-ova i drugih kriptografskih uređaja, neovisni ocjenitelji i dr.

1.4. Administracija Politike

1.4.1. Organizacija nadležna za administraciju Politike

Organizacija nadležna za administraciju Politike pružanja kvalificirane usluge elektroničke preporučene dostave:

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

1.4.2. Postupak donošenja Politike

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

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

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

1.5. Definicije i kratice

1.5.1. 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	Korisnik kako je definiran Općim uvjetima korištenja servisa ePošta, koji 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)	Korisnik koji 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	HP d.d. ili drugi pružatelj usluge povjerenja, koji pruža uslugu elektroničke preporučene dostave
Tijelo za ocjenu sukladnosti	Tijelo ovlašteno pozitivnim propisom 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.

1.6.2. 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
OCSP	Online Certificate Status Protocol
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. Odgovornost za objavu informacija i repozitorija

Repozitorij sustava za pružanje QERDS održava HP d.d. kao kvalificirani pružatelj usluga povjerenja te je odgovoran za dokumente i informacije u njima. Repozitorij je javno dostupan i sadrži:

- javni ključ i certifikat, koji HP d.d. koristi za napredni/kvalificirani elektronički pečat korisničkog sadržaja i QERDS dokaza i
- dokumente za QERDS.

Repozitorij je dostupan na web adresi: https://www.eposta.hr/info

3. Identifikacija i potvrđivanje identiteta

3.1. Identifikacija i autentifikacija korisnika

Identifikacija Fizičke osobe kod ugovaranja QERDS dostave obavljat će 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.

Osobnom iskaznicom identificiraju se građani Republike Hrvatske, dok se strane osobe identificiraju isključivo putovnicom.

Identifikacija Pravne osobe ili registrirane djelatnosti koju obavlja fizička osoba kod ugovaranja QERDS obavljat će 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 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.

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, korisnik može koristiti kvalificiranu uslugu elektroničke preporučene dostave.

Registrirani korisnik ne može otvoriti dodatan korisnički račun koji bi sadržavao njegove osobne podatke, a o čemu ga povratno upozorava sustav ili operater u poštanskom uredu.

Opisani načini identifikacije korisnika provode se i kod gubitka, oštećenja ili sumnje na kompromitaciju autentifikacijskih elemenata.

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 mobilne aplikacije ePošta 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, čini 2-faktorsku autentifikaciju.

4. Operativno upravljanje uslugom

HP d.d., kao kvalificirani pružatelj usluga povjerenja, pruža uslugu u skladu s Uredbom eIDAS, Zakonom o provedbi eIDAS Uredbe, te standardizacijskim dokumentima, te 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. provjerava 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:

a) delegirani scenarij – potpis provodi pružatelj usluge,
b) scenarij dodatne sigurnosti – potpis provodi pošiljatelj.

Sustav osigurava QERDS dokaze o prijamu pošiljke za slanje, te o isporuci (engl. consignment) i uručenju (engl. handover) pošiljke. QERDS dokazi se štite naprednim/kvalificiranim elektroničkim 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) i čuvaju 10 (deset) godina.

5. Mjere zaštite opreme i prostora, organizacijske mjere sigurnosti i nadzor nad radom zaposlenika

Mjere zaštite koje provodi HP d.d. su:

- definiranje i dodjeljivanje uloga povjerenja za QERDS,
- nadzor nad radom zaposlenika,
- upravljanje imovinom,
- kontrola pristupa,
- kriptografske kontrole,
- fizička zaštita opreme i prostora,
- zaštita operacija,
- mrežna sigurnost,
- upravljanje incidentima,
- prikupljanje revizijskih zapisa,
- upravljanje kontinuitetom poslovanja i
- definirano postupanje u slučaju prestanka pružanja usluge.

Mjere zaštite opreme i prostora, organizacijske mjere sigurnosti i nadzor nad radom zaposlenika opisani su detaljno u dokumentu Pravila postupanja.

6. Tehničke mjere sigurnosti sustava za pružanje QERDS

Par ključeva za elektronički pečat generira se u štićenoj zoni na kriptografskom uređaju, uz minimalno dvostruku kontrolu ovlaštenih osoba.

Duljine su ključeva i algoritmi korišteni u sustavu za pružanje QERDS:

- HP QERDS – duljina ključa = 2048 bitova, algoritam=sha256WithRSA

Rok valjanosti HP QERDS certifikata za napredni/kvalificirani elektronički pečat i para ključeva iznosi dvije (2) godine.

Za pohranu privatnih ključeva koriste se kriptografski uređaji sukladno standardu FIPS PUB 140-2, level 3 i/ili CC EAL 4+.

Privatni ključevi za napredni/kvalificirani elektronički pečat pohranjeni na kriptografskom modulu aktiviraju se nakon pokretanja aplikativnog sustava ePošta na poslužiteljima HP d.d. Za aktiviranje je nužna pouzdana autentifikacija koja se odnosi na kriptografske module. Privatni ključevi za napredni/kvalificirani elektronički pečat deaktiviraju se zaustavljanjem rada sustava ePošta.

Kvalificirani elektronički vremenski žig, koji HP d.d. koristi u pružanju usluge je eksternaliziran kod drugog kvalificiranog pružatelja usluga povjerenja (nalazi se na EU Trusted listi).

Ostale tehničke mjere sigurnosti sustava za pružanje QERDS su opisane detaljno u dokumentu Pravila postupanja.

7. Profili certifikata i liste opozvanih certifikata

Kvalificirani elektronički pečat HP d.d. koji se koristi u pružanju QERDS, podržan je kvalificiranim certifikatom sukladnim ETSI 319 411-2 QCP-l-qscd politici izdanim od kvalificiranog pružatelja usluga povjerenja (QTSP) i onemogućava neotkrivenu izmjenu podataka.

Polje Subject unutar certifikata sadržava potpuno ime pružatelja QERDS – HP d.d.

Putanja do liste opozvanih certifikata i OCSP servisa za provjeru informacije o statusu certifikata kvalificiranog pružatelja usluga povjerenja, koji je izdao certifikat za HP d.d., nalazi se unutar certifikata u poljima CRL Distrubution Points i Authority Information Access.

8. Revizija usklađenosti i druge provjere

Nadzor pružanja kvalificiranih usluga povjerenja iz opsega ovih Pravila postupanja provodi nadležno nacionalno tijelo (Ministarstvo gospodarstva i održivog razvoja) sukladno odredbama eIDAS uredbe, provedbenih akata donesenih temeljem te Uredbe i Zakona o provedbi eIDAS uredbe. Vanjske provjere sukladnosti provode se najmanje svake 2 (dvije) godine sukladno Uredbi eIDAS. 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.

9. Druga financijska i pravna pitanja

9.1. Naknada za korištenje usluge

Korištenje QERDS naplaćuje se sukladno važećem cjeniku HP-a d.d.

9.2. Osiguranje od odgovornosti

U pogledu rizika od odgovornosti za štetu sukladno članku 13. eIDAS Uredbe, HP d.d. raspolaže odgovarajućim osiguranjem od odgovornosti. HP d.d. raspolaže s dostatnim sredstvima i ima financijsku stabilnost za pružanje kvalificiranih usluga povjerenja.

9.3. Povjerljivost informacija

Svi zaposlenici HP d.d. koji sudjeluju u radu sustava za pružanje QERDS dužni su čuvati povjerljivost informacija/podataka definiranih u ovoj točki. Obveza čuvanja povjerljivih informacija/podataka odnosi se i na zaposlenike vanjskih pružatelja usluga, što mora biti regulirano ugovorom o poslovnoj suradnji između HP d.d. i vanjskih pružatelja usluga. Sve informacije/podaci iz sustava za pružanje QERDS koji nisu označeni kao javni smatraju se povjerljivim informacijama/podacima, uključujući sve informacije/podatke potrebne za pružanje kvalificiranih usluga povjerenja, klasificirane podatke i one informacije/podatke čijim bi otkrivanjem nastala šteta za sudionike u procesu.

9.4. Zaštita osobnih podataka

HP d.d. je usvojila mjere zaštite osobnih podataka u skladu s Uredbom (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). HP d.d. je odgovoran za zaštitu osobnih podataka obrađenih tijekom pružanja kvalificiranih usluga povjerenja.

U postupku registracije korisnika i nakon toga HP d.d. je ovlašten prikupljati osobne podatke koji su potrebni za valjano utvrđivanje identiteta korisnika te druge podatke potrebne za valjano davanje kvalificiranih usluga povjerenja. Osobni podaci koje prikupi HP d.d., i koji se ne prikazuju u javnim evidencijama i/ili registrima koji se za potrebe pružanja kvalificiranih usluga povjerenja moraju propisano voditi, povjerljivi su osobni podaci koje HP d.d. odgovarajuće štiti.

HP d.d. je ovlašten, osim za potrebe ispunjenja zakonskih obveza, odnosno obveza po Ugovoru, koristiti se osobnim podacima i objavljivati ih samo na osnovi pisane privole korisnika koja se može dati u zahtjevu za ugovaranje usluge ili kasnije.

Osobni podaci mogu se dati na uvid trećim stranama isključivo pod uvjetima koji su predviđeni zakonom.

9.5. Zaštita intelektualnog vlasništva

Svi podaci i dokumentacija objavljena u javnom repozitoriju sustava za pružanje QERDS intelektualno su vlasništvo HP-a d.d.

Object identifiers numbers (OIDs) koji se koriste, vlasništvo su HP-a d.d. i registrirani su kod nadležnog tijela.

HP d.d. ne polaže pravo intelektualnog vlasništva na softver koji se koristi u sustavu za pružanje QERDS, a koji je u vlasništvu trećih osoba.

9.6. Obveze i odgovornosti

9.6.1. Obveze pružatelja usluge

HP d.d., kao kvalificirani pružatelj usluga 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,
- propisnu zaštitu osobnih podataka,
- provedbu interne i vanjske provjere sukladnosti,
- sukladnost sa 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.

9.6.2. Obveze korisnika

Korisnici su obvezni:

- 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., te ste 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

9.6.3. Obveze pouzdajućih strana

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, sama je odgovorna za rizike kod pouzdavanja u napredni/kvalificirani elektronički pečat i kvalificirani elektronički vremenski žig HP-a d.d.

Sve promjene koje utječu na pružanje QERDS usluge, pouzdajuća strana obvezna je prijaviti HP-u d.d.

9.7. Ograničenje odgovornosti

HP d.d., kao pružatelj kvalificirane usluga povjerenja, ne preuzima odgovornost za eventualnu štetu koja bi mogla nastati u sljedećim slučajevima:

- ako je registracija korisnika provedena na temelju pogrešnih ili nevjerodostojnih podataka podnesenih od podnositelja zahtjeva,
- ako je usluga QERDS upotrijebljena na nepravilan ili zlonamjeran način,
- ako su nepogode ili gubici nastali u razdoblju između podnošenja zahtjeva za registracijom i isporuke autentifikacijskih elemenata podnositelju zahtjeva,
- ako korisnik ili pouzdajuća strana nisu postupali u skladu s odredbama ove Politike i Pravila postupanja,
- ako je došlo do zloupotrebe ili sigurnosne kompromitacije računala korisnika odnosno pouzdajuće strane
- ako je korisnik omogućio korištenje QERDS neovlaštenim osobama
- ako je računalo korisnika ili pouzdajuće strane funkcioniralo na neispravan način
- ako je došlo do prekida rada ili neispravnog rada infrastrukture koja nije pod nadležnošću ili pod kontrolom sustava za pružanje QERDS ili
- ako su nastupile okolnosti koje se mogu opisati kao viša sila.

Osim onog za što je HP d.d. izričito odgovoran navedeno u točki 9.6 ove Politike, HP d.d. kao pružatelj kvalificiranih usluga 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 istoj točci Politike.

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 ovom Politikom i Pravilima postupanja.

9.8. Naknada štete

Svaki sudionik sustava za pružanje QERDS odgovara oštećenom za štetu koju je počinio zbog nepoštivanja odredbe ove Politike, Pravila postupanja i važećih relevantnih propisa.

9.9. Rješavanje žalbi i sporova

Korisnici mogu HP-u d.d. uputiti prigovore u vezi pružanja kvalificirane usluge povjerenja, na što će HP d.d. odgovoriti. Prigovori se podnose i postupak se odvija na način određen Općim uvjetima korištenja servisa ePošta. Svi sporovi između HP-a d.d. i korisnika koji bi se mogli pojaviti tijekom korištenja QERDS, rješavat će se mirnim putem. U ostalim slučajevima sporovi će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu hrvatskog prava. Iznimno, ako je primjenjivo, korisnik – fizička osoba, uz uvjet da su ispunjene pretpostavke propisane Zakonom o alternativnom rješavanju potrošačkih sporova pod kojima se isti smatra potrošačem, ima pravo temeljem tog Zakona pokrenuti postupak rješavanja potrošačkog spora pred tijelom za alternativno rješavanje sporova na adresi: https://ec.europa.eu/consumers/odr.

9.10. Mjerodavni propisi

Kvalificiranu uslugu povjerenja iz opsega ove Politike HP d.d. pruža u skladu s propisima navedenima pod točkom 1.1. ove Politike.

9.11. Stupanje na snagu

Ova Politika na snagu stupa danom donošenja, a primjenjuje se od 15. prosinca 2023. godine, čime prestaje važiti Politika pružanja kvalificirane usluge elektroničke preporučene dostave od 01.01.2022. godine.

Broj: HP-19/1-038964/23

HP-Hrvatska pošta d.d.
Predsjednik Uprave

Ivan Čulo

IVAN ČULO
HR-05588836254

HP D.D.
HR-87311810356

Elektronički potpisano: 14.12.2023T13:33:03 (UTC:2023-12-14T12:33:03Z)
ELECTRONICALLY SIGNED
Provjera: https://esign.certilia.com/provjera
VERIFICATION
Broj zapisa: fdb6c8b3-c1d2-4039-bece-28e863ef5e76
RECORD ID