



# Pravilnik o postupcima pružanja usluge Identityum ID Wallet

OID: 1.3.6.1.4.1.65996.4.2.1.1

**Datum stupanja na snagu:** 24.08.2026  
**Vlasnik dokumenta:** Identityum  
**Odobrio:** direktor Identityuma  
**Javni repozitorij:**  
<https://identityum.com/terms-policies/>

**Pružatelj usluge:** Identity Consortium d.o.o.  
**Adresa sjedišta:** Trogirska ulica 2, 42000 Varaždin, Hrvatska  
**Matični broj subjekta (MBS):** 070166678  
**Osobni identifikacijski broj (OIB):** 44867795324  
**Opći kontakt:** [info@identityum.com](mailto:info@identityum.com)  
**Korisnička podrška:** [support@identityum.com](mailto:support@identityum.com)



## POVIJEST IZMJENA

| VERZIJA | DATUM IZMJENE | AUTOR     | OPIS IZMJENA                                                                                                                                                    |
|---------|---------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | 17.07.2025.   | R. Ilijaš | Početna verzija                                                                                                                                                 |
| 2.0     | 24.08.2026.   | R. Ilijaš | Cjelovita verzija usklađena s Identityum kanonskim modelom razdvajanja Walleta, usluge Identify, Identityum PID-a, autentikacije i povezanih usluga povjerenja. |

Verzija 2.0 izdaje se kao cjelovita zamjenska verzija. Zbog toga, izmjene nisu pojedinačno označene **ŽUTO** kao inače.



## SADRŽAJ

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| 1. Opće informacije .....                                                         | 7  |
| 1.1. Svrha dokumenta.....                                                         | 7  |
| 1.2. Normativni status .....                                                      | 7  |
| 1.3. Opseg.....                                                                   | 8  |
| 1.4. Pitanja izvan opsega.....                                                    | 8  |
| 1.5. Ciljana publika .....                                                        | 9  |
| 1.6. Dokumentacijski okvir i razrješavanje nedosljednosti .....                   | 9  |
| 1.7. Primjenjivi propisi, norme i smjernice .....                                 | 10 |
| 1.7.1. Propisi Europske unije i Republike Hrvatske .....                          | 10 |
| 1.7.2. Norme i tehničke specifikacije .....                                       | 10 |
| 1.7.3. Javni i interni Identityumovi dokumenti.....                               | 11 |
| 1.8. Pojmovi, definicije i kratice .....                                          | 11 |
| 1.9. Upravljanje dokumentom, odobravanje i upravljanje izmjenama .....            | 12 |
| 2. Model i granice usluge Identityum Wallet .....                                 | 13 |
| 2.1. Opis usluge ID Walleta .....                                                 | 13 |
| 2.2. Kanonski objekti i njihovo razdvajanje.....                                  | 13 |
| 2.3. Funkcionalni načini rada Walleta .....                                       | 14 |
| 2.3.1. Prazan Wallet odnosno Wallet samo za autentikaciju .....                   | 14 |
| 2.3.2. Wallet s pohranjenim Identityum PID-om .....                               | 14 |
| 2.3.3. Wallet koji se koristi s povezanim certifikatom.....                       | 14 |
| 2.3.4. Posebne eID vjerodajnice i vanjski regulatorni statusi.....                | 14 |
| 2.4. Sudionici i uloge .....                                                      | 14 |
| 2.5. Granice usluge i tehničke granice .....                                      | 15 |
| 2.6. Normativne funkcionalnosti Walleta (TO-BE).....                              | 15 |
| 2.7. Funkcije izvan opsega Walleta i vanjski uvjeti .....                         | 15 |
| 2.8. Dopuštene i zabranjene uporabe .....                                         | 15 |
| 2.9. Pretpostavke i ograničenja pouzdanja .....                                   | 16 |
| 3. Podnošenje zahtjeva, uspostava autentikacijskih faktora i izrada Walleta ..... | 17 |
| 3.1. Izravno pokretanje i B2B ponuda Walleta .....                                | 17 |
| 3.2. Dobrovoljan odabir Korisnika .....                                           | 17 |
| 3.3. Informacije, Uvjeti korištenja Walleta i obavijest o privatnosti.....        | 17 |
| 3.4. Registracijski podaci za prazan Wallet.....                                  | 17 |
| 3.5. Uspostava AUTH-A i AUTH-D .....                                              | 18 |
| 3.6. Značenje AUTH-D u praznom Walletu .....                                      | 18 |
| 3.7. Izrada i aktivacija praznog Walleta.....                                     | 18 |
| 3.8. Identifikator Walleta i pravilo jedinstvenosti.....                          | 18 |
| 3.9. Povezivanje uređaja i autentikatora .....                                    | 19 |
| 3.10. Dokazi o uspostavi i revizijski trag .....                                  | 19 |
| 3.11. Neuspjela, prekinuta i ponovljena uspostava .....                           | 19 |
| 4. Sučelje Walleta prema usluzi Identify i Identityum PID-u .....                 | 20 |
| 4.1. Pokretanje ili nastavak usluge Identify iz Walleta .....                     | 20 |
| 4.2. Funkcionalna i dokumentacijska granica Identifyja.....                       | 20 |



|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| 4.3. Identify tijekomovi neovisni o postojanju Walleta .....                | 20 |
| 4.4. Rezultat Identifyja dostupan Walletu .....                             | 20 |
| 4.5. Pohrana ili povezivanje rezultata na strani Walleta .....              | 21 |
| 4.6. LoIP kao metapodatak rezultata Identifyja .....                        | 21 |
| 4.7. Izdavanje PID-a neovisno o Walletu .....                               | 21 |
| 4.8. Razdvajanje izdavanja PID-a i njegove dostupnosti u Walletu .....      | 21 |
| 4.9. Neovisni odabiri PID-a i povezanih usluga .....                        | 22 |
| 4.10. Svježina PID-a i upućivanje na novi Identify postupak .....           | 22 |
| 4.11. Dokazi Identifyja i usluga povjerenja izvan Walleta .....             | 22 |
| 4.12. Neuspjeli i ručno obrađeni postupci Identifyja .....                  | 22 |
| 5. Svojstva autentikacije i sigurnosni model Walleta .....                  | 23 |
| 5.1. Prazan Wallet kao autentikacijski kontekst .....                       | 23 |
| 5.2. Rezultati autentikacije bez identifikacije .....                       | 23 |
| 5.3. Uvjeti za sredstvo elektroničke identifikacije .....                   | 23 |
| 5.4. Autentikacijski režim, LoIP PID-a i eIDAS LoA .....                    | 23 |
| 5.5. Autentikacijski faktori i kategorije .....                             | 24 |
| 5.6. Dopuštene kombinacije faktora .....                                    | 24 |
| 5.7. Komponente Walleta, uređaja i poslužiteljske strane .....              | 25 |
| 5.8. Granice vjerodajnica i kriptografskih ključeva .....                   | 25 |
| 5.9. Zaštita od umnožavanja, neovlaštene izmjene i ponovnog izvođenja ..... | 26 |
| 5.10. Kontrola i posjed Korisnika .....                                     | 26 |
| 5.11. Zaštita pohranjenih podataka i integrirana zaštita privatnosti .....  | 26 |
| 5.12. Regulatorni status i ograda od tvrdnji .....                          | 27 |
| 6. Upravljanje životnim ciklusom Walleta i sadržaja Walleta .....           | 28 |
| 6.1. Statusi Walleta i odvojenost povezanih objekata .....                  | 28 |
| 6.2. Redovna upotreba .....                                                 | 28 |
| 6.3. Upravljanje autentikacijskim faktorima .....                           | 28 |
| 6.4. Dodavanje, uklanjanje i migracija uređaja .....                        | 29 |
| 6.5. Promjene kontakta i identifikatora računa .....                        | 30 |
| 6.6. Dodavanje, ažuriranje, zastarijevanje i uklanjanje PID-a .....         | 30 |
| 6.7. Suspenzija Walleta .....                                               | 30 |
| 6.8. Ponovna aktivacija Walleta .....                                       | 31 |
| 6.9. Trajni opoziv ili zatvaranje Walleta .....                             | 31 |
| 6.10. Obnova i zamjena .....                                                | 31 |
| 6.11. Oporavak pristupa .....                                               | 31 |
| 6.12. Gubitak, krađa i kompromitacija .....                                 | 32 |
| 6.13. Brisanje podataka Walleta i zadržani dokazi .....                     | 32 |
| 6.14. Informacije o statusu i obavijesti Korisniku .....                    | 32 |
| 7. Autentikacija i autorizacija s pomoću Walleta .....                      | 34 |
| 7.1. Vrste autentikacijskih i autorizacijskih transakcija Walleta .....     | 34 |
| 7.2. Pokretanje od strane Pouzdajuće strane ili povezane usluge .....       | 34 |
| 7.3. Identifikacija Pouzdajuće strane .....                                 | 35 |
| 7.4. Određivanje potrebnog autentikacijskog režima .....                    | 35 |
| 7.5. Odabir faktora i pojačana autentikacija .....                          | 35 |
| 7.6. Dinamička autentikacija .....                                          | 36 |



|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| 7.7. Vezivanje izazova, jednokratne vrijednosti, sesije i publike .....     | 36 |
| 7.8. Provjere statusa Walleta i vjerodajnica .....                          | 37 |
| 7.9. Potvrda Korisnika i autorizacija transakcije .....                     | 37 |
| 7.10. Rezultat autentikacije bez identifikacije .....                       | 38 |
| 7.11. Pseudonimni identifikatori specifični za Pouzdajuću stranu .....      | 38 |
| 7.12. Autentikacijska tvrdnja i dokazi .....                                | 38 |
| 7.13. Neuspjela autentikacija i otkrivanje zlouporabe .....                 | 38 |
| 7.14. Obveze Pouzdajuće strane .....                                        | 39 |
| 8. Podaci u Walletu i predstavljanje Identityum PID-a .....                 | 41 |
| 8.1. Kategorije podataka Walleta .....                                      | 41 |
| 8.2. PID pohranjen ili povezan s Walletom .....                             | 41 |
| 8.3. Validirani i nevalidirani podaci .....                                 | 41 |
| 8.4. Izvori, podrijetlo, LoIP i svježina .....                              | 42 |
| 8.5. Zaštićena pohrana .....                                                | 43 |
| 8.6. Pristup Korisnika i upravljanje podacima .....                         | 44 |
| 8.7. Odabir i smanjenje količine podataka .....                             | 44 |
| 8.8. Predstavljanje PID-a i dijeljenje atributa .....                       | 45 |
| 8.9. Vezivanje uz primatelja, svrhu i transakciju .....                     | 45 |
| 8.10. Provjera statusa i svježine PID-a .....                               | 46 |
| 8.11. Ažuriranje, uklanjanje i ponovna upotreba .....                       | 46 |
| 8.12. Povijest aktivnosti, izvoz i prenosivost .....                        | 47 |
| 8.13. Odvajanje od zadržanih regulatornih dokaza .....                      | 48 |
| 9. Sučelja Walleta s uslugom Identify i povezanim uslugama povjerenja ..... | 49 |
| 9.1. Odnos s uslugom Identityum Identify .....                              | 49 |
| 9.2. Neobvezna ponuda Walleta nakon postupka Identify .....                 | 49 |
| 9.3. Neovisni odabiri PID-a i povezane usluge povjerenja .....              | 49 |
| 9.4. Granica usluga povjerenja .....                                        | 49 |
| 9.5. Mjerodavni dokumenti za povezane usluge povjerenja .....               | 50 |
| 9.6. Wallet-side zahtjev i prihvrat uvjeta povezane usluge .....            | 50 |
| 9.7. Prikaz rezultata i statusa povezane usluge u Walletu .....             | 50 |
| 9.8. Prihvatljivost certifikata bez PID-a pohranjenog u Walletu .....       | 50 |
| 9.9. Autentikacija Walletom za upotrebu udaljenog ključa .....              | 51 |
| 9.10. Učinak događaja Walleta na certifikate i ključeve .....               | 51 |
| 9.11. Usluge izvan opsega Pravilnika Walleta .....                          | 52 |
| 10. Upravljanje sigurnošću i operativnim poslovima .....                    | 53 |
| 10.1. Organizacija i odgovornosti .....                                     | 53 |
| 10.2. Upravljanje rizicima i informacijskom sigurnošću .....                | 54 |
| 10.3. Uloge, kompetencije i razdvajanje dužnosti .....                      | 55 |
| 10.4. Upravljanje dobavljačima .....                                        | 55 |
| 10.5. Kontrole pristupa, kriptografije i sigurnosti podataka .....          | 56 |
| 10.6. Upravljanje promjenama i konfiguracijama .....                        | 57 |
| 10.7. Zapisivanje, dokazi i vođenje evidencije .....                        | 57 |
| 10.8. Čuvanje i sigurno uklanjanje .....                                    | 58 |
| 10.9. Praćenje i upravljanje incidentima .....                              | 59 |
| 10.10. Kontinuitet poslovanja i oporavak od katastrofe .....                | 60 |



|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| 10.11. Prestanak usluge .....                                                          | 60 |
| 10.12. Revizija i ocjenjivanje sukladnosti .....                                       | 61 |
| 11. Informacije za Korisnike, privatnost i pravna pitanja .....                        | 63 |
| 11.1. Objavljena definicija usluge .....                                               | 63 |
| 11.2. Uvjeti korištenja .....                                                          | 63 |
| 11.3. Sigurnosne preporuke .....                                                       | 64 |
| 11.4. Obavijest o privatnosti i uloge u zaštiti osobnih podataka .....                 | 64 |
| 11.5. Kontrola, autorizacija i prava Korisnika .....                                   | 66 |
| 11.6. Naknade .....                                                                    | 67 |
| 11.7. Odgovornosti Korisnika .....                                                     | 67 |
| 11.8. Odgovornosti Pouzdajuće strane .....                                             | 68 |
| 11.9. Odgovornosti i ograničenja Identyuma .....                                       | 69 |
| 11.10. Podrška i prijavljivanje sigurnosnih događaja .....                             | 70 |
| 11.11. Pritužbe i rješavanje sporova .....                                             | 70 |
| 11.12. Mjerodavno pravo .....                                                          | 70 |
| 11.13. Obavješćavanje o promjenama .....                                               | 71 |
| Prilozi .....                                                                          | 73 |
| Prilog A — Matrica kanonskih funkcija i granica regulatornog statusa .....             | 73 |
| Prilog B — Zahtjevi autentikacije prema radnji .....                                   | 75 |
| Prilog C — Matrica životnog ciklusa Walleta, PID-a, certifikata i ključa .....         | 76 |
| Prilog D — Matrica rezultata autentikacije bez identifikacije i otkrivanja PID-a ..... | 77 |
| Prilog E — Matrica dokaza i čuvanja .....                                              | 78 |
| Prilog F — Matrica primjenjivosti regulative i mjerodavnih dokumenata .....            | 79 |



## 1. Opće informacije

### 1.1. Svrha dokumenta

Ovim Pravilnikom o postupcima pružanja usluge Identityum ID Wallet (dalje: Pravilnik) opisuju se prakse koje Identity Consortium d.o.o. (dalje: Identityum) primjenjuje pri pružanju, radu, zaštiti i upravljanju životnim ciklusom usluge Identityum ID Wallet.

Njegova je svrha Korisnicima, Pouzdajućim stranama, Poslovnim klijentima, revizorima, ocjeniteljima i nadležnim tijelima pružiti transparentan i provjerljiv opis usluge Walleta, bez poistovjećivanja Walleta s provjerom identiteta, podacima za identifikaciju osobe, sredstvima elektroničke identifikacije, certifikatima ili uslugama udaljenog potpisivanja.

Ovim se Pravilnikom osobito opisuju:

- a) izrada i uporaba ID Walleta bez pohranjenih identifikacijskih podataka;
- b) neobvezno pokretanje ili nastavak usluge Identify iz Walleta te primitak, povezivanje, pohrana i predstavljanje Identityum PID-a koji izdaje Identify;
- c) uspostava i upravljanje autentikacijskim faktorima Walleta;
- d) autentikacija i autorizacija putem Walleta, uključujući pseudonimnu autentikaciju bez tvrdnje o provjerenom identitetu osobe;
- e) kontrolirano predstavljanje PID atributa Pouzdajućim stranama;
- f) sučelja između Walleta, usluge Identityum Identify i usluga povjerenja;
- g) odvojeni životni ciklusi Walleta, PID-a, autentikacijskih faktora, certifikata i kriptografskih ključeva; te
- h) prakse sigurnosti, dokazivanja, upravljanja, privatnosti i informiranja korisnika koje se primjenjuju na uslugu Walleta.

### 1.2. Normativni status

Ovaj je Pravilnik Identityumova javna izjava o operativnim, organizacijskim, sigurnosnim praksama i praksama životnog ciklusa koje se primjenjuju na ID Wallet. Odobrava ga direktor Identityuma i obvezuje Identityum u dijelu u kojem opisuje prakse koje se Identityum obvezuje provoditi.

Dokument je strukturiran uzimajući u obzir četiri područja iz Provedbene uredbe Komisije (EU) 2015/1502 za pouzdanost elektroničke identifikacije: registraciju, upravljanje sredstvima elektroničke identifikacije, autentikaciju te upravljanje i organizaciju. Takvo strukturno usklađenje samo po sebi ne predstavlja tvrdnju da je ID Wallet ili bilo koja povezana vjerodajnica prijavljena, certificirana ili da joj je formalno dodijeljena eIDAS razina pouzdanosti. Ako nije izričito navedeno drukčije, objava ovog Pravilnika ne predstavlja tvrdnju da je ID Wallet europski novčanik za digitalni identitet, da je izdan u okviru prijavljenog nacionalnog sustava

| Pravilnik o postupcima pružanja usluge Identityum ID Wallet   OID: 1.3.6.1.4.1.65996.4.2.1.1 |              |                                     |                      |                |
|----------------------------------------------------------------------------------------------|--------------|-------------------------------------|----------------------|----------------|
| Datum: 24.08.2026.                                                                           | Verzija: 2.0 | Vlasnik: Identity Consortium d.o.o. | Klasifikacija: Javno | Stranica: 7/80 |



elektroničke identifikacije ili da ispunjava zahtjeve razine pouzdanosti Low, Substantial ili High. Kanonska i mjerodavna verzija ovog Pravilnika jest verzija na hrvatskom jeziku. Svaki prijevod na engleski ili drugi jezik ima isključivo informativni karakter; u slučaju razlike mjerodavan je tekst na hrvatskom jeziku.

### 1.3. Opseg

Ovaj se Pravilnik primjenjuje na uslugu ID Walleta koju Identityum izravno pruža fizičkim osobama. Wallet se može izraditi i ostati aktivan bez Identityum PID-a ili drugih podataka o provjerenom identitetu osobe. Takav Wallet pruža kontekst autentikacije i autorizacije, ali samim svojim postojanjem ne predstavlja sredstvo elektroničke identifikacije niti uspostavlja provjereni identitet osobe.

Opseg obuhvaća račun Walleta, njegov provjereni kontaktni identifikator, autentikacijske faktore, podržana sučelja, sadržaj Walleta, upute za Korisnika, interakcije s Pouzdajućim stranama, događaje životnog ciklusa te zapise potrebne za rad i dokazivanje tih funkcija.

Kada se Wallet koristi za podnošenje zahtjeva, aktivaciju ili autorizaciju povezane usluge povjerenja, ovim se Pravilnikom uređuje interakcija na strani Walleta. Životni ciklusi certifikata, privatnog ključa, udaljenog QSCD-a i usluge povjerenja i dalje su uređeni primjenjivim CP-om, TSPS-om, Izjavom o objavi podataka i Uvjetima korištenja.

### 1.4. Pitanja izvan opsega

Izvan primarnog opsega ovog Pravilnika nalaze se:

- i) cjelovito funkcioniranje usluge Identityum Identify i konačna odluka Poslovnog klijenta o onboardingu, KYC-u, AML-u ili odobravanju pristupa;
- j) detaljni mehanizmi provjere identiteta, biometrijski pragovi i dokazne kontrole uređene TSPS-om i kontroliranom internom dokumentacijom;
- k) politike certifikata, certifikacijski profili, OID-evi politika i cjeloviti životni ciklusi certifikata;
- l) upravljanje i certificirana konfiguracija udaljenih QSCD ili QSealCD usluga;
- m) izrada i validacija elektroničkih potpisa ili pečata, osim interakcije Korisnika na strani Walleta;
- n) kvalificirani elektronički vremenski žigovi;
- o) elektronička identifikacija pravnih osoba i životni ciklus QLSeal certifikata;
- p) definiranje i izvođenje Identify mehanizama COL-C i COL-D te definiranje zasebnih vjerodajnica Identityum SMS, WEB, MOBILE, NIAS ili C2G, osim njihova izričito opisanog sučelja s Walletom; te
- q) funkcije europskog novčanika za digitalni identitet koje nisu izričito navedene kao dio Identityumove usluge.





## 1.5. Ciljana publika

Ovaj je Pravilnik namijenjen:

- a) fizičkim osobama koje koriste ili namjeravaju koristiti Identityum ID Wallet;
- b) Pouzdajućim stranama koje prihvaćaju autentikaciju, PID ili druge podatke predstavljene putem ID Walleta;
- c) Poslovnim klijentima koji integriraju ID Wallet kao mogućnost autentikacije ili ponovne uporabe identiteta u okviru usluge Identityum Identify;
- d) pružateljima usluga povjerenja i drugim pružateljima usluga koji koriste ID Wallet u vezi sa svojim uslugama;
- e) revizorima, tijelima za ocjenjivanje sukladnosti i neovisnim ocjeniteljima;
- f) nadzornim, regulatornim i drugim nadležnim tijelima;
- g) osoblju Identityuma odgovornom za upravljanje, sigurnost, rad i podršku usluge ID Walleta; te
- h) vanjskim dobavljačima čije usluge bitno podupiru ID Wallet.

Pravilnik je tehnički i normativni dokument usluge. Nije namijenjen zamjeni uputa za korisnike, smjernica o pristupačnosti, kontekstualnih obavijesti, zaslona za davanje pristanka ili materijala korisničke podrške.

## 1.6. Dokumentacijski okvir i razrješavanje nedosljednosti

Dokumentacija kojom Identityum uređuje Wallet i povezane usluge sastoji se od međusobno povezanih javnih i internih dokumenata. Pojedini dokument primjenjuje se prvenstveno na pitanja koja su mu prema svrsi i opsegu dodijeljena; ne uspostavlja se jedinstvena linearna hijerarhija za pitanja koja različiti dokumenti uređuju na različitim razinama.

Dokumentacijski okvir obuhvaća: (1) Politike i profile Identityum usluga povjerenja (CP), koji određuju politike, profile, OID-eve, dopuštene uporabe i značenje profila; (2) Pravilnik o postupcima pružanja Identityum usluga povjerenja (TSPS), koji uređuje organizacijske, proceduralne, sigurnosne i tehničke prakse usluga povjerenja te u svojem poglavlju 11 predstavlja CPS; (3) ovaj Pravilnik Walleta, kao primarni dokument za izradu, uporabu i životni ciklus Walleta, autentikaciju i autorizaciju Walletom te pohranu, povezivanje, prikaz, predstavljanje i uklanjanje PID-a na strani Walleta; (4) Uvjete korištenja i izjave o objavi podataka, koji uređuju ugovorne odnose, prava, obveze, ograničenja uporabe, odgovornost i pritužbe; te (5) kontroliranu internu dokumentaciju koja razrađuje provedbene postupke, arhitekturu, konfiguracije i dokaze.

Za pitanja provjere identiteta, izdavanja PID-a, određivanja LoIP-a i identity-proofing use caseova mjerodavni su TSPS kada se Identify koristi u kontekstu usluge povjerenja te odgovarajuća kontrolirana dokumentacija Identifyja u drugim kontekstima. Za certifikate,



ključeve, potpise, pečate i udaljeni QSCD mjerodavni su CP, TSPS/CPS, primjenjivi profil, izjava o objavi podataka i uvjeti predmetne usluge. Ovaj Pravilnik ostaje mjerodavan za radnje i učinke na strani Walleta. Ako se utvrdi nedosljednost, prvenstveno se primjenjuju važeći propisi i obvezujući regulatorni zahtjevi; nedosljednost se procjenjuje prema predmetu i funkcionalnom opsegu svakog dokumenta; do usklađenja se ne primjenjuje tumačenje koje bi umanjilo zahtijevanu sigurnost, razinu pouzdanosti, kvalificirani status ili prava korisnika; a dokumentacija se usklađuje kroz kontrolirani postupak upravljanja promjenama.

## 1.7. Primjenjivi propisi, norme i smjernice

### 1.7.1. Propisi Europske unije i Republike Hrvatske

Glavni regulatorni okvir obuhvaća Uredbu (EU) br. 910/2014, kako je izmijenjena Uredbom (EU) 2024/1183, Uredbu (EU) 2016/679, primjenjive propise o kibernetičkoj sigurnosti te hrvatske propise kojima se ti akti provode ili dopunjuju.

Provedbena uredba Komisije (EU) 2015/1502 koristi se kao primarna referenca za strukturu pouzdanosti registracije, upravljanja sredstvima elektroničke identifikacije, autentikacije te upravljanja i organizacije. Zahtjevi specifični za europske novčanike za digitalni identitet, uključujući Provedbenu uredbu Komisije (EU) 2024/2979, koriste se samo kao projektne smjernice koje ne predstavljaju tvrdnju o statusu, i to kada Identyum izričito preuzme usklađeno načelo.

### 1.7.2. Norme i tehničke specifikacije

ETSI TS 119 461 primjenjuje se na Identify postupke provjere identiteta u opsegu i use caseovima identificiranim u mjerodavnom TSPS-u kada Identyum kao TSP sam provodi takvu provjeru; ne primjenjuje se na samu izradu praznog Walleta. ETSI EN 319 401 i ETSI EN 319 411-1/-2 primjenjuju se na povezane usluge povjerenja prema CP-u i TSPS-u. ETSI TS 119 431-1 primjenjuje se na politiku i sigurnosne zahtjeve udaljenog potpisivanja/SSAS-a, uključujući SAD i dokazivanje sole control, a ne na opću autentikaciju Walletom. ETSI TS 119 472-2 i ETSI TR 119 462 relevantni su za EUDI/EAA kontekst i ne pretvaraju Identyumov proizvodno specifični PID u EUDI PID. ISO/IEC 27001, ISO/IEC 27002, relevantne biometrijske norme i EN 301 549 primjenjuju se u opsegu utvrđenom sustavom upravljanja, tehničkim dizajnom i regulatornim obvezama.

Upućivanje na normu ne znači da se svaka odredba primjenjuje na svaku funkciju Walleta. Mjerodavni dokument, točan opseg, verzija, dokaz i eventualno obrazloženo izuzeće vode se u kontroliranoj matrici sukladnosti. Funkcija pristupa Identifyju dostupna je i bez prethodne izrade Walleta, tako da biometrijski faktor Walleta nije jedini put do postupka provjere identiteta.



### 1.7.3. Javni i interni Identityumovi dokumenti

Javno primjenjivi dokumenti uključuju Uvjete korištenja Walleta, Pravila privatnosti Walleta, ovaj Pravilnik, Pravilnik o postupcima pružanja Identityum usluga povjerenja (TSPS), dokument Politike i profili Identityum usluga povjerenja (CP) te primjenjive Izjave o objavi podataka za pojedine usluge.

Interni potporni dokumenti uključuju Pravilnik o autentikaciji putem ID Walleta, Pravilnik o ID mehanizmima, postupke upravljanja identitetima, politike informacijske sigurnosti i upravljanja rizicima, postupke upravljanja incidentima i kontinuitetom, tehničke specifikacije i dokazne zapise.

### 1.8. Pojmovi, definicije i kratice

Pojmovi definirani primjenjivim propisima i normama imaju značenje utvrđeno tim izvorima.

Osobito su važne sljedeće razlike specifične za proizvod:

| Pojam                         | Značenje u ovom Pravilniku                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID Wallet ili Wallet          | Identityumova zasebna usluga računa, autentikacijskog i autorizacijskog konteksta te zaštićenog okruženja za upravljanje podacima. Wallet ne provodi provjeru identiteta i ne izdaje PID.                                                                                                                                                                      |
| Prazan Wallet                 | Aktivan Wallet s uspostavljenim autentikacijskim faktorima, ali bez Identityum PID-a ili tvrdnje o provjerenom identitetu osobe.                                                                                                                                                                                                                               |
| Identityum PID                | Proizvodno specifičan strukturirani rezultat koji izdaje usluga Identify nakon uspješno dovršenog primjenjivog postupka provjere identiteta. Sadržava provjerene identifikacijske atribute i metapodatke, uključujući pripadajući LoIP. Može postojati i koristiti se bez Walleta te nije PID EUDI Walleta izdan na temelju prava Unije ili nacionalnog prava. |
| PID LoIP                      | Razina pouzdanosti rezultata provjere identiteta koju dodjeljuje Identify prema mjerodavnim pravilima. Wallet je ne izračunava niti mijenja. Razlikuje se od autentikacijskog režima Walleta i eIDAS LoA-e.                                                                                                                                                    |
| Autentikacijski režim Walleta | Kombinacija faktora i transakcijskih kontrola ostvarena za određenu operaciju Walleta. Sama po sebi nije eIDAS LoA.                                                                                                                                                                                                                                            |
| Pouzdana strana               | Strana koja prima i pouzda se u rezultat autentikacije Walleta, odobrene PID atribute ili drugi dopušteni izlaz Walleta.                                                                                                                                                                                                                                       |
| Poslovni klijent              | Organizacija koja je na temelju ugovora integrirana s uslugom Identityum Identify, Walletom ili povezanim uslugama.                                                                                                                                                                                                                                            |
| Povezana usluga povjerenja    | Usluga povjerenja čiji se zahtjev ili operacija može inicirati ili autorizirati putem Walleta, ali koja ima zasebnu politiku i životni ciklus.                                                                                                                                                                                                                 |

Oznake AUTH-A do AUTH-E označavaju autentikacijske mehanizme definirane u kontroliranoj dokumentaciji o autentikaciji Walletom. ANSign, NAuth i QNSign označavaju zasebne certifikacijske profile definirane primjenjivim CP-om i TSPS-om.



## 1.9. Upravljanje dokumentom, odobravanje i upravljanje izmjenama

Vlasnik dokumenta koordinira periodični pregled, usklađenost s povezanom dokumentacijom, kontrolu verzija, odobravanje i objavu. Pregled se provodi najmanje jednom godišnje i nakon svake bitne promjene usluge, pravnog okvira, sigurnosti, arhitekture ili opsega.

U svakoj odobrenoj verziji navode se oznaka verzije, datum stupanja na snagu, vlasnik, osoba ili tijelo koje ju je odobrilo, javni repozitorij i opis izmjena. Zamijenjene javne verzije čuvaju se u arhivi dokumentacije u skladu s Identyumovim pravilima upravljanja kontroliranom dokumentacijom.



## 2. Model i granice usluge Identityum Wallet

### 2.1. Opis usluge ID Walleta

ID Wallet je poslužiteljska usluga kojom upravlja Identityum i koja je dostupna putem podržanih web i mobilnih sučelja. Korisniku omogućuje uspostavu autentikacijskih faktora Walleta, autentikaciju i autorizaciju dopuštenih operacija, upravljanje podržanim podacima te, ako Korisnik tako odabere, pohranu i predstavljanje Identityum PID-a.

Wallet je modularan. Izrada Walleta, izdavanje PID-a u usluzi Identify, pohrana ili povezivanje PID-a s Walletom, zahtjev za povezanu uslugu povjerenja, izdavanje certifikata i stavljanje certifikata na raspolaganje zasebni su događaji s odvojenim dokazima i životnim ciklusima. Dovršenje jednog događaja ne znači odabir ili dovršetak drugoga.

### 2.2. Kanonski objekti i njihovo razdvajanje

| Objekt                       | Primarna funkcija                                                                               | Neovisan status ili životni ciklus                                                                                                                      |
|------------------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wallet                       | Autentikacija, autorizacija i pristup zaštićenim podacima                                       | Aktivan, suspendiran ili trajno zatvoren/opozvan                                                                                                        |
| Autentikacijski faktor       | Provjera znanja, posjedovanja, kontrole računa ili biometrijskog svojstva                       | Uspostavljen, dostupan, blokiran, zamijenjen ili uklonjen                                                                                               |
| Identityum PID               | Strukturirani rezultat usluge Identify: provjereni identifikacijski atributi, podrijetlo i LoIP | Izdaje ga i ažurira Identify; može postojati bez Walleta, biti transakcijski upotrijebljen ili se prema odabiru Korisnika pohraniti/povezati s Walletom |
| Dokazi o provjeri identiteta | Dokaz o Identify postupku ili o postupku usluge povjerenja; nije aktivni sadržaj Walleta        | Čuva se zasebno prema mjerodavnim pravilima Identifyja ili TSPS-a, neovisno o pohrani ili uklanjanju PID-a iz Walleta                                   |
| Certifikat                   | Funkcija autentikacije ili potpisivanja specifična za profil                                    | U obradi, aktivan, istekao ili opozvan; suspenzija certifikata nije podržana                                                                            |
| Privatni ključ               | Kriptografska operacija specifična za profil                                                    | Zaštićen, uporabljiv, blokiran ili uništen prema primjenjivom životnom ciklusu ključa                                                                   |

Logičko ili tehničko povezivanje objekata ne spaja njihove pravne ili operativne životne cikluse. Primjerice, uklanjanjem PID-a iz sadržaja Walleta ne brišu se zasebno čuvani dokazi za postojeći certifikat niti se samo zbog toga mijenja status tog certifikata.



## 2.3. Funkcionalni načini rada Walleta

### 2.3.1. Prazan Wallet odnosno Wallet samo za autentikaciju

Prazan Wallet ne sadržava Identityum PID i ne daje tvrdnju o provjerenom identitetu osobe. Njime se može utvrditi da je isti autentikacijski kontekst Walleta pod kontrolom osobe koja je ispunila zahtijevane faktore te se može vratiti pseudonimni identifikator specifičan za Pouzdajuću stranu, poveznica s transakcijom i ostvareni autentikacijski režim Walleta.

Rezultat koji se odnosi samo na autentikaciju nije elektronička identifikacija u smislu koji se primjenjuje na prijavljeni eID sustav, nema eIDAS LoA-u i ne smije se tumačiti kao potvrda osobnog imena, nacionalnog identifikatora, PID LoIP-a ili drugog identifikacijskog atributa.

### 2.3.2. Wallet s pohranjenim Identityum PID-om

Ako je Korisnik uspješno dovršio odobreni postupak provjere identiteta i odabere pohraniti izdani Identityum PID u Wallet, Wallet može ovlaštenoj Pouzdajućoj strani predstaviti odabrane provjerene attribute. Autentikacija i otkrivanje PID-a ostaju zasebni koraci.

### 2.3.3. Wallet koji se koristi s povezanim certifikatom

Wallet se može koristiti za autentikaciju i autorizaciju uporabe zasebno izdanog ANSign, NAuth ili QNSign certifikata čak i ako PID na kojem se certifikat temelji nije pohranjen kao aktivni sadržaj Walleta. Ispunjavanje uvjeta ovisi o aktivnom Walletu, odgovarajućim dokazima o provjeri identiteta, statusu certifikata, dostupnosti ključa i zahtjevima primjenjivog profila.

### 2.3.4. Posebne eID vjerodajnice i vanjski regulatorni statusi

Posebna eID vjerodajnica ili integracija uređuje se vlastitim profilom i dokumentacijom te se ne izvodi iz samog postojanja Walleta, PID-a ili broja autentikacijskih faktora. Tvrdnja o prijavljenom eID sredstvu, eIDAS LoA-i ili EUDI Wallet statusu dopuštena je tek nakon dovršetka svih primjenjivih vanjskih postupaka ocjenjivanja, odobrenja ili prijave.

## 2.4. Sudionici i uloge

Glavni su sudionici Korisnik, Identityum, Poslovni klijenti, Pouzdajuće strane, pružatelji povezanih usluga povjerenja, vanjski dobavljači te nadležna revizijska ili nadzorna tijela. Jedan subjekt može obavljati više uloga, ali odgovornosti se utvrđuju zasebno za svaku funkciju.

Ugovorni odnos za Wallet sklapa se izravno između Identityuma i Korisnika. Poslovni klijent može omogućiti ili onemogućiti prikaz ponude Walleta u svojem integriranom Identify tijeku, ali ne može izraditi Wallet niti sklopiti odnos za Wallet u ime Korisnika bez njegova izričitog odabira.



## 2.5. Granice usluge i tehničke granice

Granica pod nadzorom Identityuma uključuje pozadinski sustav Walleta, zapise o autentikacijskim faktorima, zaštićeni sadržaj Walleta, poslužiteljsku biometrijsku provjeru, sučelja Pouzdajućih strana, upravljanje statusima, nadzor i revizijske dokaze. Podržani uređaj Korisnika pruža sučelje i može sadržavati autentikacijski materijal vezan uz uređaj, ali ne sadržava cjelokupnu uslugu Walleta.

Wallet nije QSCD. Kvalificirani potpisni ključevi i operacije izrade potpisa pripadaju zasebno uređenoj granici udaljenog QSCD-a i usluge povjerenja. Wallet osigurava dopuštenu autentikaciju i autorizaciju transakcije potrebnu za pozivanje te usluge.

## 2.6. Normativne funkcionalnosti Walleta (TO-BE)

Normativni dio ovog Pravilnika opisuje kanonsko ciljno ponašanje Walleta kao važeću praksu: izradu praznog Walleta, autentikaciju i autorizaciju Walletom, neobvezno pokretanje ili nastavak usluge Identify, neobveznu pohranu ili povezivanje i predstavljanje Identityum PID-a, pseudonimnu B2B prijavu te definirana sučelja s povezanim uslugama.

Ovaj TO-BE pristup ne predstavlja tvrdnju da je dovršena ocjena sukladnosti, dodijeljen kvalificirani status, proveden upis na Trusted List ili da je vanjski regulirani profil već stavljen u kvalificirani produkcijski rad. Takve se činjenice utvrđuju isključivo mjerodavnom dokumentacijom, odlukama i evidencijama za predmetnu uslugu.

## 2.7. Funkcije izvan opsega Walleta i vanjski uvjeti

COL-C i COL-D načini su usluge Identify, a Identityum SMS, WEB i MOBILE zasebne su vjerodajnice ili profili; njihovo definiranje, dokazivanje i status nisu uređeni ovim Pravilnikom. Wallet uređuje samo izričito definirano sučelje prema takvoj funkciji kada se ona koristi putem Walleta.

Vanjski regulirani status ili kvalificirana funkcija smije se javno tvrditi tek nakon odgovarajuće ocjene sukladnosti, regulatornog odobrenja ili drugog primjenjivog vanjskog preduvjeta. Do tada dokument normativno opisuje arhitekturu i kontrole TO-BE sustava, ali ne pripisuje nedovršeni vanjski status.

## 2.8. Dopuštene i zabranjene uporabe

Ovisno o tome ispunjava li Korisnik uvjete i o primjenjivom ugovoru s Pouzdajućom stranom, Wallet se može koristiti za autentikaciju kontrole nad Walletom, pseudonimnu prijavu specifičnu za Pouzdajuću stranu, autorizaciju povezane operacije, pohranu i predstavljanje odabranih PID atributa te upravljanje podržanim autentikacijskim faktorima i podacima Walleta. Wallet se ne smije koristiti za lažno predstavljanje kao druga osoba, prijenos kontrole neovlaštenoj osobi, zaobilaženje sigurnosnih kontrola, davanje lažnih podataka, ponovnu



uporabu tvrdnje izvan njezine namijenjene publike ili razdoblja valjanosti ni za prikazivanje rezultata koji se odnosi samo na autentikaciju kao provjerenog identiteta osobe ili formalne eIDAS LoA-e.

## 2.9. Pretpostavke i ograničenja pouzdanja

Od Korisnika se očekuje da štite svoje uređaje i faktore, provjere identitet i zahtjev Pouzdajuće strane, potvrđuju samo namjeravane operacije te bez nepotrebnog odgađanja prijave gubitak, kompromitaciju ili sumnjivu aktivnost.

Pouzdanjuće strane i dalje su odgovorne za validaciju cjelovitosti, izdavatelja, namijenjene publike, reference transakcije, valjanosti i statusa svakog rezultata te za utvrđivanje jesu li otkriveni atributi, PID LoIP, svježina i autentikacijski kontekst dovoljni za njihovu svrhu.

Identityum ne jamči da će Wallet prihvatiti svaka javna ili privatna usluga, da Wallet zamjenjuje identifikacijsku ispravu koju je izdalo javno tijelo, da je prijavljeno eID sredstvo ili da je europski novčanik za digitalni identitet.





### 3. Podnošenje zahtjeva, uspostava autentikacijskih faktora i izrada Walleta

#### 3.1. Izravno pokretanje i B2B ponuda Walleta

Tijek izrade Walleta može se pokrenuti izravno putem odobrenog Identityumova sučelja ili prikazati nakon uspješnog Identify tijeka provedenog za Poslovnog klijenta. Poslovni klijent može ugovorno odrediti prikazuje li se ponuda Walleta, ali ponuda ostaje odvojena od odluke Poslovnog klijenta o onboardingu.

Prikaz ponude ne dovodi do izrade Walleta. Izrada Walleta započinje tek kada Korisnik izričito zatraži Wallet i stupi u izravni odnos za Wallet s Identityumom.

#### 3.2. Dobrovoljan odabir Korisnika

Izrada i uporaba Walleta dobrovoljne su. Poslovni klijent može odrediti posljedice Korisnikova odabira unutar vlastite usluge, ali ne smije prikazivati izradu Walleta kao zahtjev Identityuma ako Korisnik nije odabrao stupiti u odnos za Wallet.

Odbijena ili napuštena ponuda Walleta ne poništava inače dovršen rezultat usluge Identify niti sprječava uporabu rezultata u transakciji za koju je dobiven, uz primjenu odgovarajućih pravila Poslovnog klijenta i provjere identiteta.

#### 3.3. Informacije, Uvjeti korištenja Walleta i obavijest o privatnosti

Prije izrade Walleta Korisniku se u čitljivom obliku omogućuje pristup primjenjivim Uvjetima korištenja Walleta, Pravilima privatnosti, glavnim značajkama usluge, obveznim autentikacijskim faktorima, sigurnosnim preporukama i dostupnim kanalima podrške.

Korisnik obavlja izričitu i evidentiranu radnju prihvata Uvjeta korištenja Walleta. Prihvat odnosa za Wallet odvojen je od svakog naknadnog ugovora s Pretplatnikom ili radnje prihvata certifikata za povezanu uslugu povjerenja.

#### 3.4. Registracijski podaci za prazan Wallet

Za izradu praznog Walleta zahtijeva se najmanji opseg podataka o računu i komunikacijskih podataka potrebnih za izradu, zaštitu i rad usluge. Identityum prije aktivacije provjerava broj mobilnog telefona ili adresu e-pošte odabranu kao jedinstveni identifikator računa Walleta.

Identityum za samu izradu praznog Walleta ne zahtijeva podatke iz identifikacijske isprave, osobno ime ni rezultat provjere identiteta. Podaci prikupljeni samo radi uspostave računa Walleta ne smiju se opisivati kao provjereni podaci o identitetu osobe.



### 3.5. Uspostava AUTH-A i AUTH-D

Tijekom izrade novog Walleta Korisnik u okviru jedne povezane sesije uspostave određuje sljedeće obvezne primarne autentikacijske faktore:

- a) AUTH-A — PIN ID Walleta, kao faktor znanja; i
- b) AUTH-D — Identityum biometrija lica, kao biometrijski faktor.

Svi faktori koji čine događaj uspostave moraju se dovršiti unutar najduljeg trajanja povezane sesije definiranog kontroliranim pravilnikom o autentikaciji. Ako oba obvezna faktora nisu uspostavljena, Wallet se ne može aktivirati.

Ako su dostupni, mogu se uspostaviti podržani dodatni faktori. Njihovo dodavanje ne zamjenjuje obveznu početnu uspostavu AUTH-A i AUTH-D i ne stvara provjereni identitet osobe.

### 3.6. Značenje AUTH-D u praznom Walletu

Za prazan Wallet AUTH-D se sastoji od provjere živosti i uspostave zaštićenog biometrijskog prikaza za naknadnu autentikaciju Walletom. Njime se potvrđuje kontinuitet autentikacijskog konteksta Walleta kada se naknadna snimka žive osobe uspješno usporedi s tim prikazom.

Uspostava AUTH-D za prazan Wallet ne uključuje usporedbu s fotografijom iz identifikacijske isprave, ne dokazuje identitet Korisnika, ne izdaje Identityum PID i ne uspostavlja niti povećava PID LoIP.

### 3.7. Izrada i aktivacija praznog Walleta

Wallet se izrađuje i postaje aktivan nakon što je provjereni kontaktni identifikator povezan s računom, nakon što su uspostavljeni obvezni faktori Walleta i prihvaćeni Uvjeti korištenja Walleta. Za tu aktivaciju nije potrebna zasebna odluka o provjeri identiteta.

Aktivan prazan Wallet može se koristiti samo za funkcije koje ne zahtijevaju PID atribute ni drugu zasebno uspostavljenu tvrdnju o identitetu. Može autentificirati kontrolu nad Walletom, omogućiti pseudonimnu prijavu specifičnu za Pouzdajuću stranu i autorizirati dopuštene povezane operacije.

### 3.8. Identifikator Walleta i pravilo jedinstvenosti

Svaki Wallet ima interni neopisni identifikator i jedan provjereni broj mobilnog telefona ili adresu e-pošte koji se koriste kao jedinstveni identifikator računa. Za isti provjereni broj mobilnog telefona ili istu provjerenu adresu e-pošte istodobno se može izraditi samo jedan Wallet.

Pravilo se temelji na identifikatoru računa, a ne na osobi. Fizička osoba koja kontrolira više provjerenih brojeva mobilnog telefona ili adresa e-pošte može imati više Walleta. Zasebni Walleti ne spajaju se automatski ni ručno.



Interni identifikator Walleta ne otkriva se kao zajednički identifikator među klijentima. Kada je potreban stabilan identifikator za prijavu u privatnom sektoru, koriste se pseudonimni identifikatori specifični za pojedinu Pouzdajuću stranu.

### 3.9. Povezivanje uređaja i autentikatora

Osnovni Wallet ne smatra se trajno vezanim uz jedan uređaj opće namjene. Korisnik mu može pristupiti putem podržanog sučelja nakon dovršetka autentikacije zahtijevane za tu operaciju. Ako je registriran AUTH-E ili drugi autentikator specifičan za uređaj, pripadajući kriptografski ili autentikacijski materijal veže se uz taj autentikator i njime se upravlja kao zasebnim faktorom. Za registraciju novog faktora potrebna je autentikacija definirana u kontroliranom Pravilniku o autentikaciji putem ID Walleta.

### 3.10. Dokazi o uspostavi i revizijski trag

Identyum evidentira dovoljno dokaza za rekonstrukciju izrade Walleta, uključujući provjereni identifikator računa, primjenjive verzije dokumenata, radnju prihvata, vrste uspostavljenih faktora, relevantne identifikatore transakcije i sesije, vremenske oznake, ishode i svako iznimno postupanje.

Dokazi potvrđuju izradu i kontrolu računa Walleta. Ne smiju se označavati kao dokazi o provjeri identiteta osobe ako odobreni postupak provjere identiteta nije zasebno dovršen.

### 3.11. Neuspjela, prekinuta i ponovljena uspostava

Wallet se ne aktivira ako Korisnik napusti postupak, ne prođe provjeru odabranog identifikatora računa, ne uspostavi obvezni faktor ili ne dovrši zahtijevanu radnju prihvata.

Ponovni pokušaji, ograničenja učestalosti i mjere privremene odgode primjenjuju se u skladu s kontroliranim pravilima autentikacije i sprječavanja prijevara. Neuspjela uspostava praznog Walleta ne smije stvoriti PID niti se prikazati kao neuspješna odluka o provjeri identiteta ako provjera identiteta nije ni pokušana.



## 4. Sučelje Walleta prema usluzi Identify i Identityum PID-u

### 4.1. Pokretanje ili nastavak usluge Identify iz Walleta

Korisnik u Walletu može zasebno odabrati pokretanje ili nastavak postupka Identify radi dobivanja ili osvježavanja identitetskog rezultata. Wallet ostaje uporabljiv bez tog odabira, a pokretanje Identifyja ne mijenja njegov status niti praznom Walletu daje tvrdnju o građanskom identitetu.

Zahtjev se predaje Identifyju uz podatke potrebne za povezivanje sesije i povrat rezultata. Wallet ne provodi provjeru identiteta, ne odlučuje o njezinu uspjehu i ne dodjeljuje LoIP.

### 4.2. Funkcionalna i dokumentacijska granica Identifyja

Identify je zasebna Identityumova usluga koja prikuplja, validira, povezuje i ocjenjuje dokaze te, kada su ispunjeni uvjeti, izdaje Identityum PID. Mjerodavna pravila postupaka, use caseova, izvora dokaza, odluke, LoIP-a i dokaznog paketa utvrđuju se TSPS-om kada se Identify koristi u kontekstu usluge povjerenja te odgovarajućom dokumentacijom Identifyja u drugim kontekstima.

Wallet je samo kanal pokretanja i povrata te, prema zasebnom odabiru Korisnika, okruženje za pohranu ili povezivanje, prikaz i predstavljanje rezultata. Zahtjevi ETSI TS 119 461 koji se odnose na identity-proofing service, njegove use caseove, dokaze i odluke ne ispunjavaju se ovim Pravilnikom Walleta.

### 4.3. Identify tijekom neovisni o postojanju Walleta

Identify se može pokrenuti izravno, iz tijeka Poslovnog klijenta, iz Walleta ili iz drugog odobrenog kanala. Postojanje Walleta nije preduvjet za provedbu Identifyja ni za izdavanje PID-a.

Rezultat Identifyja može se upotrijebiti samo u tekućoj transakciji ili se, ako je izdani PID namijenjen ponovnoj uporabi, naknadno povezati s Walletom na temelju zasebnog odabira Korisnika. Uspješnim Identifyjem Wallet se ne izrađuje automatski.

### 4.4. Rezultat Identifyja dostupan Walletu

Wallet prihvaća samo strukturirani rezultat koji Identify izda za dopušteni kontekst i samo u opsegu potrebnom za odabranu funkciju Walleta. Rezultat može biti PID namijenjen ponovnoj uporabi ili transakcijski rezultat koji se koristi bez pohrane u Wallet.

Wallet provjerava tehničku autentičnost, cjelovitost, namijenjeni kontekst i status primljenog rezultata. Ne preispituje dokaznu odluku Identifyja, ne utvrđuje prihvatljive izvore dokaza i iz primljenih podataka samostalno ne izračunava LoIP.



#### 4.5. Pohrana ili povezivanje rezultata na strani Walleta

Ako Korisnik odabere pohranu ili povezivanje PID-a, Wallet ga veže uz odgovarajući autentikacijski kontekst te čuva njegov sadržaj ili sigurnu referencu u skladu s arhitekturom usluge. Ta radnja ne mijenja PID niti dokaznu odluku Identifyja.

Prikupljanje dokaza, provjera živosti, biometrijska usporedba s identifikacijskim dokumentom, unakrsne provjere i dokazni pragovi pripadaju Identifyju. AUTH-D Walleta zaseban je autentikacijski faktor; sam po sebi ne dokazuje građanski identitet i ne prenosi dokaznu vrijednost na rezultat Identifyja.

Wallet evidentira pokretanje, povrat, odabir pohrane ili povezivanja i rezultat tehničke obrade na strani Walleta. Ograničenja pokušaja, pragove i razloge identity-proofing odluke evidentira Identify u svojem dokaznom sustavu.

#### 4.6. LoIP kao metapodatak rezultata Identifyja

Identify utvrđuje ishod provjere identiteta i dodjeljuje LoIP prema mjerodavnim pravilima. Wallet prima, čuva i predstavlja tu oznaku uz PID, ali je ne izračunava, ne povećava i ne smanjuje.

LoIP izražava pouzdanost rezultata provjere identiteta i nije autentikacijski režim Walleta ni eIDAS LoA. ETSI TS 119 461 definira Baseline i Extended LoIP; svaka Identityumova interna podrazina Extended područja mora biti definirana i mapirana u mjerodavnom TSPS-u ili dokumentaciji Identifyja, a ne kao zasebna ETSI razina u ovom Pravilniku.

#### 4.7. Izdavanje PID-a neovisno o Walletu

Nakon uspješne odluke Identify izdaje Identityum PID s provjerenim atributima i potrebnim metapodacima o podrijetlu, vremenu i LoIP-u. PID može postojati i koristiti se bez Walleta.

Wallet ne izdaje, ne potpisuje kao izdavatelj i ne mijenja sadržaj PID-a. Naziv Identityum PID oznaka je proizvoda i ne predstavlja tvrdnju da je riječ o PID-u EUDI Walleta ili identifikacijskim podacima izdanim na temelju prava Unije ili nacionalnog prava.

#### 4.8. Razdvajanje izdavanja PID-a i njegove dostupnosti u Walletu

Izdavanje PID-a u Identifyju i njegova pohrana ili povezivanje s Walletom zasebni su, neovisno evidentirani događaji. Nakon izdavanja Korisniku se prikazuju relevantni podaci i zasebno se traži odluka želi li PID učiniti dostupnim kroz Wallet.

Odbijanje pohrane ili povezivanja ne poništava PID ni rezultat Identifyja. Rezultat se može koristiti u dopuštenoj tekućoj transakciji ili kao ulaz u zasebno uređeni postupak usluge povjerenja, dok se dokazni paket čuva izvan aktivnog sadržaja Walleta.



#### 4.9. Neovisni odabiri PID-a i povezanih usluga

Nakon uspješnog Identifyja Korisnik neovisno odlučuje hoće li PID pohraniti ili povezati s Walletom i hoće li zasebno zatražiti povezanu uslugu povjerenja. Nijedna od tih odluka nije automatska posljedica druge.

Sučelje jasno razdvaja pohranu/povezivanje PID-a, predstavljanje PID-a, zahtjev za uslugu povjerenja, pretplatnički ugovor i svaku autorizaciju uporabe ključa. Primjenjivi profili i kriteriji prihvatljivosti utvrđuju se CP-om i TSPS-om, a svaka radnja i njezin rezultat zasebno se evidentiraju.

#### 4.10. Svježina PID-a i upućivanje na novi Identify postupak

Wallet može ponuditi ponovno predstavljanje dostupnog PID-a samo ako njegovi metapodaci o izvoru, LoIP-u, vremenu, statusu i atributima zadovoljavaju zahtjev konkretne transakcije i ako je Korisnik tu transakciju zasebno autorizirao.

Ako PID nije dostatan, Wallet zaustavlja predstavljanje ili Korisnika upućuje u odgovarajući Identify tijek. Samo Identify može provesti dodatnu provjeru i izdati novi ili ažurirani rezultat s novom odlukom i LoIP-om; Wallet nakon toga ažurira vlastitu kopiju ili referencu prema odabiru Korisnika.

#### 4.11. Dokazi Identifyja i usluga povjerenja izvan Walleta

Dokaze o provjeri identiteta čuva Identify odnosno dokazni sustav QTSP-a kada se rezultat koristi za uslugu povjerenja. Dokazi o pretplatniku, certifikatu i potpisu čuvaju se u sustavima usluge povjerenja. Nijedna od tih kategorija nije aktivni sadržaj Walleta.

Uklanjanjem ili brisanjem PID-a iz Walleta ne brišu se zasebno čuvani dokazi niti se samim time opoziva certifikat. Obrnuto, čuvani dokazi ne postaju dostupni kao aktivni sadržaj Walleta i ne omogućuju predstavljanje PID-a nakon njegova uklanjanja.

#### 4.12. Neuspjeli i ručno obrađeni postupci Identifyja

Ako Identify vrati neuspjeh, prekid ili rezultat koji nije namijenjen pohrani ili predstavljanju, Wallet ne stvara niti mijenja PID. Korisniku prikazuje dopušteni status i eventualni sljedeći korak, a detaljni razlog i dokaz ostaju u sustavu Identifyja.

Ručni pregled, zamjenski postupak i odluka o LoIP-u pripadaju Identifyju i provode se samo prema njegovoj mjerodavnoj dokumentaciji. Wallet ne omogućuje ručno nadjačavanje te odluke.



## 5. Svojstva autentikacije i sigurnosni model Walleta

### 5.1. Prazan Wallet kao autentikacijski kontekst

Prazan Wallet jest kontekst za autentikaciju i autorizaciju povezan s verificiranim brojem mobilnog telefona ili adresom e-pošte, internim identifikatorom Walleta i autentikacijskim faktorima Walleta. Ne sadržava Identyum PID niti njime nastaje verificirana tvrdnja o građanskom identitetu.

Osoba koja kontrolira prazan Wallet može se autentificirati prema Identyumu ili ugovorno povezanoj Pouzdajućoj strani iz privatnog sektora s pomoću pseudonimnog identifikatora specifičnog za tu Pouzdajuću stranu. Rezultat potvrđuje uspješnu autentikaciju Walletom za određenu transakciju; njime se osoba ne identificira na temelju građanskog identiteta.

### 5.2. Rezultati autentikacije bez identifikacije

Rezultat autentikacije bez identifikacije može sadržavati Identyum kao izdavatelja, namjeravanu Pouzdajuću stranu ili publiku, pseudonimni identifikator specifičan za Pouzdajuću stranu, podatke o vremenu i valjanosti, vezivanje uz transakciju te postignuti autentikacijski režim Walleta.

Ne smije sadržavati niti implicirati građansko ime, nacionalni identifikator, Identyum PID, LoIP PID-a ili eIDAS LoA-u, osim ako su ti podaci ili tvrdnje zasebno utvrđeni, zatraženi i autorizirani prema primjenjivom profilu usluge.

### 5.3. Uvjeti za sredstvo elektroničke identifikacije

Postojanjem Walleta ili uspješnom autentikacijom Walletom ne nastaje automatski sredstvo elektroničke identifikacije. Ako Identyum naknadno izda ili omogući posebno definiranu eID vjerodajnicu, u primjenjivoj dokumentaciji sustava moraju se utvrditi potpuno sredstvo, njegovi osobni identifikacijski podaci, pravila izdavanja i životnog ciklusa, autentikacijski mehanizam te svaka formalno ocijenjena razina pouzdanosti.

NAuth je certifikat za autentikaciju utemeljenu na certifikatu. Nije automatski prijavljeno sredstvo elektroničke identifikacije i nema formalnu eIDAS LoA-u, osim ako je takav status izričito utvrđen posebnim odobrenim eID sustavom ili integracijom.

### 5.4. Autentikacijski režim, LoIP PID-a i eIDAS LoA

| Pojam                         | Što izražava                                                                  | Što sam po sebi ne utvrđuje                     |
|-------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------|
| Autentikacijski režim Walleta | Faktore i kontrole transakcije koji su uspješno provedeni za radnju u Walletu | Građanski identitet, LoIP PID-a ili eIDAS LoA-u |



| Pojam                 | Što izražava                                                                                           | Što sam po sebi ne utvrđuje                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| LoIP Identityum PID-a | Pouzdanost rezultata i dokaza provjere identiteta                                                      | Sigurnost autentikacijskog sredstva ili eIDAS LoA-u                        |
| Profil certifikata    | Dopuštenu namjenu ključa i certifikata te zahtjeve politike                                            | Status prijavljenog eID sredstva                                           |
| eIDAS LoA             | Cjelovitu pouzdanost eID sredstva u pogledu upisa, upravljanja sredstvom, autentikacije i organizacije | Rezultat izveden isključivo iz dvofaktorske autentikacije ili LoIP-a PID-a |

Identityum ne preslikava automatski razine LoIP-a PID-a ili kombinacije faktora Walleta na eIDAS razine Low, Substantial ili High. Svako formalno preslikavanje zahtijeva potpunu ocjenu svih primjenjivih elemenata pouzdanosti i izričitu kontroliranu tvrdnju u mjerodavnoj dokumentaciji eID sustava.

## 5.5. Autentikacijski faktori i kategorije

| Oznaka | Autentikacijski faktor                                                                   | Operativna kategorija                                                |
|--------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| AUTH-A | PIN ID Walleta                                                                           | Znanje                                                               |
| AUTH-B | Verificirani broj mobilnog telefona i dokazana kontrola povezanog komunikacijskog kanala | Posjedovanje ili kontrola kanala, ovisno o provedbi predmetne radnje |
| AUTH-C | Verificirana adresa e-pošte, Google račun ili Apple račun                                | Kontrola vanjskog računa                                             |
| AUTH-D | Identityum biometrija lica                                                               | Svojstvenost                                                         |
| AUTH-E | Identityum mobilni autentikator                                                          | Posjedovanje povezanog autentikatora                                 |

AUTH-A i AUTH-D obvezni su pri početnoj izradi Walleta. Dodatni faktori mogu se uspostaviti i upotrebljavati samo za radnje za koje ih dopušta kontrolirana autentikacijska politika.

## 5.6. Dopuštene kombinacije faktora

Kombinacija faktora odabire se prema zatraženoj radnji, kontroliranoj autentikacijskoj politici Walleta, sigurnosnoj postavci koju je odabrao Korisnik, zahtjevima Pouzdajuće strane i riziku transakcije. Svi faktori koji čine jedan autentikacijski događaj moraju se provesti tijekom iste dopuštene povezane sesije.

| Radnja               | Zadani zahtjev  |
|----------------------|-----------------|
| Izrada novog Walleta | AUTH-A + AUTH-D |





| Radnja                                                         | Zadani zahtjev                                                                  |
|----------------------------------------------------------------|---------------------------------------------------------------------------------|
| Dodavanje ili izmjena identifikacijskih podataka               | AUTH-A + AUTH-D; dodatno AUTH-E kada se primjenjuje stroži režim                |
| Predstavljanje PID-a ili dijeljenje identifikacijskih podataka | AUTH-A + AUTH-D ili AUTH-E, ovisno o primjenjivoj politici i postavci Korisnika |
| Pseudonimna prijava Walletom                                   | AUTH-A + odobreni drugi faktor za tu transakciju                                |
| Radnja u Walletu višeg rizika                                  | AUTH-A + AUTH-D + AUTH-E kada je potrebno                                       |
| Autorizacija transakcije QNSign/QES s pomoću AUTH-E            | Isključivo mrežni push mehanizam izazov–odgovor                                 |

Može se zahtijevati snažnija kombinacija faktora, ali uspješnim provođenjem snažnije kombinacije samim se po sebi ne povećava LoIP PID-a niti nastaje formalna eIDAS LoA.

## 5.7. Komponente Walleta, uređaja i poslužiteljske strane

Wallet radi putem podržanih korisničkih sučelja i komponenti na poslužiteljskoj strani pod kontrolom Identityuma. U poslužiteljskom okruženju upravlja se zaštićenim sadržajem Walleta, zapisima o autentikaciji, biometrijskom usporedbom, statusom, interakcijama s Pouzdajućim stranama i dokazima.

Korisnički uređaj opće namjene ostaje izvan izravne administrativne kontrole Identityuma. Materijal AUTH-E vezan uz uređaj generira se i štiti za registrirani autentikator te se ne smatra zamjenjivim s centralno zaštićenim privatnim ključevima certifikata.

## 5.8. Granice vjerodajnica i kriptografskih ključeva

Autentikacijski ključevi, ključevi certifikata, ključevi za zaštitu podataka Walleta i ključevi usluge imaju posebne namjene. Ključ koji se upotrebljava za jednu funkciju ne smije se prikazivati niti ponovno upotrebljavati kao ključ drugog profila samo zato što te funkcije dijele tehničku infrastrukturu.

Generiranje, zaštita i uporaba privatnih ključeva pretplatnika, uključujući HSM/SAM, udaljeni QSCD, SAD i mehanizme kojima se dokazuje sole control, uređuju se TSPS-om i dokumentacijom udaljene usluge potpisivanja. Wallet može prenijeti autentikacijski rezultat i potvrdu konkretne transakcije, ali sam nije QSCD niti se iz samih faktora Walleta izvodi ispunjenje zahtjeva za kvalificirani potpis.

NAAuth je autentikacijski certifikat i ne upotrebljava se za izradu elektroničkih potpisa. ANSign i QNSign potpisni su profili uređeni pripadajućim politikama. Detaljne informacije o upravljanju ključevima i certificiranim uređajima ostaju u TSPS-u i kontroliranim postupcima.



## 5.9. Zaštita od umnožavanja, neovlaštene izmjene i ponovnog izvođenja

Autentikacijski kontekst Walleta štiti se kombinacijom kontrole faktora ili vjerodajnice na poslužiteljskoj strani, višefaktorske autentikacije, privatnih ključeva koje nije moguće izvesti, vezivanja uz transakciju i provjere statusa.

Kopirano korisničko sučelje ili poznavanje identifikatora Walleta nisu dovoljni za reprodukciju autentikacijskog konteksta Walleta. Upotreba Walleta zahtijeva i uspješnu provjeru primjenjivih autentikacijskih faktora te valjane faktore ili vjerodajnice na poslužiteljskoj strani.

Ključevi mobilnog autentikatora vezani uz uređaj generiraju se zasebno za svaki registrirani uređaj i čuvaju u zaštićenoj kriptografskoj pohrani uređaja. Registracija novog autentikatora zahtijeva autentikaciju putem postojećeg Walleta.

U autentikacijskim transakcijama upotrebljavaju se kratkotrajni podaci sesije ili izazova, a transakcije se vežu uz uslugu koja ih zahtijeva i namjeravanu radnju. Prethodno upotrijebljeni jednokratni faktor ili vjerodajnica, izazov ili autorizacija ne mogu se ponovno upotrijebiti kao valjano odobrenje nove transakcije.

Pseudonimni identifikatori specifični za Pouzdajuću stranu dodatno smanjuju rizik praćenja ili povezivanja među različitim Poslovnim klijentima.

Zahtjevi za autentikaciju i njihovi rezultati zaštićeni su u pogledu cjelovitosti, vremenski ograničeni te vezani uz namjeravanu Pouzdajuću stranu, publiku i transakciju. Kopirano sučelje, identifikator Walleta ili prethodni odgovor nisu dovoljni za reprodukciju valjane nove autentikacije.

## 5.10. Kontrola i posjed Korisnika

Korisnik dokazuje kontrolu Walleta kombinacijom faktora potrebnom za predmetnu radnju. Odobrenje je vezano uz prikazanog primatelja, svrhu, transakciju i opseg podataka te se ne smije smatrati općim dopuštenjem za drugu radnju.

Kontrola Walleta ne zahtijeva izravan posjed centralno zaštićenih ključeva certifikata. Uspješna autentikacija Walletom i, kada je potrebno, potvrda određene transakcije autoriziraju samo dopuštenu radnju u povezanoj kontroliranoj usluzi.

## 5.11. Zaštita pohranjenih podataka i integrirana zaštita privatnosti

Sadržaj Walleta, zapisi o autentikaciji i biometrijski prikazi zaštićeni su pri pohrani i prijenosu. Podaci se izlažu korisničkom sučelju ili ovlaštenoj Pouzdajućoj strani samo u opsegu nužnom za zatraženu i dopuštenu radnju.

Identityum za autentikacijske transakcije bez identifikacije upotrebljava pseudonimne identifikatore specifične za Pouzdajuću stranu kako bi smanjio nepotrebno povezivanje



podataka među klijentima. Autentikacijom se ne otkrivaju podaci PID-a, a otkrivanje PID-a ne uključuje dodatni sadržaj Walleta izvan autoriziranog opsega.

## 5.12. Regulatorni status i ograda od tvrdnji

ID Wallet ne predstavlja se kao europski novčanik za digitalni identitet, identifikacijska isprava koju izdaje tijelo javne vlasti niti Wallet izdan u okviru prijavljenog nacionalnog sustava elektroničke identifikacije. Primjena odabranih načela sigurnosti, privatnosti i interoperabilnosti na Wallet ne mijenja taj status.

Identityum formalnu tvrdnju o eID vjerodajnici, LoA-i, prijavi ili sukladnosti objavljuje tek nakon što budu utvrđeni pripadajući opseg, sustav i dokazi te dovršena potrebna vanjska odobrenja. Takav se status ne smije izvoditi iz marketinške terminologije, broja faktora, LoIP-a PID-a ili dostupnosti povezanog certifikata.



## 6. Upravljanje životnim ciklusom Walleta i sadržaja Walleta

### 6.1. Statusi Walleta i odvojenost povezanih objekata

Wallet, autentikacijski faktori, PID, certifikati, privatni ključevi i povezane usluge imaju odvojene statuse i događaje životnog ciklusa. Identityum održava njihove tehničke veze tako da događaj koji utječe na jedan objekt proizvodi samo učinke definirane za ovisne funkcije.

Događaj životnog ciklusa mora se zabilježiti s vremenom, inicijatorom, razlogom, objektom na koji utječe te posljedičnim statusom ili ograničenjem. Izraz za status jednog objekta ne smije se primjenjivati na drugi objekt ako odgovarajuća radnja životnog ciklusa nije stvarno provedena.

### 6.2. Redovna upotreba

Tijekom redovne upotrebe Korisnik može pregledavati podatke Walleta i upravljati njima, autentificirati se prema podržanim uslugama, autorizirati dijeljenje podataka te upotrebljavati povezane eID funkcije i funkcije usluga povjerenja.

Za svaku sigurnosno osjetljivu radnju potrebna je kombinacija autentikacije definirana za tu radnju. Svi faktori koji čine jedan autentikacijski događaj moraju se provesti tijekom iste povezane sesije, koja ne smije trajati dulje od 15 minuta.

Autentikacijom prema Walletu ne otkrivaju se sami po sebi podaci PID-a. Za otkrivanje je potreban zaseban zahtjev u kojem su navedeni Pouzdajuća strana i zatraženi podaci, nakon čega slijedi autorizacija Korisnika.

Identityum može zahtijevati snažniju autentikaciju ako radnja, Pouzdajuća strana ili primjenjiva politika usluge zahtijeva višu razinu pouzdanosti.

Prazan Wallet ostaje ograničen na funkcije autentikacije bez identifikacije i autorizacije. Upravljanje PID-om i njegovo predstavljanje postaju dostupni tek kada je PID zasebno izdan i pohranjen ili na drugi način stavljen na raspolaganje za autoriziranu transakciju.

### 6.3. Upravljanje autentikacijskim faktorima

Autentikacijski faktori mogu se dodati ili ukloniti tek nakon što se Korisnik uspješno autentificira s pomoću faktora propisanih za tu promjenu.

Za dodavanje mobilnog autentikatora potrebni su:

- PIN ID Walleta;
- biometrija lica; i
- verifikacija registriranog broja mobilnog telefona.

Korisnik može registrirati više od jednog mobilnog autentikatora.



Za uklanjanje mobilnog autentikatora potrebni su PIN i biometrija lica. Ista dvofaktorska kombinacija potrebna je za dodavanje ili uklanjanje verificiranog broja mobilnog telefona odnosno adrese e-pošte, Google računa ili Apple računa koji se upotrebljavaju kao autentikacijski faktor Walleta.

PIN se ne može ukloniti dok je Wallet aktivan. Obvezni PIN ili faktor biometrije lica može se promijeniti samo posebno podržanim sigurnosnim postupkom kojim se čuva pouzdano povezivanje s Korisnikom.

Svaka se promjena bilježi i odmah utječe na dopuštenost i upotrebu svake funkcije koja ovisi o promijenjenom faktoru.

Blokiranje ili uklanjanje faktora Walleta utječe na radnje koje zahtijevaju taj faktor. Time se samim po sebi ne suspendira certifikat jer profili Identityum certifikata ne podržavaju suspenziju certifikata.

## 6.4. Dodavanje, uklanjanje i migracija uređaja

Osnovni ID Wallet nije trajno vezan uz jedan uređaj. Korisnik mu može pristupiti s drugog podržanog uređaja nakon uspješne autentikacije prema Walletu.

Uređaj postaje posebno vezan uz Wallet kada se na njemu registrira Identityum mobilni autentikator. Registracijom nastaje novi autentikacijski faktor specifičan za uređaj i ne kopira se postojeći autentikator s drugog uređaja.

Korisnik može imati više registriranih mobilnih autentikatora. Svakim se upravlja neovisno i može se ukloniti bez uklanjanja ostalih.

Za dodavanje novog vezanog uređaja potrebna je autentikacija navedena u odjeljku 6.3. Događaji registracije i uklanjanja bilježe se u revizijskom tragu Walleta.

Budući da se podaci Walleta čuvaju na poslužiteljskoj strani, pri migraciji na novi uređaj nije potrebno prenositi PID ni drugi sadržaj Walleta između uređaja.

Korisnik s novog uređaja pristupa postojećem Walletu i, ako to želi, registrira novi mobilni autentikator. Registracijom nastaje novi kriptografski materijal specifičan za uređaj koji se povezuje s postojećim Walletom.

Nakon aktivacije novog autentikatora prethodni se autentikator može zadržati ili ukloniti u skladu s odjeljkom 6.3.

Ako je prethodni uređaj izgubljen ili postoji mogućnost njegove kompromitacije, Korisnik bi prije povratka Walleta u redovnu upotrebu trebao najprije suspendirati Wallet i ukloniti zahvaćeni autentikator.

Migracijom ili registracijom novog autentikatora ne spajaju se zasebni Walleti. Wallet povezan s drugim verificiranim brojem mobilnog telefona ili adresom e-pošte ostaje zaseban Wallet s vlastitim životnim ciklusom.



## 6.5. Promjene kontakta i identifikatora računa

Broj mobilnog telefona ili adresa e-pošte mogu biti kontaktni podatak, autentikacijski kanal i jedinstveni identifikator računa Walleta. Promjena koja utječe na jedinstveni identifikator računa dopuštena je samo posebno podržanim postupkom i nakon verifikacije novog identifikatora.

Identyum sprječava da dva aktivna Walleta upotrebljavaju isti verificirani broj mobilnog telefona ili istu verificiranu adresu e-pošte kao jedinstveni identifikator računa. Promjenom identifikatora računa Wallet se ne spaja s drugim Walletom iste osobe.

Promjenom kontakta ili identifikatora računa ne mijenjaju se verificirani atributi PID-a. Atribut koji čini dio PID-a ažurira se samo u skladu s primjenjivim postupkom validacije i ažuriranja PID-a.

## 6.6. Dodavanje, ažuriranje, zastarijevanje i uklanjanje PID-a

PID se može dodati u Wallet samo nakon uspješnog odgovarajućeg rezultata provjere identiteta i zasebnog odabira Korisnika da ga pohrani. Pri ažuriranju se bilježe novi izvor, provjere, LoIP i vrijeme te se ne prepisuje dokazni zapis prethodnog rezultata.

Zastarjelost ili nedostatnost za određeni slučaj upotrebe mogu ograničiti dijeljenje ili ponovnu upotrebu PID-a, izdavanje novog certifikata, obnovu ili transakciju za koju su potrebni noviji dokazi. Time se Wallet ili postojeći certifikat ne opozivaju automatski.

Korisnik može ukloniti PID iz aktivnog sadržaja Walleta uz autentikaciju koju zahtijeva kontrolirana politika. Uklanjanjem se postojeći certifikat ANSign, NAuth ili QNSign ne opoziva, suspendira niti blokira samo zato što PID više nije pohranjen u Walletu.

## 6.7. Suspendizacija Walleta

Suspendizacijom se privremeno blokiraju redovna autentikacija Walletom, predstavljanje PID-a, upravljanje podacima i autorizacija povezanih radnji putem Walleta. Može je pokrenuti Korisnik ili Identyum kada se utvrdi gubitak, kompromitacija, sumnjiva aktivnost, zlouporaba, pravni zahtjev ili drugi značajan rizik.

Suspendizacija Walleta onemogućuje upotrebu udaljenih ključeva vezanih uz Wallet jer se potrebna autentikacija ili autorizacija ne može provesti. Njome se povezani certifikat ne suspendira niti opoziva i putem CRL-a ili OCSP-a ne objavljuje se status suspendiranog certifikata.

Identyum tijekom sigurnosne istrage ili istrage opoziva može zasebno blokirati upotrebu upravljanog privatnog ključa. Takva tehnička blokada nije suspendizacija certifikata i ne mijenja njegov status dok se ne donese primjenjiva odluka o životnom ciklusu certifikata.



## 6.8. Ponovna aktivacija Walleta

Wallet koji je suspendirao Korisnik može se ponovno aktivirati tek nakon uspješne autentikacije kombinacijom faktora definiranom za ponovnu aktivaciju te provedbe svake potrebne zamjene ili uklanjanja kompromitiranog faktora.

Ako je suspenziju pokrenuo Identityum, Identityum prije autorizacije ponovne aktivacije može zahtijevati sigurnosni pregled, dodatnu autentikaciju, ponovno postavljanje faktora ili ponovnu provjeru identiteta. Ponovnom aktivacijom vraćaju se samo one funkcije Walleta čije su sve ovisnosti i dalje valjane.

Ponovnom aktivacijom ne može se obnoviti certifikat koji je istekao ili opozvan niti podaci PID-a koje je Korisnik prethodno uklonio iz aktivnog sadržaja Walleta.

## 6.9. Trajni opoziv ili zatvaranje Walleta

Trajni opoziv ili zatvaranje Walleta konačni su i ne mogu se poništiti. Njima se završavaju aktivne sesije, poništavaju veze autentikacijskih faktora Walleta i aktivni sadržaj Walleta čini trajno nedostupnim u skladu s pravilima brisanja.

Trajnim opozivom, brisanjem ili zatvaranjem Walleta pokreće se opoziv svih dugoročnih certifikata ANSign, NAuth i QNSign vezanih uz taj Wallet. Identityum bilježi i provodi potrebne radnje opoziva certifikata prema primjenjivoj Politici certifikata i TSPS-u.

Ta automatska posljedica ne obuhvaća QLSeal samo zato što se pojedinačni operator koristio Walletom. Certifikat QLSeal pripada pravnoj osobi i slijedi vlastiti životni ciklus certifikata i autorizacije.

## 6.10. Obnova i zamjena

Wallet se ne obnavlja periodično kao jedinstvena vjerodajnica. Njegov identifikator računa, faktori, PID, certifikati i povezane funkcije pregledavaju se ili obnavljaju prema pripadajućim pravilima.

Zamjenski Wallet potreban je ako je prethodni Wallet trajno opozvan ili se ne može održati pouzdani kontinuitet. Novi se Wallet izrađuje prema tada važećim zahtjevima i ne spaja se automatski niti smatra nastavkom drugog Walleta povezanog s drugim identifikatorom računa.

## 6.11. Oporavak pristupa

Identityum ne otkriva niti dohvaća postojeći PIN Korisnika. Oporavak je dopušten samo posebno odobrenim postupkom koji pruža dostatnu pouzdanost za zahvaćenu radnju i čuva potrebno povezivanje Walleta s Korisnikom.

Ako Korisnik ne može ispuniti zahtjeve odobrenog postupka oporavka, Identityum ne vraća pristup samo na temelju neverificiranog zahtjeva korisničkoj podršci. Wallet se trajno ukida, a novi se Wallet izrađuje ako Korisnik želi nastaviti upotrebljavati uslugu.



## 6.12. Gubitak, krađa i kompromitacija

Korisnik mora bez nepotrebnog odgađanja postupiti ako su uređaj, autentikacijski faktor ili sesija Walleta izgubljeni, ukradeni, izloženi ili se sumnja na njihovu kompromitaciju.

Odgovarajuća neposredna radnja jest suspenzija ili trajni opoziv Walleta te obavještanje korisničke podrške Identityuma.

Identityum može neovisno suspendirati Wallet ako otkrije sumnjivu aktivnost ili primi vjerodostojnu prijavu kompromitacije.

Nakon suspenzije zahvaćeni mobilni autentikator, broj mobilnog telefona ili faktor vanjskog računa može se ukloniti. Ako se kompromitacija odnosi na PIN, vezu s biometrijom lica, PID ili sam identitet Korisnika, Identityum umjesto ponovne aktivacije može zahtijevati trajni opoziv i novi upis.

Korisnik ostaje odgovoran za zaštitu uređaja i faktora sve dok se zahvaćeni pristup ne onemogućí.

Prijava koja utječe na certifikat ili upravljani privatni ključ obrađuje se zasebno prema postupcima opoziva certifikata i kontrole ključeva. Podrška za Wallet, blokiranje ključa i opoziv certifikata moraju ostati jasno razlučivi u dokazima i javnim informacijama o statusu.

## 6.13. Brisanje podataka Walleta i zadržani dokazi

Nakon trajnog zatvaranja Walleta aktivni se sadržaj Walleta briše ili čini trajno nedostupnim prema postupku brisanja Walleta. Autentikacijske veze postaju nevaljane, a kriptografski materijal specifičan za Wallet koji više nije potreban deaktivira se ili uništava prema primjenjivim pravilima.

Brisanje aktivnog sadržaja Walleta ne zahtijeva brisanje dokaza o provjeri identiteta, pretplatničkom ugovoru, certifikatu, autentikaciji, sigurnosti ili životnom ciklusu koje Identityum mora zasebno čuvati. Takvi se dokazi štite, ograničeni su svrhom i uklanjaju nakon isteka primjenjivog razdoblja čuvanja.

## 6.14. Informacije o statusu i obavijesti Korisniku

| Status Walleta              | Značenje                                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Aktivan                     | Wallet se može upotrebljavati za funkcije čije su zasebne ovisnosti i statusi valjani.                                        |
| Suspendiran                 | Redovna upotreba Walleta privremeno je blokirana; status certifikata ostaje nepromijenjen samo na temelju suspenzije Walleta. |
| Trajno opozvan ili zatvoren | Wallet se ne može ponovno aktivirati; opozivaju se dugoročni certifikati ANSign, NAuth i QNSign vezani uz njega.              |





Korisnik se putem dostupnog registriranog kanala obavještava o značajnim događajima životnog ciklusa i sigurnosti Walleta. Obavijesti o izdavanju, prihvatu, isteku i opozivu certifikata uređene su zasebno primjenjivom dokumentacijom usluga povjerenja.



## 7. Autentikacija i autorizacija s pomoću Walleta

### 7.1. Vrste autentikacijskih i autorizacijskih transakcija Walleta

| Vrsta transakcije Walleta                     | Dopušteni rezultat                                                                                                                                                   |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pseudonimna B2B prijava                       | Potvrda uspješne autentikacije Walletom s pseudonimnim identifikatorom specifičnim za Pouzdajuću stranu; bez građanskog identiteta ili eIDAS LoA-e.                  |
| Autentikacija uz predstavljanje PID-a         | Rezultat autentikacije Walletom zajedno s odabranim atributima PID-a koje je Korisnik zasebno zatražio i autorizirao.                                                |
| Autorizacija povezane usluge                  | Potvrda da je Korisnik autorizirao definiranu radnju, uključujući prihvatljivu radnju udaljenog potpisivanja.                                                        |
| Pojačana autentikacija                        | Provjera dodatnog faktora koju zahtijevaju transakcija, postavka Korisnika, Pouzdajuća strana ili politika povezane usluge.                                          |
| Autentikacija utemeljena na NAuth certifikatu | Dokaz kontrole nad NAuth ključem ako integracija izričito zahtijeva ili prihvaća NAuth certifikat; ne predstavlja automatski transakciju prijavljenim eID sredstvom. |

Identityum SMS, WEB i MOBILE, kada su definirani i omogućeni u mjerodavnim profilima, ostaju zasebne eID vjerodajnice. Ne postaju autentikacijski režimi Walleta niti im ovaj Pravilnik dodjeljuje eIDAS LoA-u.

### 7.2. Pokretanje od strane Pouzdajuće strane ili povezane usluge

Autentikaciju putem odobrenog Identityum sučelja pokreće registrirana Pouzdajuća strana ili Identityum usluga koja djeluje za definiranu transakciju.

Zahtjev sadržava, ovisno o primjenjivosti:

- Pouzdajuću stranu;
- transakciju ili sesiju;
- zatraženi autentikacijski režim Walleta ili, kada je primjenjivo, zasebno definirani zahtjev u pogledu vjerodajnice;
- radnju koju treba autorizirati;
- sve zatražene attribute PID-a;
- svrhu zahtjeva; i
- registrirano odredište odgovora na koje se rezultat treba vratiti.

Korisnik može pristupiti autentikacijskom tijeku preusmjeravanjem iz preglednika, poveznicom aplikacije, QR kodom ili drugim podržanim kanalom. Neovisno o kanalu, zahtjev mora biti sljediv do registrirane Pouzdajuće strane i određene transakcije.

Zahtjevi koji su nepotpuni, istekli, izmijenjeni ili zaprimljeni iz neregistrirane integracije odbijaju se.



### 7.3. Identifikacija Pouzdajuće strane

Prije obrade zahtjeva za autentikaciju Identityum provjerava je li Pouzdajuća strana registrirana i ovlaštena za upotrebu zatražene usluge.

Provjera se temelji na registriranim tehničkim vjerodajnicama Pouzdajuće strane, odobrenim sučeljima i krajnjim točkama, ugovornom statusu i kanonskom identitetu Pouzdajuće strane.

Kanonski identitet Pouzdajuće strane predstavlja stvarnu uslugu ili organizaciju za koju se provodi autentikacija. Njime se upravlja neovisno o promjenama domena, tehničkih klijenata, adresa preusmjerenja ili drugih pojedinosti implementacije.

Korisniku se prije potvrde transakcije prikazuje jasna i čitljiva identifikacija Pouzdajuće strane. Ako se strana koja podnosi zahtjev ne može pouzdano identificirati, transakcija se ne dovršava.

Ugovorna i tehnička registracija Pouzdajuće strane predstavlja kontrolu Identityuma za ovu uslugu. Ne smije se opisivati kao registracija Pouzdajuće strane EUDI Walleta ili certifikat pristupa Pouzdajuće strane EUDI Walleta, osim ako je taj zasebni uređeni okvir stvarno implementiran.

### 7.4. Određivanje potrebnog autentikacijskog režima

Potrebni režim određuje se prema radnji, primjenjivoj autentikacijskoj politici Walleta, zahtjevu Pouzdajuće strane, sigurnosnoj postavci Korisnika, politici povezane usluge i procijenjenom riziku. Ako se zahtjevi razlikuju, primjenjuje se najstroži primjenjivi minimum.

U rezultatu se navodi postignuti autentikacijski režim Walleta ili određena upotrijebljena vjerodajnica. Rezultatu se ne dodjeljuje eIDAS LoA samo zato što je bilo dostupno ili uspješno upotrijebljeno više faktora.

### 7.5. Odabir faktora i pojačana autentikacija

Ako se ne primjenjuje drugi odobreni režim, za autentikaciju ili dijeljenje PID-a potrebni su:

1. PIN ID Walleta; i
2. Identityum biometrija lica ili Identityum mobilni autentikator.

Za strožu transakciju mogu se zahtijevati sva tri faktora: PIN, biometrija lica i mobilni autentikator.

Za odobrenu transakciju nižeg rizika Pouzdajuća strana može dopustiti PIN zajedno s verificiranim brojem mobilnog telefona ili faktorom vanjskog računa. Takva lakša kombinacija ne može se upotrijebiti ako je Korisnik odabrao stroži režim ili ako primjenjiva usluga zahtijeva snažniju autentikaciju.

Svi faktori koji čine jedan autentikacijski događaj moraju se provesti tijekom iste povezane sesije, koja ne smije trajati dulje od 15 minuta.



Ako se mobilni autentikator upotrebljava za radnju visokog rizika ili radnju kvalificirane usluge povjerenja, Identityum može zahtijevati mrežni push način potvrđivanja umjesto izvanmrežne jednokratne lozinke.

Pojačana autentikacija može zahtijevati dodatni faktor ili snažniju dopuštenu kombinaciju. Ako Pouzdajuća strana zahtijeva i novije identifikacijske podatke ili viši LoIP PID-a, taj se zahtjev obrađuje zasebnom pojačanom provjerom identiteta ili PID-a, a ne samo dodavanjem autentikacijskog faktora.

## 7.6. Dinamička autentikacija

Ako to zahtijevaju rizik ili pravna priroda radnje, autentikacija se dinamički povezuje s određenom transakcijom.

U informacijama prikazanim Korisniku navodi se radnja koja se odobrava te, ovisno o primjenjivosti, Pouzdajuća strana, zatraženi podaci, referentna oznaka transakcije i relevantni dokument ili usluga.

Potvrdom Korisnik autorizira samo prikazanu transakciju. Ona se ne može tumačiti kao odobrenje druge transakcije, druge Pouzdajuće strane ili šireg otkrivanja podataka.

Mobilni autentikator može provoditi dinamičku autentikaciju mrežnim postupkom izazov–odgovor. Zahtjev se prikazuje na registriranom uređaju i odobrava kriptografskim odgovorom izrađenim na tom uređaju.

Statička ili izvanmrežna autentikacija jednokratnom lozinkom može se upotrebljavati samo kada je dopušta primjenjivi autentikacijski režim.

## 7.7. Vezivanje izazova, jednokratne vrijednosti, sesije i publike

Svakoј autentikacijskoј transakciji dodjeljuje se jedinstveni kontekst transakcije.

Ako se upotrebljava protokol utemeljen na izazovu, Identityum generira nov i nepredvidiv izazov koji vrijedi samo ograničeno vrijeme i za jedan pokušaj autentikacije.

Zahtjev za autentikaciju i odgovor na njega vezuju se uz relevantne:

- sesiju Korisnika;
- Pouzdajuću stranu ili publiku;
- identifikator transakcije;
- zatraženi autentikacijski režim;
- zatraženi opseg PID-a, kada je primjenjivo; i
- odobreno odredište odgovora.

Odgovor namijenjen jednoј Pouzdajućoj strani ne može prihvatiti druga Pouzdajuća strana. Jednako tako, rezultat autentikacije iz jedne transakcije ne može se prenijeti u drugu transakciju ili sesiju.



Autentikacijske poruke štite se tijekom prijenosa i provjeravaju u pogledu cjelovitosti, podrijetla, razdoblja valjanosti i konteksta transakcije.

Identyum sprječava ponovnu upotrebu isteklih ili prethodno prihvaćenih izazova, autentikacijskih odgovora i jednokratnih lozinki.

Mrežni način mobilnog autentikatora koristi zaštićeni postupak izazov–odgovor. Izazov se dostavlja registriranom autentikatoru, a odgovor se izrađuje s pomoću kriptografskog materijala vezanog uz uređaj. Identyum validira dobiveni odgovor prije odobravanja pristupa. Rezultati autentikacije vraćaju se samo na odobrene krajnje točke povezane s Pouzdajućom stranom koja ih je zatražila. Odbijaju se zahtjevi čiji se identifikatori transakcije, publika, odredište preusmjerenja ili drugi zaštićeni parametri ne podudaraju.

## 7.8. Provjere statusa Walleta i vjerodajnica

Prije dovršetka autentikacijske transakcije Walletom Identyum provjerava je li Wallet aktivan, jesu li potrebni faktori dostupni i valjani za tu radnju te je li zahtjev važeći i vezan uz registriranu Pouzdajuću stranu ili povezanu uslugu.

Ako transakcija uključuje certifikat ili udaljeni ključ, zasebno se provjeravaju status certifikata, dopuštenost profila i dostupnost ključa. Suspenzijom Walleta blokira se upotreba utemeljena na Walletu, ali se ne mijenja status certifikata. Opozvani ili istekli certifikat ne može se obnoviti ponovnom aktivacijom Walleta.

## 7.9. Potvrda Korisnika i autorizacija transakcije

Korisniku se prije potvrde prikazuju identitet Pouzdajuće strane i priroda zatražene radnje.

U zahtjevu za autentikaciju bez identifikacije jasno se navodi da se neće otkriti atributi PID-a.

Ako se zahtijeva dijeljenje podataka, Korisniku se prikazuju i:

- zatraženi atributi;
- navedena svrha;
- relevantne informacije o valjanosti ili pristupu; i
- sve dodatne informacije potrebne za donošenje informirane odluke.

Korisnik mora dati izričitu potvrdu. Odbijanjem ili napuštanjem zahtjeva transakcija se završava bez nastanka uspješnog rezultata autentikacije ili dijeljenja podataka.

Privola za jednu transakciju ne predstavlja trajno dopuštenje za nepovezane buduće transakcije.

Privola za obradu osobnih podataka upotrebljava se samo kada je privola primjenjiva pravna osnova. Sigurnosna potvrda, ugovorna uputa ili autorizacija transakcije ne smiju se označavati kao privola prema GDPR-u samo zato što Korisnik klikne kontrolu za odobravanje.



## 7.10. Rezultat autentikacije bez identifikacije

Ako nisu zatraženi atributi PID-a, Wallet može vratiti rezultat autentikacije bez identifikacije. U rezultatu se navodi namjeravana Pouzdajuća strana, sadržava se pseudonimni identifikator specifičan za Pouzdajuću stranu te bilježe autentikacijski kontekst i ishod transakcije.

Pouzdanja strana ne smije taj rezultat upotrebljavati kao dokaz da je Identityum verificirao ili otkrio građanski identitet Korisnika. Ako je potreban građanski identitet, Pouzdajuća strana mora zasebnim postupkom opisanim u Poglavlju 8. zatražiti i primiti potrebne attribute PID-a.

## 7.11. Pseudonimni identifikatori specifični za Pouzdajuću stranu

Pri autentikaciji Walletom upotrebljava se pseudonimni identifikator specifičan za Pouzdajuću stranu koji je sadržan u autentikacijskoj tvrdnji ili jednakovrijednom rezultatu autentikacije.

Identifikator je stabilan za istog Korisnika i istu kanonsku Pouzdajuću stranu, ali se razlikuje među Pouzdajućim stranama. Ne otkriva interni identifikator Walleta, nacionalni identifikator ni drugu zajedničku vrijednost namijenjenu povezivanju podataka među klijentima.

Ne izdaje se zaseban anonimni certifikat. Identityum kontrolirani odnos između Korisnika, Walleta i identifikatora specifičnih za Pouzdajuću stranu čuva isključivo radi upravljanja životnim ciklusom, odgovora na incidente i zakonski opravdanih dokaznih svrha.

Podaci o građanskom identitetu otkrivaju se Pouzdajućoj strani samo zasebnom transakcijom dijeljenja PID-a koju je autorizirao Korisnik.

Identifikator se može izdati za prazan Wallet. U tom slučaju identificira isti odnos Walleta u kontekstu kanonske Pouzdajuće strane, a ne verificirani građanski identitet Korisnika.

## 7.12. Autentikacijska tvrdnja i dokazi

Nakon uspješne autentikacije Identityum putem odobrenog sučelja vraća rezultat zaštićen u pogledu cjelovitosti. Ovisno o slučaju upotrebe, u rezultatu se navode Identityum, namjeravana publika, identifikator specifičan za Pouzdajuću stranu, autentikacijski kontekst, referentna oznaka transakcije, vrijeme izdavanja, razdoblje valjanosti i ishod.

Rezultat ne sadržava attribute PID-a, osim ako je njihovo otkrivanje bilo dio zasebno prikazanog i autoriziranog zahtjeva. Identityum bilježi dovoljno dokaza za rekonstrukciju zahtjeva, Pouzdajuće strane, provedenih kategorija faktora, radnje Korisnika, rezultata i opsega svih dostavljenih podataka.

## 7.13. Neuspjela autentikacija i otkrivanje zlouporabe

Autentikacija nije uspješna ako potrebni faktor nije uspješno proveden, ako je transakcija istekla, Wallet ili vjerodajnica nisu valjani ili se odgovor ne može vezati uz Pouzdajuću stranu koja ga je zatražila i predmetnu transakciju.



Korisniku se može dopustiti ponavljanje autentikacije unutar kontroliranih ograničenja broja pokušaja. Ako je prethodna transakcija ili prethodni izazov istekao ili se više ne može sigurno upotrijebiti, potrebna je nova transakcija ili novi izazov.

Identyum može zahtijevati pojačanu autentikaciju ako je:

- zatražena radnja osjetljivija od trenutačne sesije;
- Pouzdajuća strana zatražila snažniji režim;
- to potrebno prema sigurnosnim postavkama Korisnika;
- zasebno primjenjiva vjerodajnica ne ispunjava navedeni zahtjev razine pouzdanosti; ili
- transakcija povezana s povišenim rizikom.

Lakši autentikacijski režim ne upotrebljava se kao zamjena ako je bio potreban snažniji režim, ali se nije mogao provesti.

Identyum prati autentikacijske aktivnosti radi otkrivanja znakova zlouporabe, prijevare ili neovlaštene kontrole Walleta.

Relevantni događaji mogu uključivati ponovljene neuspjele pokušaje, neuobičajene obrasce autentikacije, nevaljane ili ponovljene odgovore transakcije, zlouporabu vjerodajnica, nedosljedne informacije o sesiji ili aktivnost povezanu s prijavljenim gubitkom ili kompromitacijom.

Ovisno o procijenjenom riziku Identyum može:

- odbiti transakciju;
- zahtijevati snažniju autentikaciju;
- privremeno blokirati autentikacijski faktor;
- suspendirati Wallet ili blokirati zahvaćeni faktor odnosno upotrebu upravljanog ključa;
- obavijestiti Korisnika;
- pokrenuti istragu incidenta; ili
- zahtijevati ponovnu provjeru identiteta.

Detaljna pravila i pragovi otkrivanja povjerljivi su i ne objavljuju se u ovom Pravilniku.

Nemogućnost provedbe potrebnog snažnijeg režima ne rješava se prešutnim povratkom na slabiji režim. Transakcija se odbija ili ponovno pokreće u okviru izričito dopuštenog alternativnog tijeka.

## 7.14. Obveze Pouzdajuće strane

Pouzdanu stranu koja upotrebljava ID Wallet mora:

- održavati ažurnima svoje registracijske podatke, tehničke vjerodajnice i odobrene krajnje točke;
- točno se identificirati Identyumu i Korisniku;
- zahtijevati samo razinu autentikacije i podatke potrebne za navedenu svrhu;



- štiti rezultate autentikacije i podatke PID-a od neovlaštenog pristupa ili ponovne upotrebe;
- validirati cjelovitost, izdavatelja, publiku, razdoblje valjanosti i vezivanje uz transakciju svakog rezultata;
- provjeriti ispunjavaju li postignuti autentikacijski režim Walleta, svaka izričito primjenjiva razina pouzdanosti vjerodajnice, LoIP i svježina PID-a vlastite zahtjeve;
- poštovati primjenjive ugovorne obveze te obveze privatnosti i zaštite osobnih podataka; i
- prijaviti Identityumu sumnju na kompromitaciju ili zlouporabu odnosno značajne incidente povezane s integracijom.

Rezultat autentikacije bez identifikacije ne smije se smatrati dokazom da su Pouzdajućoj strani otkriveni ili za nju verificirani podaci o građanskom identitetu.

Pouzdajuće strane ne smiju pokušavati izvesti interni identifikator Walleta Identityuma, povezivati pseudonime specifične za različite Pouzdajuće strane niti ponovno upotrebljavati identifikator specifičan za Pouzdajuću stranu izvan konteksta Pouzdajuće strane za koji je generiran.

Pouzdajuća strana ostaje odgovorna za odluku o odobravanju pristupa, sklapanju transakcije ili pouzdanju u predstavljene podatke PID-a.





## 8. Podaci u Walletu i predstavljanje Identityum PID-a

### 8.1. Kategorije podataka Walleta

| Kategorija                                         | Primjeri i status                                                                                                                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Podaci računa Walleta                              | Interni identifikator Walleta, verificirani broj mobilnog telefona ili adresa e-pošte kao identifikator računa, status i konfiguracija.                                                         |
| Autentikacijski podaci                             | Veze faktora, zaštićeni biometrijski prikaz, registracija autentikatora i sigurnosni događaji.                                                                                                  |
| Identityum PID                                     | Kopija ili sigurna referenca na PID koji je izdao Identify, zajedno s provjerenim atributima i metapodacima podrijetla, LoIP-a i vremena, ako je Korisnik odabrao dostupnost PID-a kroz Wallet. |
| Drugi verificirani podaci                          | Podaci validirani putem odobrenog izvora ili pružatelja i označeni njihovim podrijetlom i statusom.                                                                                             |
| Podaci koje je dao Korisnik ili prilagođeni podaci | Podaci koji se ne prikazuju kao verificirani, osim ako je proveden definirani postupak validacije.                                                                                              |
| Informacije o aktivnostima                         | Korisniku vidljivi zapisi o podržanim događajima autentikacije, otkrivanja i životnog ciklusa.                                                                                                  |

### 8.2. PID pohranjen ili povezan s Walletom

Identityum PID izdaje Identify kao strukturirani identitetski rezultat. Wallet, prema odabiru Korisnika, čuva zaštićenu kopiju PID-a ili sigurnu referencu koja omogućuje njegov dohvat i predstavljanje; pritom ne postaje izdavatelj PID-a niti preuzima odluku o njegovu LoIP-u.

PID ne mora biti fizička datoteka na uređaju Korisnika ni trajno pohranjena kopija u Walletu. Sučelje može prikazivati podatke iz zaštićene kopije ili ih dohvatiti preko sigurne reference, uz očuvanje izdavatelja, cjelovitosti, statusa i metapodataka rezultata Identifyja.

### 8.3. Validirani i nevalidirani podaci

Podaci pohranjeni u Walletu razvrstavaju se prema tome jesu li njihov izvor i sadržaj verificirani.

Podaci označeni kao validirani nose tvrdnju i metapodatke izvora koji je proveo mjerodavni postupak validacije. Wallet čuva i prikazuje oznaku izvora, status verifikacije i, kada je riječ o PID-u, LoIP koji je dodijelio Identify; samom pohranom podaci ne postaju validirani.

**Nevalidirani podaci** mogu se pohranjivati za određene slučajeve upotrebe, ali moraju se jasno razlikovati od verificiranih podataka. Ne čine dio Identityum PID-a i ne smiju podupirati eID vjerodajnicu, izdavanje certifikata ili drugu reguliranu funkciju, osim ako se naknadno verificiraju.



Kada se podaci predstavljaju Pouzdajućoj strani, u rezultatu se navodi jesu li podaci verificirani, samodeklarirani ili na drugi način nepoduprti tvrdnjom Identityuma o pouzdanosti.

Uz privolu Korisnika Poslovni klijent može upisati vlastite poslovne podatke u Wallet Korisnika. Takvi podaci mogu uključivati informacije koje proizlaze iz odnosa tog Klijenta i Korisnika. Podaci su kriptirani pod kontrolom Klijenta, a Identityum ih ne može pročitati bez pristupa koji omogućuje Klijent.

Klijent je odgovoran za zakonitost, točnost, značenje i životni ciklus prilagođenih poslovnih podataka. Ako nije drukčije zasebno navedeno, Identityum ne verificira te podatke i u vezi s njima ne iznosi tvrdnju o LoIP-u ili autentičnosti.

Klijent može dopustiti drugoj pravnoj osobi čitanje podataka tako da joj omogućuje potreban kriptografski pristup, ali za njihovu upotrebu ili otkrivanje putem Walleta i dalje je potrebna privola Korisnika.

Sučeljem i pri otkrivanju čuva se razlika između verificiranih atributa PID-a, drugih validiranih podataka i podataka dostavljenih bez verifikacije Identityuma. Podaci ne postaju verificirani samom pohranom u Walletu.

## 8.4. Izvori, podrijetlo, LoIP i svježina

Identityum bilježi podrijetlo verificiranih podataka Walleta.

Podrijetlom se može utvrditi:

- identifikacijska isprava, registar, eID, certifikat, banka ili drugi izvor iz kojeg podaci potječu;
- metoda prikupljanja podataka;
- je li izvor bio primaran ili je upotrijebljen za dodatnu validaciju;
- vrijeme dohvaćanja ili predstavljanja; i
- relevantni status verifikacije.

Ako je atribut pribavljen iz više izvora, u PID-u se mogu zabilježiti relevantni izvori i rezultat unakrsne validacije.

Podrijetlo ostaje povezano s atributom kada se on pohranjuje, osvježava ili dijeli, u opsegu potrebnom da Korisnik i Pouzdajuća strana procijene pouzdanost podataka.

Svaki PID koji je dostupan kroz Wallet nosi LoIP koji mu je dodijelio Identify prema mjerodavnoj dokumentaciji Identifyja ili TSPS-u.

Wallet čuva samo one podatke o podrijetlu i statusu koji su dio izdanog PID-a ili su potrebni za njegovu dopuštenu uporabu. Potpuni dokazni rezultati iz kojih je izveden LoIP ostaju u dokaznom sustavu Identifyja ili QTSP-a, izvan aktivnog sadržaja Walleta.



Detaljni bodovi, pragovi, identity-proofing mehanizmi i pokazatelji prijave nisu dio sadržaja Walleta. Održavaju se u mjerodavnim kontroliranim dokaznim zapisima Identifyja ili usluge povjerenja i dostupni su samo ovlaštenim stranama za dopuštenu svrhu.

Kada Wallet predstavlja PID, prenosi LoIP i samo one metapodatke o izvoru, statusu i svježini koje je izdao ili potvrdio Identify i koji su potrebni za konkretnu autoriziranu svrhu.

PID i njegovi atributi sadržavaju vremenske oznake koje pokazuju kada su podaci pribavljeni ili verificirani.

Nastavak upotrebljivosti atributa može ovisiti o:

- valjanosti njegova izvornog izvora;
- isteku, suspenziji ili opozivu identifikacijske isprave ili vjerodajnice;
- vremenu proteklom od verifikacije;
- promjeni koju je priopćio autoritativni izvor; i
- zahtjevu Pouzdajuće strane u pogledu svježine.

Podaci mogu ostati vidljivi u Walletu nakon što prestanu ispunjavati određeni zahtjev svježine. U tom se slučaju bez dodatne validacije ili osvježnog PID-a ne mogu predstavljati kao aktualni za taj slučaj upotrebe.

Osvježavanjem PID-a nastaju ažurirani podaci o podrijetlu, vremenske oznake, rezultati verifikacije i LoIP. Raniji dokazi mogu se i dalje zasebno čuvati radi revizije i pravnih svrha. LoIP pripada rezultatu provjere identiteta i ne smije se objediniti s postignutim autentifikacijskim režimom Walleta u jednu nepoduprtu tvrdnju o pouzdanosti.

## 8.5. Zaštićena pohrana

PID i drugi zaštićeni podaci Walleta čuvaju se u pozadinskom sustavu Identityuma unutar sigurnosnog konteksta specifičnog za Korisnika te se putem podržanog sučelja stavljaju na raspolaganje tek nakon autentifikacije potrebne za tu radnju.

Zaštićeni sadržaj Walleta kriptiran je pri pohrani i prijenosu te se na uređaju Korisnika ne čuva kao obična čitljiva lokalna kopija. Ako su čitljivi podaci privremeno potrebni radi prikaza, validacije ili dijeljenja, obrada se provodi samo u kontroliranom okruženju, a privremeni se materijal uklanja u skladu s primjenjivim sigurnosnim postupkom.

Administrativni pristup i pristup podrške ograničeni su ulogom, svrhom, odobrenjem i zapisivanjem. Aktivnošću podrške ne nastaje neograničena sekundarna kopija sadržaja Walleta. Svaka iznimna kopija dokaza potrebna za incident, pravni zahtjev ili regulatornu svrhu obrađuje se kao zasebno zadržani dokaz, a ne kao aktivni sadržaj Walleta.

Zasebno zadržani dokazi o provjeri identiteta i uslugama povjerenja nisu obični aktivni sadržaj Walleta i podliježu kontrolama pristupa i čuvanja opisanim u odjeljcima 8.13. i 10.8.



## 8.6. Pristup Korisnika i upravljanje podacima

Korisnik nakon uspješne autentikacije može pristupiti podacima pohranjenima u svojem ID Walletu i pregledati ih.

Wallet prikazuje podatke u razumljivom obliku te, kada je relevantno, i njihov status verifikacije, izvor, LoIP, datum prikupljanja, valjanost ili svježina.

Pristup Korisnika ne uključuje nužno povjerljive sigurnosne informacije kao što su interni pokazatelji prijave, detaljni tehnički bodovi, kriptografske tajne ili revizijski zapisi sustava.

Ako je podatke u Wallet pohranila treća strana, mogućnost Korisnika da ih tumači, mijenja ili izvozi može ovisiti i o primjenjivom formatu, enkripciji i pravima te treće strane.

Podatke u Wallet mogu dodati:

- Korisnik;
- Identityum nakon odobrenog postupka prikupljanja ili verifikacije; ili
- treća strana koja djeluje uz privolu Korisnika.

Zahtjev za dodavanje ili ažuriranje PID-a u Walletu zahtijeva autentikaciju Walletom, ali samo prikupljanje, validacija i izdavanje ažuriranog PID-a provode se u Identifyju.

Verificirani identifikacijski podaci mogu se ažurirati samo putem odobrenog izvora ili postupka verifikacije. U osvježenom rezultatu bilježe se njegovo podrijetlo, vrijeme verifikacije i LoIP, umjesto prešutne promjene dokazne povijesti prethodnog rezultata.

Samodeklarirani podaci ili podaci koji nisu identifikacijski mogu se uređivati podržanom funkcijom Walleta, ali njihov status ostaje nevalidiran, osim ako ih Identityum naknadno verificira.

## 8.7. Odabir i smanjenje količine podataka

Pouzdajuća strana može zatražiti samo attribute potrebne za navedenu svrhu.

Identityum Korisniku prikazuje opseg zatraženih podataka i ne otkriva nikakav dodatni sadržaj Walleta samo zato što se Korisnik autentificirao.

Ako integracija dopušta neobvezne attribute, Korisnik ih može isključiti iz otkrivanja. Atributi označeni kao obvezni za zatraženu uslugu ne mogu se izostaviti ako Korisnik želi dovršiti tu transakciju.

Ako Pouzdajuća strana treba samo stabilni identifikator računa, autentikacija se može dovršiti pseudonimom specifičnim za Pouzdajuću stranu bez otkrivanja imena Korisnika, nacionalnog identifikatora ili drugih podataka o građanskom identitetu.

Zahtjevi za autentikaciju bez identifikacije ne smiju pokrenuti otkrivanje PID-a. Ako Pouzdajuća strana treba samo pseudonim na razini računa, ne uključuju se građansko ime, nacionalni identifikator niti drugi atribut PID-a.



## 8.8. Predstavljanje PID-a i dijeljenje atributa

PID se predstavlja u zaštićenoj transakciji koju pokreće ovlaštena Pouzdajuća strana, a potvrđuje Korisnik.

PID se ne mora otkriti kao jedan potpuni skup podataka. Identityum može dostaviti samo odabrane attribute zajedno s metapodacima potrebnima za njihovo tumačenje i validaciju.

Ovisno o zahtjevu, otkriveni rezultat može uključivati:

- verificirane identifikacijske attribute;
- njihov izvor ili podrijetlo;
- primjenjivi LoIP;
- vrijeme pribavljanja ili verifikacije podataka;
- informacije o valjanosti ili svježine; i
- status PID-a ili relevantnog atributa.

Podaci se prenose iz pozadinskog sustava Identityuma ovlaštenoj Pouzdajućoj strani putem odobrenog sučelja. Autorizacija je ograničena na određenog primatelja, transakciju, opseg podataka i, kada je primjenjivo, razdoblje pristupa.

Podaci Walleta dijele se samo u transakciji koju je autorizirao Korisnik.

Korisniku se prije potvrde prikazuju Pouzdajuća strana, zatraženi podaci i navedena svrha. Otkrivanje je ograničeno na odabranog primatelja, attribute i transakciju.

Dijeljeni rezultat može uključivati zatražene podatke zajedno s informacijama o izvoru, LoIP-u, svježine i valjanosti potrebnima za njihovo tumačenje.

Podaci pripremljeni za Pouzdajuću stranu štite se za tog primatelja i stavljaju na raspolaganje putem vremenski ograničenog mehanizma pristupa. Ako nije dogovoreno i objavljeno drugo razdoblje, zadano razdoblje dostupnosti iznosi pet dana. Nakon isteka ili preuzimanja privremene se dostavne kopije brišu u skladu s primjenjivom politikom pohrane.

Podaci autentikacijskih faktora ne dijele se s Pouzdajućom stranom.

## 8.9. Vezivanje uz primatelja, svrhu i transakciju

Korisniku se prije otkrivanja prikazuju čitljivi identitet Pouzdajuće strane, zatraženi atributi, navedena svrha i kontekst transakcije. Autorizacija je ograničena na tog primatelja, opseg i transakciju ili dopušteno razdoblje pristupa.

Prethodno odobrenje autentikacije ili otkrivanja ne može se smatrati dopuštenjem za novog primatelja, novu svrhu, drugi opseg podataka ili nepovezanu transakciju. Zahtjevi koji se ne mogu pouzdano vezati uz registriranu Pouzdajuću stranu odbijaju se.



## 8.10. Provjera statusa i svježine PID-a

Prije predstavljanja podataka PID-a Identityum utvrđuje jesu li zatraženi atributi dostupni i ispunjavaju li primjenjive zahtjeve statusa i valjanosti.

Rezultat Pouzdajućoj strani pruža dovoljno informacija da procijeni:

- odakle podaci potječu;
- kako i kada su verificirani;
- primjenjivi LoIP PID-a;
- jesu li izvor ili dokazi na kojima se podaci temelje i dalje valjani; i
- ispunjavaju li podaci zatraženi zahtjev svježine.

Pouzdajuća strana ostaje odgovorna za utvrđivanje jesu li PID i LoIP dostatni za njezinu pravnu ili poslovnu svrhu.

Ako je raspoloživi PID prestar, nepotpun ili ispod zatraženog LoIP-a, Wallet ne mijenja njegov status ni LoIP nego zaustavlja predstavljanje ili upućuje Korisnika u Identify radi novog ili osvježnog rezultata.

Ako PID ne ispunjava zatražene zahtjeve, transakcija se može nastaviti samo nakon odobrenog postupka ponovne validacije, osvježavanja ili pojačane provjere. Pouzdajuća strana ostaje odgovorna za odluku je li dobiveni PID dostatan za njezinu pravnu ili poslovnu svrhu.

## 8.11. Ažuriranje, uklanjanje i ponovna upotreba

Korisnik može iz Walleta zatražiti pokretanje postupka za ažuriranje PID-a, ali novi izvor, provjere, odluku, LoIP i vrijeme utvrđuje Identify. Wallet nakon uspješnog ishoda zamjenjuje ili povezuje novu kopiju/referencu, uz očuvanje odvojenih dokaznih zapisa.

Korisnik može ukloniti pojedinačne attribute PID-a ili cijeli PID iz aktivnog sadržaja Walleta nakon autentikacije potrebne za tu radnju. Uklanjanjem se prekida buduće predstavljanje uklonjenih podataka putem Walleta, ali se ne povlače podaci koji su već zakonito dostavljeni Pouzdajućoj strani niti brišu dokazi koje Identityum mora zasebno čuvati.

Uklanjanjem PID-a iz sadržaja Walleta ne mijenja se status postojećeg certifikata ANSign, NAuth ili QNSign niti se samim time blokira odgovarajući privatni ključ. Uklanjanje može onemogućiti buduće dijeljenje PID-a ili zahtijevati nove dokaze za izdavanje, obnovu, promjenu ključa ili drugu reguliranu radnju.

Postojeći PID može se ponovno upotrijebiti u naknadnom postupku Identify, uvođenja korisnika ili drugoj podržanoj transakciji samo ako sadržava potrebne attribute i ispunjava primjenjive zahtjeve LoIP-a, valjanosti i svježine. Svaka ponovna upotreba zahtijeva novi zahtjev i autorizaciju Korisnika; ranijim dijeljenjem ne nastaje neograničen ili trajan pristup.



Ako postojeći PID nije dostatan, Identify može prikupiti dodatne attribute, ponovno validirati podatke ili provesti novi postupak. Wallet ovlaštenu Pouzdajuću stranu obavještava samo u okviru valjanog zahtjeva i bez automatskog otkrivanja promijenjene vrijednosti.

Korisnik može primati obavijesti Walleta o značajnim ažuriranjima, uklanjanjima, događajima životnog ciklusa ili sigurnosno osjetljivim promjenama. Trajno zatvaranje Walleta i konačno postupanje s podacima Walleta uređeni su Poglavljem 6.

## 8.12. Povijest aktivnosti, izvoz i prenosivost

Wallet Korisniku pruža pregled značajnih aktivnosti povezanih s njegovim podacima, ako to podržava relevantno sučelje.

Pregled može uključivati:

- dodavanje, ažuriranje ili brisanje podataka Walleta;
- zahtjeve za dijeljenje podataka i njihove ishode;
- uključenu Pouzdajuću stranu;
- događaje autentikacije i vjerodajnica;
- promjene autentikacijskih faktora; i
- suspenziju, ponovnu aktivaciju ili opoziv Walleta.

Identyum zasebno vodi revizijske zapise dostatne za rekonstrukciju značajnih radnji Walleta. Takvi zapisi mogu sadržavati vremenske oznake, referentne oznake transakcija, identifikatore Walleta ili identifikatore specifične za Pouzdajuću stranu, uključene kategorije podataka i ishod događaja.

Revizijski zapisi ne omogućuju redovan pristup potpunom sadržaju Walleta i mogu se čuvati dulje od odgovarajućih aktivnih podataka ako je to potrebno u pravne, sigurnosne ili dokazne svrhe.

Kada je podržano, Korisnik može izvesti odabrane podatke iz ID Walleta u uobičajenom strojno čitljivom ili čovjeku čitljivom formatu.

Izvoz može uključivati odabrane podatke Walleta i relevantne metapodatke, kao što su njihov izvor, status verifikacije, LoIP i datum prikupljanja.

Izvoz ne uključuje:

- interna sigurnosna pravila ili pokazatelje prijevare Identityuma;
- kriptografske privatne ključeve zaštićene u centralnim ili udaljenim okruženjima;
- povjerljive ključeve za enkripciju druge strane;
- interne sustavske i revizijske zapise; ili
- podatke čijim bi se izvozom povrijedila prava trećih strana ili primjenjivo pravo.



Izvezena podatkovna datoteka sama po sebi nije aktivni Identityum PID, eID vjerodajnica ni rezultat autentikacije. Njezin naknadni prihvata i dokazna vrijednost ovise o formatu, zaštiti cjelovitosti i zahtjevima strane koja je prima.

Funkcionalnost izvoza ili povijesti aktivnosti ne uključuje privatne ključeve, autentikacijske tajne, zaštićene biometrijske predloške, sigurnosno osjetljive interne dokaze niti zapise čije je otkrivanje ograničeno zakonom ili sigurnosnim zahtjevima.

### 8.13. Odvajanje od zadržanih regulatornih dokaza

Aktivnim podacima Walleta upravlja se radi funkcija koje Korisnik koristi te oni podliježu pravilima brisanja Walleta i privatnosti. Dokazi Identifikacija, pretplatnika, certifikata, potpisa i sigurnosti koji se čuvaju u pravne ili regulatorne svrhe drže se zasebno uz kontrolirani pristup. Brisanjem ili uklanjanjem aktivnog sadržaja Walleta ne brišu se dokazi za koje vrijedi dulje primjenjivo razdoblje čuvanja. Čuvanjem tih dokaza PID ne postaje ponovno aktivni sadržaj Walleta niti se dopušta njegovo daljnje predstavljanje Pouzdajućoj strani.





## 9. Sučelja Walleta s uslugom Identify i povezanim uslugama povjerenja

### 9.1. Odnos s uslugom Identityum Identify

Identityum Identify i Wallet zasebne su usluge koje međusobno djeluju. Identify provodi provjeru identiteta i izrađuje rezultat transakcije te, ako je primjenjiva odluka uspješna, Identityum PID. Wallet pruža neobvezno okruženje za naknadnu pohranu, upravljanje, autentikaciju i autorizirano predstavljanje.

Korisnik može dovršiti Identify bez izrade Walleta, može imati prazan Wallet bez dovršetka postupka Identify te može dovršiti Identify bez pohrane dobivenog PID-a u Wallet. U dokumentaciji i sučelju čuvaju se sve te dopuštene mogućnosti.

### 9.2. Neobvezna ponuda Walleta nakon postupka Identify

Poslovni klijent može konfigurirati hoće li se Korisniku koji je uspješno dovršio njegov integrirani tijek Identify ponuditi izrada Identityum Walleta. Ponuda se daje samo ako to dopuštaju relevantni ugovor s Poslovnim klijentom i tijek Identityuma.

Potreban je izričit odabir Korisnika. Poslovni klijent ne može u ime Identityuma učiniti odnos Walleta obveznim niti izraditi Wallet bez neposrednog prihvata primjenjivih Uvjeta korištenja Walleta od strane Korisnika.

### 9.3. Neovisni odabiri PID-a i povezane usluge povjerenja

Nakon odgovarajućeg rezultata Identifyja Korisnik neovisno odabire hoće li PID pohraniti ili povezati s Walletom i hoće li zasebno zatražiti određenu uslugu povjerenja. Odbijanje jedne mogućnosti samo po sebi ne onemogućuje drugu, ako su ispunjeni kriteriji mjerodavnog CP-a i TSPS-a.

Wallet prije radnje prikazuje točnu uslugu i profil na koji se zahtjev odnosi te upućuje na mjerodavne uvjete. Generička oznaka ne smije sugerirati da je svaki profil kvalificiran, da je kvalificirani status već stečen ili da su certifikat i PID automatski uključeni u Wallet.

### 9.4. Granica usluga povjerenja

Wallet se može upotrebljavati za zahtijevanje, pristup ili autorizaciju povezane Identityum usluge povjerenja. Wallet sam po sebi nije certifikacijsko tijelo, udaljeni QSCD ni usluga izrade potpisa, a pohrana običnog sadržaja Walleta ne uključuje upotrebljiv privatni ključ certifikata. Izdavanje certifikata, registracija Pretplatnika, prihvrat certifikata, status certifikata, zaštita ključa, izrada potpisa i dokazi uređeni su primjenjivom Politikom certifikata, TSPS-om, Izjavom o objavi podataka, Uvjetima korištenja i kontroliranim postupcima.



## 9.5. Mjerodavni dokumenti za povezane usluge povjerenja

| Pitanje                                        | Mjerodavni dokument                                        | Uloga Walleta                                                                                                       |
|------------------------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Podržani profil i kriteriji prihvatljivosti    | CP te odgovarajući TSPS/CPS                                | Wallet prikazuje dostupnu zasebnu uslugu; ne određuje profil ni prihvatljivost.                                     |
| Zahtjev i pretplatnički ugovor                 | TSPS, Uvjeti korištenja i Izjava o objavi podataka         | Wallet može prikazati informacije i zabilježiti izričitu radnju Korisnika.                                          |
| Izdavanje, status i životni ciklus certifikata | CP i TSPS/CPS                                              | Odvojeni su od pohrane PID-a i životnog ciklusa Walleta, osim izričito definiranih učinaka.                         |
| Udaljeno potpisivanje i uporaba ključa         | TSPS i dokumentacija SSAS-a, uključujući ETSI TS 119 431-1 | Wallet je korisničko sučelje za autentikaciju i potvrdu transakcije; sam ne dokazuje sole control ni status QSCD-a. |

Ovaj Pravilnik ne propisuje mapiranje LoIP-a na certifikacijske profile ni sadržaj paketa. Takva pravila, uključujući dopuštene kombinacije profila i sve kvalificirane tvrdnje, utvrđuju se CP-om i TSPS-om te postaju operativno primjenjiva tek nakon ispunjenja potrebnih vanjskih uvjeta.

## 9.6. Wallet-side zahtjev i prihvrat uvjeta povezane usluge

Kada se zahtjev za povezanu uslugu povjerenja pokreće iz Walleta, Wallet prije radnje Korisniku prikazuje točnu uslugu/profil i omogućuje pristup primjenjivim uvjetima i informacijama na trajnom mediju. Korisnik zatim zasebnom namjernom radnjom podnosi zahtjev ili prihvaća ugovor prema postupku uređenom TSPS-om.

Wallet evidentira prikazane informacije, verzije upućenih dokumenata, radnju Korisnika, vrijeme i referencu transakcije te taj dokaz predaje mjerodavnom sustavu usluge povjerenja. Pravna valjanost zahtjeva i sadržaj pretplatničkog odnosa određuju se izvan ovog Pravilnika.

## 9.7. Prikaz rezultata i statusa povezane usluge u Walletu

Ako mjerodavni postupak usluge povjerenja zahtijeva prikaz izdanog certifikata, prihvrat, aktivaciju ili drugu radnju prije uporabe, Wallet može pružiti to korisničko sučelje. Svaka takva radnja ostaje zasebna od ranijeg zahtjeva i ugovora te se provodi prema CP-u i TSPS-u.

Wallet evidentira korisnički prikaz i radnju te razmjenjuje status s mjerodavnim sustavom usluge povjerenja. Izdavanje, aktivacija, odbijanje, status i daljnje postupanje s certifikatom određuju se isključivo prema CP-u i TSPS-u.

## 9.8. Prihvatljivost certifikata bez PID-a pohranjenog u Walletu

Dugoročni ANSign, NAuth i QNSign zahtijevaju aktivan Wallet te odgovarajući rezultat provjere identiteta i dokazni paket povezan sa subjektom i zahtjevom za certifikat. PID ne mora ostati pohranjen kao aktivni sadržaj Walleta.



Prazan Wallet sam po sebi ne utvrđuje identitet za certifikat. Unatoč tome, može ostati valjano okruženje za autentikaciju i autorizaciju certifikata čija je osnova identiteta zasebno utvrđena, povezana i zadržana prema primjenjivim pravilima usluga povjerenja.

## 9.9. Autentikacija Walletom za upotrebu udaljenog ključa

Za upotrebu privatnog ključa krajnjeg korisnika kojim upravlja Identityum potrebne su autentikacija Walletom i autorizacija transakcije propisane za predmetni profil i radnju. Uspješnom autentikacijom Walletom autorizira se samo određena kriptografska radnja i Korisniku se ne daje izravan pristup privatnom ključu.

Kada je AUTH-E dio postupka autorizacije udaljenog potpisivanja, koristi se kroz transakcijski vezan mrežni tijek izazov–odgovor koji korisniku prikazuje podatke potrebne za svjesnu potvrdu. Ispunjenje zahtjeva za SAD, sole control i kvalificirani elektronički potpis dokazuje se cjelinom SSAS/QSCD postupka prema TSPS-u i ETSI TS 119 431-1, a ne samim postojanjem AUTH-E ili Walleta.

## 9.10. Učinak događaja Walleta na certifikate i ključeve

| Događaj Walleta ili PID-a                        | Učinak na ANSign, NAuth i QNSign                                                                                                                                                                |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wallet je aktivan                                | Certifikat se može upotrebljavati ako su certifikat, ključ, potrebni faktori i povezana usluga zasebno valjani.                                                                                 |
| Wallet je suspendiran                            | Upotreba ključa utemeljena na Walletu blokirana je; status certifikata ostaje nepromijenjen samo zbog suspenzije Walleta.                                                                       |
| Wallet je ponovno aktiviran                      | Upotreba se može nastaviti samo ako su certifikat i druge ovisnosti i dalje valjani.                                                                                                            |
| PID je zastario ili nedostatan                   | Status postojećeg certifikata ostaje nepromijenjen; za novo izdavanje, obnovu ili određenu transakciju mogu biti potrebni osvježeni dokazi o identitetu.                                        |
| PID je uklonjen iz Walleta                       | Status postojećeg certifikata i prihvatljivost ključa ostaju nepromijenjeni samo zbog uklanjanja.                                                                                               |
| Wallet je trajno opozvan, izbrisan ili zatvoren  | Prema kanonskom pravilu zatvaranja i mjerodavnom CP-u/TSPS-u opozivaju se dugoročni certifikati ANSign, NAuth i QNSign vezani uz Wallet; izvršenje i dokaz opoziva pripadaju usluzi povjerenja. |
| Pojedinačni certifikat je istekao ili je opozvan | Prestaje samo funkcija zahvaćenog certifikata; Wallet može ostati aktivan.                                                                                                                      |

Identityum ne podržava privremenu suspenziju certifikata. Ako je tijekom istrage potrebno neposredno ublažavanje rizika, Identityum može blokirati upotrebu upravljanog privatnog ključa



i pritom ostaviti status certifikata nepromijenjenim dok se razlog opoziva ne potvrdi u dovoljnoj mjeri.

### 9.11. Usluge izvan opsega Pravilnika Walleta

Cjelovite aktivnosti CA-a i RA-a, upravljanje udaljenim QSCD-om, izrada i validacija potpisa, djelovanje QLSeal-a, kvalificirano vremensko žigosanje, usluge statusa certifikata i prestanak usluge povjerenja uređeni su izvan ovog Pravilnika.

Dostupnost povezane funkcije putem sučelja Walleta ne čini tu funkciju dijelom usluge Walleta niti čini Identityum pružateljem usluge treće strane. Za svaku se integraciju navode primjenjivi pružatelj usluge i mjerodavna dokumentacija.



## 10. Upravljanje sigurnošću i operativnim poslovima

### 10.1. Organizacija i odgovornosti

Identityum upravlja uslugom ID Walleta putem definiranih upravljačkih, operativnih, sigurnosnih, tehničkih, pravnih i potpornih funkcija. Direktor zadržava ukupnu odgovornost za upravljanje uslugom, raspodjelu resursa, odobravanje politika i prihvatanje značajnih preostalih rizika.

Glavne odgovornosti raspoređene su kako slijedi:

| Funkcija                                         | Glavne odgovornosti                                                                                                       |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Uprava</b>                                    | Upravljanje uslugom, odobravanje politika, resursi i prihvatanje značajnih rizika                                         |
| <b>Rizici i usklađenost</b>                      | Upravljanje rizicima, regulatorno praćenje, nadzor usklađenosti i izvještavanje uprave                                    |
| <b>Informacijska sigurnost</b>                   | Upravljanje sigurnošću, praćenje, nadzor pristupa i upravljanje incidentima                                               |
| <b>Tehnologija i infrastruktura</b>              | Razvoj, rad infrastrukture, uvođenje u rad, dostupnost i oporavak                                                         |
| <b>Upravljanje sučeljem s uslugom Identify</b>   | Integracijska pravila, prijenos zahtjeva i rezultata te razdvajanje ovlasti; identity-proofing odluke ostaju u Identifyju |
| <b>Zaštita osobnih podataka i pravni poslovi</b> | Upravljanje privatnošću, pravna dokumentacija i obveze obavještanja                                                       |
| <b>Korisnička podrška</b>                        | Upiti Korisnika, upravljanje zahtjevima podrške i eskalacija                                                              |
| <b>Vlasnici procesa i imovine</b>                | Kontrola nad dodijeljenim procesima, sustavima, informacijama i drugom imovinom                                           |

Korisnička podrška organizirana je u tri razine. Podrška prve razine zaprima, bilježi i početno analizira upite. Složenija procesna ili tehnička pitanja eskaliraju se podršci druge razine, dok pitanja koja zahtijevaju intervenciju u softveru ili detaljnu analizu sustava rješavaju ovlašteni tehnički stručnjaci. Komunikacija s Korisnicima i promjene statusa zahtjeva čuvaju se u sustavu podrške.

Detaljna raspodjela uloga, zamjenici i interne linije izvještavanja održavaju se u kontroliranoj organizacijskoj dokumentaciji Identityuma.

Odgovornost za uslugu Walleta ostaje na Identityumu i kada dobavljač obavlja potpunu aktivnost. Odgovornosti povezanih usluga povjerenja uređene su odgovarajućim TSPS-om i ulogama usluge.



## 10.2. Upravljanje rizicima i informacijskom sigurnošću

Usluga ID Walleta uključena je u okvir upravljanja poslovnim rizicima i rizicima informacijskih sustava Identityuma na razini cijele organizacije.

Rizici se utvrđuju i procjenjuju najmanje jednom godišnje te dodatno nakon značajnih promjena, uključujući uvođenje novih usluga ili tehnologija, značajne arhitekturne promjene, značajne incidente ili promjene koje utječu na kritične procese.

Pri procjeni se razmatraju relevantna imovina, prijetnje, ranjivosti, postojeće kontrole, vjerojatnost i mogući učinak. Rizici se klasificiraju kao niski, srednji ili visoki te bilježe u povjerljivom Registru poslovnih rizika.

Ovisno o procjeni Identityum može:

- prihvatiti rizik;
- smanjiti ga dodatnim kontrolama; ili
- prenijeti dio rizika putem dobavljača, ugovora ili osiguranja.

Ako se odabere ublažavanje, u Registru rizika navode se kontrola, odgovorna osoba, rok provedbe i očekivani preostali rizik. Preostali rizik ponovno se procjenjuje nakon provedbe i prihvaća ga ovlaštena upravljačka funkcija.

Rezultati rizika preispituju se u godišnjim i, kada je potrebno, ad hoc izvještajima. Sam okvir upravljanja rizicima podliježe periodičnom internom preispitivanju.

ID Wallet radi unutar okvira upravljanja informacijskom sigurnošću i privatnošću Identityuma.

Okvirom se uspostavljaju kontrole namijenjene očuvanju:

- povjerljivosti identifikacijskih, biometrijskih i autentikacijskih podataka;
- cjelovitosti i autentičnosti PID-a, vjerodajnica i dokaza transakcija;
- dostupnosti Walleta i potpornih usluga; i
- odgovornosti za sigurnosno osjetljive radnje.

Zahtjevi sigurnosti i privatnosti primjenjuju se tijekom projektiranja, razvoja, testiranja i produkcijskog rada usluge, pružanja podrške, postupanja s incidentima i prestanka usluge.

Identityum održava odobrene politike i postupke koji obuhvaćaju kontrolu pristupa, upravljanje imovinom, promjenama i incidentima, čuvanje podataka, fizičku sigurnost, upravljanje dobavljačima i kontinuitet poslovanja. Detaljne tehničke konfiguracije i pravila otkrivanja ostaju povjerljivi.

Pri procjeni rizika razlikuju se funkcije Walleta za autentikaciju bez identifikacije, funkcije identifikacijskih podataka i ovisnosti o uslugama povjerenja. Kontrole i kriteriji prihvata razmjerni su stvarnoj funkciji i ne pretpostavljaju višu klasifikaciju pouzdanosti od one koja je formalno utvrđena.



### 10.3. Uloge, kompetencije i razdvajanje dužnosti

Sigurnosno osjetljive odgovornosti razdvajaju se kako bi se smanjila mogućnost da jedna osoba samostalno uvede, odobri i prikrije neovlaštenu radnju.

Osobito:

- razvojni inženjeri podnose izmjene softvera na pregled;
- uvođenje u produkciju ograničeno je na ovlašteno osoblje;
- promjene infrastrukture zahtijevaju odobrenje odgovorne tehničke funkcije;
- odluke u postupku Identify donosi isključivo osoblje kojem je ta uloga dodijeljena prema mjerodavnoj dokumentaciji Identifyja; uloge Walleta ne nadjačavaju takvu odluku;
- osoblje korisničke podrške nema neograničen pristup produkcijskim sustavima; i
- privilegirani pristup sam po sebi ne ovlašćuje na promjene zapisa o identitetu, vjerodajnicama ili Walletu.

Ako strogo organizacijsko razdvajanje nije praktično, Identityum primjenjuje kompenzacijske kontrole kao što su neovisno odobrenje, stručni pregled druge osobe, zabilježeno uvođenje u rad, višestruka kontrola ili naknadna verifikacija.

Dodjele pristupa i uloga preispituju se pri promjeni odgovornosti te se bez odgađanja uklanjaju kada više nisu potrebne.

Osoblje se raspoređuje u uloge povezane s ID Walletom prema svojim kompetencijama, odgovornostima i potrebi za pristupom.

Prije odobravanja pristupa osoblje se upoznaje s obvezama povjerljivosti, informacijske sigurnosti i zaštite osobnih podataka. Provjere prošlosti ili prikladnosti provode se kada je to zakonito i razmjerno ulozi.

Osoblje prolazi osposobljavanje primjereno svojim odgovornostima. Ono, ovisno o primjenjivosti, uključuje:

- sigurnu upotrebu informacijskih sustava i upravljanje njima;
- postupanje s osobnim i biometrijskim podacima;
- prepoznavanje i prijavljivanje incidenata;
- sigurne prakse izmjena softvera i infrastrukture;
- eskalaciju korisničke podrške; i
- razgraničenje ovlasti i sigurno postupanje na sučelju Walleta s uslugom Identify.

Osposobljavanje se ponavlja kada se uvedu značajne promjene ili kada incident, revizija ili procjena rizika pokažu potrebu za dodatnim kompetencijama.

### 10.4. Upravljanje dobavljačima

Identityum se može oslanjati na vanjske pružatelje infrastrukture, hostinga, komunikacija, sigurnosnih komponenti, izvora identiteta ili drugih potpornih usluga.



U postupku upravljanja dobavljačima razmatraju se važnost isporučene funkcije, osjetljivost uključenih podataka, operativne ovisnosti i učinak koji bi neispunjenje obveza dobavljača moglo imati na uslugu ID Walleta.

Relevantni ugovori s dobavljačima uređuju pitanja kao što su povjerljivost, zaštita osobnih podataka, ograničenja pristupa, sigurnosni incidenti, dostupnost usluge, podugovaranje, kontinuitet, revizijski dokazi i prestanak.

Pristup dobavljača sustavima ili opremi pod kontrolom Identityuma mora biti autoriziran, ograničen na potrebnu svrhu i zabilježen. Kritični dobavljači uključuju se u primjenjive postupke upravljanja rizicima, incidentima, promjenama i kontinuitetom.

Upotreba vanjskog dobavljača ne uklanja odgovornost Identityuma za funkcije za koje je izjavljeno da su u opsegu usluge ID Walleta.

Uloga dobavljača, pristup podacima, ovisnost usluge, sigurnosne obveze, dužnosti u slučaju incidenta, mjere kontinuiteta i dokazi dokumentiraju se i preispituju. Izdvajanje poslova ne prenosi odgovornost Identityuma za njegove obveze u vezi s Walletom.

## 10.5. Kontrole pristupa, kriptografije i sigurnosti podataka

Identityum bilježi relevantnu materijalnu i nematerijalnu imovinu te informacijsku imovinu i ljudske resurse u Registru imovine. Svakoj zabilježenoj imovini dodjeljuje se vlasnik odgovoran za njezino utvrđivanje, klasifikaciju, upotrebu, zaštitu i upravljanje životnim ciklusom.

Imovina se klasificira prema važnosti za povjerljivost, cjelovitost, dostupnost i zaštitu osobnih podataka. Imovina koja podupire regulirane funkcije ili funkcije usluga povjerenja dodatno se utvrđuje unutar opsega relevantne usluge.

Fizički pristup kritičnoj poslužiteljskoj, mrežnoj i kriptografskoj opremi ograničen je na ovlaštene osobe. Bilježe se identitet, vrijeme i svrha pristupa. Ako je oprema smještena kod vanjskog pružatelja podatkovnog centra, pristup opremi u vlasništvu Identityuma i dalje podliježe odobrenju i nadzoru Identityuma. Fizički prostori s kritičnom opremom prate se odgovarajućim sigurnosnim kontrolama, uključujući bilježenje pristupa i videonadzor.

Tehničke kontrole uključuju kontrolirani administrativni pristup, kriptiranu komunikaciju, segmentaciju mreže, vatrozide, sigurnosno praćenje i odvajanje kritičnih kriptografskih komponenti od općih aplikacijskih usluga.

Javni opis tih kontrola namjerno je ograničen. Detaljne sigurnosne zone, mrežne adrese, konfiguracije praćenja, metode pristupa i dijagrami sustava održavaju se u povjerljivoj dokumentaciji. Postojeća arhitektura razdvaja produkcijske usluge u zaštićene zone i osigurava zalihosne komponente usluge radi dostupnosti i oporavka.

Pristup aktivnom sadržaju Walleta, autentikacijskim podacima, biometrijskim prikazima i zasebno zadržanim dokazima o identitetu ili uslugama povjerenja ograničen je ulogom i





svrhom. Administrativni pristup i osjetljive radnje bilježe se te podliježu primjenjivim kontrolama razdvajanja i pregleda.

## 10.6. Upravljanje promjenama i konfiguracijama

Izmjene softvera i infrastrukture uređene su zasebnim kontroliranim postupcima.

Identityum održava neovisna razvojna, testna i produkcijska okruženja. Promjena se ne uvodi izravno u produkciju bez prethodnog testiranja i odobrenja, osim ako je hitni postupak potreban radi neposrednog sigurnosnog rizika ili rizika dostupnosti.

Izmjene softvera slijede kontrolirani put koji uključuje upravljanje izvornim kodom, pregled drugih članova tima, uvođenje u razvojno okruženje, funkcionalno testiranje, testiranje u testnom okruženju i ovlašteno uvođenje u produkciju. Verzije za izgradnju i uvođenje mogu se identificirati, a prethodne verzije koje se mogu uvesti čuvaju se kada je to potrebno radi povrata na prethodno stanje.

Promjene infrastrukture procjenjuju se u pogledu opsega, rizika, očekivanog učinka, mogućeg prekida rada i povrata na prethodno stanje. Redovne i hitne promjene zahtijevaju autorizaciju primjerenu njihovoj hitnosti i riziku. Produkcijske promjene najprije se testiraju u testnom okruženju, a po mogućnosti i u razvojnom okruženju kada je primjenjivo.

Prije produkcijske promjene zahvaćeni vlasnici procesa i, kada je potrebno, Poslovni klijenti obavještavaju se o očekivanom prekidu rada, privremenim ograničenjima usluge ili potrebnim radnjama integracije.

Nakon uvođenja Identityum provjerava radi li zahvaćena usluga pravilno. Neuspjele promjene poništavaju se ili ispravljaju s pomoću pripremljenog mehanizma povrata na prethodno stanje. Promjena Walleta koja mijenja sučelje prema Identifyju, uvodi autentikacijski faktor, mijenja podatkovni model ili predstavljanje PID-a, uvodi novu povezanu uslugu ili vanjsku tvrdnju o statusu, mijenja tijek autorizacije potpisivanja ili značajno utječe na privatnost zahtijeva dokumentiranu procjenu učinka i koordinirano ažuriranje zahvaćene dokumentacije.

## 10.7. Zapisivanje, dokazi i vođenje evidencije

Identityum vodi zapise dostatne za dokazivanje i rekonstrukciju sigurnosno relevantnih i operativno značajnih događaja ID Walleta.

Zapisi, ovisno o primjenjivosti, uključuju:

| Područje                       | Primjeri                                                                                                                                                        |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Izrada Walleta i veza s PID-om | Identifikator računa, uspostava faktora, referenca Identify transakcije, primitak rezultata i odabir pohrane/povezivanja; bez identity-proofing dokaza i odluke |
| Životni ciklus Walleta         | Izrada, aktivacija, suspenzija, ponovna aktivacija, opoziv i zatvaranje                                                                                         |



| Područje                           | Primjeri                                                                         |
|------------------------------------|----------------------------------------------------------------------------------|
| <b>Autentikacijski faktori</b>     | Dodavanje, zamjena i uklanjanje faktora i uređaja                                |
| <b>Autentikacija i dijeljenje</b>  | Pouzdajuća strana, transakcija, vjerodajnica, odluka Korisnika i otkriveni opseg |
| <b>Životni ciklus vjerodajnice</b> | Izdavanje, promjene statusa, istek i opoziv                                      |
| <b>Administracija</b>              | Privilegirani pristup te događaji konfiguracije i uvođenja u rad                 |
| <b>Podrška i incidenti</b>         | Prijave Korisnika, komunikacija, eskalacija, istraga i rješavanje                |

U zapisima se navode relevantno vrijeme, radnja, objekt, inicijator ili automatizirani proces i rezultat. Kada je potrebno, navode se i politika, verzija softvera ili konfiguracija koja se u tom trenutku primjenjivala.

Revizijski i dokazni zapisi zaštićeni su od neovlaštenog pristupa, izmjene i brisanja. Pristup je ograničen na osoblje s opravdanom operativnom, sigurnosnom, pravnom ili revizijskom potrebom.

Model dokaza Walleta razlikuje izradu računa, uspostavu faktora, pokretanje Identifyja, primitak rezultata, odabir pohrane/povezivanja PID-a, autentikaciju, predstavljanje PID-a, autorizaciju povezane usluge i događaje životnog ciklusa. Dokazi o provjeri identiteta, pretplatniku, certifikatu, potpisu i statusu certifikata vode se zasebno u mjerodavnim sustavima i dokumentaciji.

## 10.8. Čuvanje i sigurno uklanjanje

Razdoblje čuvanja određuje se prema kategoriji zapisa, pravnoj svrsi i mjerodavnoj usluzi. Na obični sadržaj Walleta i opće zapise Walleta ne primjenjuje se automatski razdoblje čuvanja primjenjivo na dokaze QTSP-a.

| Kategorija zapisa                                                       | Radni model čuvanja                                                                                              |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Dokazi QTSP-a o identitetu, Pretplatniku, certifikatu i potpisu         | Deset godina prema primjenjivom TSPS-u i kontroliranom rasporedu čuvanja.                                        |
| Opći operativni i sigurnosni zapisi koji nisu uključeni u dokaze QTSP-a | Tri godine, osim ako se primjenjuje drugi pravni zahtjev, zahtjev povezan s incidentom ili dokazni zahtjev.      |
| Aktivni sadržaj Walleta                                                 | Tijekom razdoblja potrebnog za funkciju Walleta i u skladu s Pravilima privatnosti Walleta i pravilima brisanja. |



| Kategorija zapisa                                                | Radni model čuvanja                                                                                                    |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Zapisi o sigurnosnom incidentu ili pod pravnom zabranom brisanja | Tijekom primjenjivog razdoblja povezanog s incidentom, zastarom, regulatornim zahtjevom ili pravnom zabranom brisanja. |

Nakon isteka primjenjivog razdoblja zapisi se sigurno brišu, anonimiziraju ili čine trajno nedostupnima, osim ako se zbog zakonite zabrane brisanja ili druge dokumentirane osnove zahtijeva nastavak čuvanja.

## 10.9. Praćenje i upravljanje incidentima

Identityum prati relevantne događaje u aplikaciji, infrastrukturi, mreži, autentikaciji i privilegiranom pristupu radi otkrivanja kvarova, neovlaštenih aktivnosti, pokazatelja prijevare i sigurnosnih incidenata.

Praćenje uključuje pregled zapisa i automatizirano otkrivanje putem sigurnosnih kontrola uvedenih u relevantnim zonama sustava.

Događaji se procjenjuju prema mogućem učinku na povjerljivost, cjelovitost, dostupnost, autentičnost, Korisnike, Poslovne klijente i regulirane usluge.

Praćenjem se podupire i upravljanje ranjivostima. Utvrđene ranjivosti procjenjuju se prema ozbiljnosti i zahvaćenim sustavima te se otklanjaju, ublažavaju ili formalno upravljaju ovisno o riziku.

Detaljna pravila otkrivanja, pragovi upozorenja i arhitektura praćenja povjerljivi su.

Svaki zaposlenik ili drugi ovlašteni korisnik informacijskog sustava mora prijaviti sumnju na incident. Korisnici i Poslovni klijenti mogu prijaviti sumnju na problem putem uspostavljenih kanala korisničke podrške, iz kojih se potencijalno ozbiljna pitanja eskaliraju odgovornoj sigurnosnoj ili tehničkoj funkciji.

Incidenti se klasificiraju kao niski, srednji ili visoki prema njihovu operativnom i sigurnosnom učinku. Incidenti koji utječu na kritične funkcije identiteta, autentikacije Walletom, statusa vjerodajnica, kriptografije ili dokaza mogu se klasificirati kao visoki čak i ako je šira platforma dostupna.

Životni ciklus upravljanja incidentom obuhvaća:

1. pripremu;
2. identifikaciju i klasifikaciju;
3. ograničavanje;
4. iskorjenjivanje;
5. oporavak; i
6. izvještavanje i naučene lekcije.



Ograničavanje ima prednost ako bi nastavak rada mogao povećati štetu. Oporavak uključuje verifikaciju i testiranje prije povratka zahvaćene komponente u produkciju.

Ako incident utječe na osobne podatke, cjelovitost usluge ili regulirane funkcije, Identyum procjenjuje potrebu za obavještanjem zahvaćenih Korisnika, Poslovnih klijenata i nadležnih tijela unutar primjenjivih zakonskih ili ugovornih rokova.

Svaki značajni incident dokumentira se. U pregledu nakon incidenta utvrđuju se uzrok, učinkovitost odgovora i sve korektivne ili preventivne kontrole potrebne za smanjenje rizika ponavljanja.

Radnje u slučaju incidenta razlikuju suspenziju Walleta, blokiranje faktora, blokiranje upotrebe ključa i opoziv certifikata. Suspenzija certifikata ne upotrebljava se kao status odgovora na incident.

### 10.10. Kontinuitet poslovanja i oporavak od katastrofe

Identyum održava mjere kontinuiteta i oporavka za usluge i komponente čija bi nedostupnost mogla značajno utjecati na funkcije ID Walleta.

Mjere kontinuiteta uključuju zaštićene sigurnosne kopije, zalihosnu infrastrukturu ili infrastrukturu koja se može oporaviti, postupke obnove, alternativne načine komunikacije i definirane odgovornosti za oporavak.

Kritične aplikacijske i sigurnosne komponente rade uz primarne i sekundarne mogućnosti usluge. Relevantni podaci i komponente usluge sinkroniziraju se ili repliciraju radi potpore nastavku rada ili oporavku nakon kvara primarnog okruženja.

Nakon incidenta ili katastrofe sustavi se obnavljaju iz odobrenih izvora ili sigurnosnih kopija, primjenjuju se potrebna ažuriranja i sigurnosni ispravci, a dobivena se konfiguracija testira prije nastavka produkcijske upotrebe.

Obnovom se ne vraća Wallet ili vjerodajnica koja je prije prekida valjano opozvana, istekla ili ukinuta.

Prioriteti oporavka uzimaju u obzir cjelovitost i status autentikacije Walletom, transakcija Pouzdajućih strana, zaštićenog sadržaja Walleta i ovisnosti o povezanim uslugama povjerenja. Oporavljena komponenta vraća se u rad tek nakon verifikacije njezine sigurnosti i dosljednosti podataka.

### 10.11. Prestanak usluge

Identyum održava mjere za uredan prestanak ID Walleta ili povezane eID funkcije.

Postupkom prestanka obuhvaćaju se:

- prestanak izdavanja novih Walleta ili vjerodajnica;
- obavještanje Korisnika, Poslovnih klijenata i nadležnih tijela;



- postupanje s aktivnim Walletima, funkcijama Walleta te povezanim vjerodajnicama i sesijama;
- očuvanje zakonom propisanih dokaza;
- izvoz, povrat ili brisanje podržanih podataka Korisnika;
- prestanak pristupa dobavljača i administratora; i
- nastavak dostupnosti informacija potrebnih za tumačenje ranijih transakcija.

U slučaju planiranog prestanka Korisnici se, kada je to razumno moguće, obavještavaju dovoljno unaprijed i dobivaju upute o raspoloživim mogućnostima izvoza ili zamjene podataka. Prestanak povezanih certifikata, usluga povjerenja ili funkcija udaljenog potpisivanja dodatno je uređen primjenjivom Politikom certifikata i Pravilnikom o postupcima pružanja usluga povjerenja.

Planiranje prestanka uključuje posljedice za aktivne Wallete, obavještavanje Korisnika, pristup podacima prihvatljivima za izvoz ili njihov izvoz, brisanje aktivnog sadržaja, zaštitu i čuvanje dokaza te opoziv vezanih dugoročnih certifikata ANSign, NAuth i QNSign kada se Walleti trajno zatvore.

## 10.12. Revizija i ocjenjivanje sukladnosti

Identityum preispituje rad ID Walleta putem upravljačkog nadzora, izvještavanja o rizicima, internih kontrola i revizija.

Aktivnosti upravljanja rizicima provode se najmanje jednom godišnje, uz dodatne procjene nakon značajnih promjena. Cjelokupni okvir upravljanja poslovnim rizicima neovisno se preispituje u planiranim razmacima.

Revizijama se, među ostalim, mogu ispitati:

- usklađenost s ovim Pravilnikom;
- provedba kontrola sigurnosti i privatnosti;
- pristup i razdvajanje dužnosti;
- upravljanje imovinom i dobavljačima;
- promjene softvera i infrastrukture;
- postupci upravljanja incidentima i kontinuitetom; i
- potpunost i zaštita dokaza.

Nalazi se dodjeljuju odgovornim osobama i prate dok se korektivna radnja ne dovrši i verificira. Neovisna ocjenjivanja sukladnosti ili certifikacijske revizije provode se kada to zahtijevaju pravni okvir, primjenjiva norma ili posebna tvrdnja o pouzdanosti koju iznosi Identityum.

Identityum objavljuje tvrdnju o LoA-i, certifikaciji ili regulatornoj sukladnosti samo za opseg i produkcijsku konfiguraciju koji su formalno ocijenjeni i odobreni.



Revizijom prema opsegu usluge povjerenja Wallet se ne certificira automatski kao sredstvo elektroničke identifikacije ili europski novčanik za digitalni identitet. Za svaku takvu tvrdnju potrebni su zasebno primjenjivi ocjenjivanje i odobrenje.



## 11. Informacije za Korisnike, privatnost i pravna pitanja

### 11.1. Objavljena definicija usluge

Identityum objavljuje dovoljno informacija kako bi budući Korisnik mogao razumjeti glavna svojstva ID Walleta prije stupanja u odnos pružanja usluge.

Objavljene informacije, ovisno o primjenjivosti, uključuju:

- identitet i kontaktne podatke Identityuma;
- glavne funkcije ID Walleta;
- uvjete za izradu i upotrebu Walleta;
- obvezne autentikacijske faktore;
- odnos između Walleta, PID-a, eID vjerodajnica i povezanih usluga povjerenja;
- primjenjive naknade;
- glavne sigurnosne mjere opreza;
- postupak suspenzije, opoziva i prestanka;
- informacije o privatnosti i pravima Korisnika; i
- dostupne kanale podrške i pritužbi.

Informacije se pružaju putem ovog Pravilnika, Uvjeta korištenja, Pravila privatnosti, sučelja usluge i drugih primjenjivih dokumenata za objavu podataka.

Informacije namijenjene Korisnicima napisane su u obliku koji bi trebao biti razumljiv bez potrebe za pristupom povjerljivoj tehničkoj ili sigurnosnoj dokumentaciji Identityuma.

Ako se povezana usluga pruža prema zasebnim uvjetima, Korisnik se o tome obavještava prije zahtijevanja ili upotrebe te usluge.

Objavljena definicija normativno opisuje kanonske TO-BE funkcije Walleta, jasno razlikuje autentikaciju bez identifikacije od predstavljanja PID-a te zasebno označuje svaki status koji ovisi o vanjskoj ocjeni sukladnosti, kvalifikaciji, prijavi ili regulatornom odobrenju.

### 11.2. Uvjeti korištenja

Ugovorni odnos za ID Wallet uređen je primjenjivim Uvjetima korištenja zajedno s Pravilima privatnosti i svim dodatnim uvjetima prihvaćenima za neobvezne ili povezane usluge.

Korisniku se mora omogućiti da pročita i zadrži primjenjive dokumente prije njihova prihvata.

Prihvat se provodi elektronički i bilježi zajedno s verzijama dokumenata i vremenom prihvata.

Osnovni ugovor za Wallet stupa na snagu tek kada je Korisnik:

1. prihvatio Uvjete korištenja i Pravila privatnosti;
2. uspješno uspostavio obvezne autentikacijske faktore Walleta; i
3. dovršio izdavanje Walleta.

Prihvat dokumenta bez dovršetka izdavanja Walleta sam po sebi ne stvara aktivni ID Wallet.



Svaka povezana eID funkcija ili usluga povjerenja podliježe vlastitim uvjetima, profilu i, kada je primjenjivo, pretplatničkom ugovoru i pravilima udaljenog potpisivanja. Prihvat i zahtjev bilježe se odvojeno od ugovora za osnovni Wallet.

Ako Uvjeti korištenja, Pravila privatnosti ili drugi dokument specifičan za uslugu određeno pitanje uređuju detaljnije od ovog Pravilnika, primjenjuje se hijerarhija dokumenata opisana u odjeljku 1.6.

Uvjeti korištenja Walleta odvojeni su od pretplatničkih ugovora za usluge povjerenja. Kada se Wallet upotrebljava za zahtijevanje paketa certifikata, informacije o uslugama povjerenja, pretplatnički ugovor i kasniji prihvat certifikata obrađuju se kao zasebne faze opisane u Poglavlju 9.

### 11.3. Sigurnosne preporuke

Identityum Korisnicima pruža informacije potrebne za sigurnu upotrebu ID Walleta.

Korisnik se obavještava da su autentikacijski faktori osobni i da se ne smiju prenijeti ili staviti na raspolaganje drugoj osobi. Posebnu pozornost potrebno je posvetiti zaštiti PIN-a Walleta, registriranih uređaja, komunikacijskih računa i mobilnih autentikatora.

Korisnicima se daju upute da:

- uređaje i podržani softver održavaju razumno sigurnima i ažurnima;
- spriječe neovlašteni pristup aktivnim sesijama Walleta;
- provjere identitet Pouzdajuće strane koja podnosi zahtjev;
- prije potvrde pregledaju zatražene podatke i pojedinosti transakcije;
- bez nepotrebnog odgađanja suspendiraju ili opozovu Wallet nakon sumnje na gubitak ili kompromitaciju; i
- Identityumu prijave sumnju na zlouporabu ili sigurnosne incidente.

Identityum može izdati dodatna upozorenja ili upute ako određena prijetnja, promjena usluge ili incident stvara povećan rizik.

U sigurnosnim informacijama objavljenima Korisnicima ne otkrivaju se povjerljiva logika praćenja, pragovi prijave, mrežne konfiguracije ili druge pojedinosti koje bi mogle oslabiti uslugu.

### 11.4. Obavijest o privatnosti i uloge u zaštiti osobnih podataka

Pravilima privatnosti objašnjava se kako Identityum prikuplja i obrađuje osobne podatke povezane s ID Walletom.

U njima se, ovisno o primjenjivosti, navode:

- kategorije osobnih podataka koji se obrađuju;
- svrhe i pravne osnove obrade;
- obrada autentikacijskih i biometrijskih podataka;





- primatelji i kategorije primatelja;
- međunarodni prijenosi podataka;
- načela čuvanja;
- sigurnosne mjere;
- prava Korisnika; i
- dostupni kontakt za privatnost i kanali za pritužbe.

Informacije o privatnosti pružaju se prije nego što Korisnik izradi Wallet i ostaju javno dostupne tijekom cijelog odnosa pružanja usluge.

Ako se novom funkcijom uvode značajno drukčija svrha obrade, kategorija podataka, primatelj ili pravna osnova, Korisnik prima relevantne informacije prije omogućavanja te funkcije.

Pravila privatnosti dio su ugovorne dokumentacije, ali ostaju mjerodavan dokument za detaljan opis obrade osobnih podataka.

Identityum djeluje kao voditelj obrade za obradu potrebnu za pružanje usluge ID Walleta i upravljanje njome, uključujući upis u Wallet, upravljanje autentikacijskim faktorima, sigurnost, podršku i radnje životnog ciklusa Walleta.

Njegova se uloga može razlikovati za povezanu uslugu.

| Kontekst obrade                                                  | Uobičajena uloga                                                                                       |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Pružanje usluge ID Walleta i upravljanje njome                   | Identityum kao voditelj obrade                                                                         |
| Vlastite eID funkcije ili funkcije usluga povjerenja Identityuma | Identityum kao voditelj obrade, u skladu s primjenjivom dokumentacijom usluge                          |
| Postupak Identify konfiguriran za Poslovnog klijenta             | Uloge raspoređene prema određenoj svrsi obrade i ugovoru s Klijentom                                   |
| Dostava podataka Pouzdajućoj strani koju je autorizirao Korisnik | Pouzdanja strana nakon primitka u pravilu postaje odgovorna za njihovu daljnju obradu                  |
| Vanjski dobavljač koji pruža podršku Identityumu                 | Dobavljač djeluje prema primjenjivom odnosu voditelja i izvršitelja obrade ili drugom ugovornom odnosu |

Poslovni klijent ne postaje pružatelj Walleta ili voditelj obrade za Wallet samo zato što je izrada Walleta ponuđena u njegovu integriranom postupku.

Iste podatke mogu obrađivati različite strane za zasebne svrhe i u zasebnim pravnim ulogama. Te se uloge određuju prema stvarnoj aktivnosti obrade, a ne prema tehničkoj činjenici da se strane koriste istom Identityum platformom.



Pravila privatnosti razlikuju ulogu Identityuma kao voditelja obrade za Wallet od njegove uloge koja može biti drukčija u kontekstu Poslovnog klijenta, Identifyja ili povezane usluge povjerenja.

Pravila privatnosti razlikuju biometrijski upis AUTH-D za prazan Wallet od biometrijske provjere identiteta, aktivni sadržaj Walleta od zasebno zadržanih dokaza te vlastite aktivnosti Identityuma kao voditelja obrade od obrade koja se provodi za Poslovnog klijenta.

### 11.5. Kontrola, autorizacija i prava Korisnika

Korisnik uvijek izravno odlučuje hoće li uspostaviti odnos za ID Wallet i prihvatiti njegove uvjete. Poslovni klijent može odrediti uvjete vlastite usluge ili ponuditi Wallet u svojem tijeku, ali ne može izraditi Wallet, prihvatiti uvjete niti upravljati sadržajem Walleta u ime Korisnika. Svako dijeljenje podataka putem Walleta zahtijeva zasebnu dopuštenu radnju Korisnika.

U svakoj transakciji dijeljenja podataka navode se Pouzdajuća strana i zatraženi podaci. Odobrenje Korisnika ograničeno je na tog primatelja, opseg i transakciju te ne predstavlja opći pristup Walletu.

Zasebna privola ili druga primjenjiva autorizacija ili prihvrat Korisnika pribavlja se kada je potrebna za:

- obradu biometrijskih podataka;
- povezanu eID funkciju ili uslugu povjerenja za koju je prema mjerodavnom dokumentu potrebna zasebna autorizacija ili prihvrat;
- otkrivanje podataka Walleta Pouzdajućoj strani;
- marketing ili drugu neobveznu komunikaciju; i
- drugu aktivnost obrade za koju je privola ili druga primjenjiva autorizacija Korisnika primjenjiva pravna osnova.

Ako se obrada temelji na privoli ili drugoj primjenjivoj autorizaciji Korisnika, Korisnik je može povući u skladu s Pravilima privatnosti. Povlačenje ne utječe na zakonitost obrade provedene prije povlačenja.

Funkcija koja tehnički ili pravno ovisi o povučenoj privoli ili drugoj primjenjivoj autorizaciji Korisnika može postati nedostupna. Wallet osobito ne može ostati aktivan bez obveznog faktora biometrije lica koji zahtijeva ovaj Pravilnik.

Privola se ne upotrebljava kao zamjena za drugu pravnu osnovu ako je obrada potrebna radi izvršenja ugovora za Wallet, ispunjavanja pravne obveze, zaštite usluge ili održavanja obveznih dokaza.

Podložno uvjetima i ograničenjima primjenjivog prava, Korisnik može ostvariti prava povezana s osobnim podacima koje obrađuje Identityum, uključujući pravo na:

- informacije i pristup osobnim podacima;



- ispravak netočnih ili nepotpunih podataka;
- brisanje kada nastavak obrade nije opravdan;
- ograničenje obrade;
- prigovor na obradu utemeljenu na legitimnim interesima ili izravnom marketingu;
- povlačenje privole ili druge primjenjive autorizacije Korisnika;
- primanje primjenjivih podataka u prenosivom formatu; i
- podnošenje pritužbe nadležnom nadzornom tijelu.

Zahtjev koji se odnosi na podatke pohranjene kao aktivni sadržaj Walleta može zahtijevati i autentikaciju Korisnika putem Walleta, osobito ako bi otkrivanje, izmjena ili brisanje mogli utjecati na identitet, sigurnost ili povezane vjerodajnice.

Verificirani atributi PID-a ne pretvaraju se u samodeklarirane podatke samo zato što Korisnik zahtijeva ispravak. Ispravak mora biti potkrijepljen odobrenim izvorom ili postupkom verifikacije.

Prava na brisanje ne obvezuju Identityum na brisanje dokaza koji se moraju čuvati prema pravnoj obvezi, politici certifikata, pravilu usluge povjerenja, zahtjevu obrane pravnih zahtjeva ili drugoj zakonitoj osnovi čuvanja.

Zahtjevi se obrađuju putem kontakata za privatnost i podršku koje objavljuje Identityum. Pravila privatnosti detaljnije opisuju pristup, ispravak, brisanje i povezana prava.

Ostvarivanje prava na zaštitu osobnih podataka ne zahtijeva brisanje zapisa koji se moraju čuvati prema primjenjivoj pravnoj obvezi ili su potrebni za postavljanje, ostvarivanje ili obranu pravnih zahtjeva. Svako se ograničenje objašnjava u skladu s primjenjivim Pravilima privatnosti i pravom.

## 11.6. Naknade

Izrada, pohrana i redovna upotreba ID Walleta pružaju se Korisniku bez posebne naknade za izdavanje Walleta ili pretplate prema važećem javno objavljenom modelu usluge.

Povezana usluga povjerenja, transakcija, usluga Poslovnog klijenta ili druga neobvezna funkcija može podlijeagati zasebnoj naknadi prema svojim primjenjivim uvjetima. Naknada koju plaća Korisnik jasno se objavljuje prije nego što Korisnik zatraži naplatnu uslugu i ne izvodi se samo iz dostupnosti Walleta.

Naknade koje plaća Poslovni klijent, Pouzdajuća strana ili druga pravna osoba uređene su relevantnim komercijalnim ugovorom i ne mijenjaju informacije o naknadama za Wallet namijenjene Korisniku.

## 11.7. Odgovornosti Korisnika

Korisnik daje točne informacije i ne smije svjesno upotrebljavati lažne, izmijenjene ili nezakonito pribavljene dokaze o identitetu.



Korisnik je odgovoran za:

1. osobnu upotrebu Walleta isključivo u zakonite svrhe;
2. zaštitu autentikacijskih faktora i registriranih uređaja;
3. pregled zahtjeva prije potvrde autentikacije ili otkrivanja;
4. održavanje kontaktnih podataka i faktora pod kontrolom Korisnika kada je to potrebno;
5. ispravljanje ili osvježavanje zastarjelih podataka podržanim postupkom;
6. prijavljivanje sumnje na neovlaštenu upotrebu bez nepotrebnog odgađanja; i
7. poštovanje sigurnosnih uputa i postupaka životnog ciklusa.

Korisnik ne smije zaobilaziti kontrole usluge, ometati sustave Identyuma, automatizirati neovlašteni pristup, unositi zlonamjerni kôd, obrnuto inženjerirati zaštićene komponente niti se služiti Walletom radi lažnog predstavljanja kao druga osoba.

Neispunjavanje obveza može dovesti do odbijanja transakcije, suspenzije ili opoziva Walleta, ukidanja vjerodajnice ili raskida ugovora.

Uvjeti korištenja zahtijevaju osobnu upotrebu, točne informacije, zaštitu autentikacijskih faktora i prijavljivanje sumnje na kompromitaciju bez nepotrebnog odgađanja.

Korisnik ne smije rezultat autentikacije praznim Walletom predstavljati kao verificirani građanski identitet niti prenijeti kontrolu Walleta, autentikacijske faktore ili odobrenja transakcija drugoj osobi.

## 11.8. Odgovornosti Pouzdajuće strane

Pouzdajuća strana može upotrebljavati ID Wallet samo na temelju primjenjivog ugovora ili odobrenog integracijskog odnosa.

Mora se točno identificirati i zahtijevati samo razinu autentikacije i podatke koji su razumno potrebni za navedenu svrhu.

Prije oslanjanja na rezultat Pouzdajuća strana mora, ovisno o primjenjivosti, provjeriti:

- izdavatelja i cjelovitost rezultata;
- namjeravanu publiku i vezivanje uz transakciju;
- valjanost i status rezultata;
- autentikacijski režim Walleta i svaku zasebno primjenjivu razinu pouzdanosti vjerodajnice;
- LoIP PID-a;
- podrijetlo i svježina podataka; i
- sva ograničenja navedena u rezultatu.

Pouzdajuća strana odgovorna je za zakonitu obradu i zaštitu podataka nakon primitka. Ne smije ponovno upotrebljavati podatke ili rezultate autentikacije izvan autorizirane svrhe, osim ako druga pravna osnova dopušta takvu obradu.



Pseudonim specifičan za Pouzdajuću stranu smije se upotrebljavati samo unutar domene za koju je izdan. Pouzdajuće strane ne smiju pokušavati povezati svoje identifikatore s identifikatorima izdanim drugoj strani niti izvesti interni identifikator Walleta Identityuma.

Pouzdanjuca strana ostaje odgovorna za svoju konačnu odluku o odobravanju pristupa, sklapanju transakcije ili prihvatu predstavljenih identifikacijskih podataka.

Pouzdanjuca strana koja primi pseudonimni rezultat autentikacije bez identifikacije ne smije izvesti građanski identitet, LoIP PID-a ili formalnu eIDAS LoA-u koji nisu izričito sadržani u rezultatu.

## 11.9. Odgovornosti i ograničenja Identityuma

Korisnik dobiva osobno, neprenosivo pravo upotrebe ID Walleta u skladu s primjenjivom dokumentacijom i pravom.

Wallet smije upotrebljavati samo fizička osoba kojoj je izdan. Ne smije se prenijeti, dijeliti, prodati ili staviti na raspolaganje drugoj osobi.

Wallet i njegovi rezultati autentikacije ne jamče da će svaka Pouzdajuća strana prihvatiti:

- određeni PID;
- navedeni LoIP;
- određenu eID vjerodajnicu;
- postignuti autentikacijski režim Walleta ili zasebno izraženu razinu pouzdanosti; ili
- Wallet kao dostatan za određenu pravnu ili poslovnu svrhu.

Pouzdanjuca strana ostaje odgovorna za utvrđivanje vlastitih dokaznih i regulatornih zahtjeva te zahtjeva rizika.

Ako nije izričito navedeno drukčije, ID Wallet nije identifikacijska isprava koju izdaje tijelo javne vlasti, prijavljeno nacionalno eID sredstvo ni europski novčanik za digitalni identitet.

Korisnik ne smije predstavljati Wallet, PID ili vjerodajnicu kao da imaju status, razinu pouzdanosti ili pravni učinak veći od onoga koji je izričito naveo Identityum.

Identityum je odgovoran za pružanje ID Walleta u skladu s primjenjivim ugovorom, ovim Pravilnikom i prisilnim propisima.

Identityum primjenjuje razumne tehničke i organizacijske mjere za zaštitu usluge, ali ne jamči neprekinutu dostupnost niti rad svakog vanjskog sustava, uređaja, mreže ili Pouzdajuće strane bez pogreške.

Identityum nije odgovoran za odluke koje samostalno donese Pouzdajuća strana, uključujući odbijanje prihvata PID-a ili rezultata autentikacije, osim ako je Identityum predmetni rezultat izradio netočno.

Odgovornost Identityuma može se ograničiti za gubitak koji proizlazi iz okolnosti izvan njegove razumne kontrole, uključujući:



- zlouporabu ili otkrivanje autentikacijskih faktora od strane Korisnika;
- nesiguran ili kompromitiran uređaj Korisnika;
- netočne podatke koje je dao Korisnik ili vanjski izvor;
- neispunjenje obveza Pouzdajuće strane ili usluge treće strane;
- prekid telekomunikacija ili interneta; i
- događaje više sile.

Nijednim ograničenjem ne isključuje se odgovornost ako je isključenje zabranjeno primjenjivim pravom. Obvezna prava potrošača i odgovornost koja proizlazi iz namjere, krajnje nepažnje ili druge osnove koja se prema zakonu ne može isključiti ostaju neizmijenjeni.

Detaljna ugovorna ograničenja navedena su u primjenjivim Uvjetima korištenja.

Svako ograničenje ili raspodjela odgovornosti podliježe prisilnim propisima i primjenjivim Uvjetima korištenja. Ovim se Pravilnikom samostalno ne stvara financijsko jamstvo, preporuka vrijednosti transakcije ili obveza razine usluge.

### 11.10. Podrška i prijavljivanje sigurnosnih događaja

Opća podrška za Wallet dostupna je putem adrese support@identityum.com i kanala podrške objavljenih za uslugu Walleta. Korisnici putem tih kanala mogu prijaviti gubitak, probleme s pristupom, sumnjivu aktivnost ili druge incidente Walleta.

Pitanja certifikata, opoziva i druga pitanja usluga povjerenja prijavljuju se putem adrese trust@identityum.com ili kanala specifičnog za uslugu navedenog u primjenjivoj dokumentaciji usluga povjerenja. Interno usmjeravanje poruka s tih adresa ne mijenja njihovu javnu svrhu.

### 11.11. Pritužbe i rješavanje sporova

Pritužbe se rješavaju prema primjenjivom objavljenom postupku za pritužbe i Uvjetima korištenja. Identityum bilježi pritužbu, potvrđuje njezin primitak putem dostupnog kontaktnog kanala i daje obrazloženi odgovor u primjenjivom roku.

Ništa u postupku za pritužbe ne ograničava obvezne potrošačke, regulatorne ili sudske pravne lijekove ni pravne lijekove povezane sa zaštitom osobnih podataka. Pritužba na povezanu uslugu treće strane može se proslijediti odgovornom pružatelju ili s njime koordinirati kada je to dopušteno i potrebno.

### 11.12. Mjerodavno pravo

Na ugovor za ID Wallet i ovaj Pravilnik primjenjuje se pravo Republike Hrvatske, uz pridržaj svih prisilnih pravila zaštite potrošača ili drugih pravila koja se primjenjuju na Korisnika neovisno o ugovornom izboru prava.

Strane će prije pokretanja sudskog postupka nastojati riješiti spor putem podrške, pritužbe ili drugog odgovarajućeg mirnog postupka.



Ako se spor ne može riješiti mirnim putem, nadležnost se utvrđuje prema primjenjivom pravu i odredbama Uvjeta korištenja.

Ugovornom odredbom o nadležnosti potrošaču se ne oduzima nijedno obvezno pravo na pokretanje postupka pred drugim nadležnim sudom prema primjenjivom potrošačkom pravu.

Uvjeti korištenja određuju hrvatsko pravo i predviđaju prethodno mirno rješavanje sporova.

### 11.13. Obavješćavanje o promjenama

Identityum može ažurirati uslugu ID Walleta, ovaj Pravilnik, Uvjete korištenja, Pravila privatnosti ili drugi primjenjivi dokument.

Promjena se procjenjuje prema učinku na:

- prava i obveze Korisnika;
- obradu podataka;
- sigurnost i autentikaciju;
- podržane vjerodajnice i tvrdnje o pouzdanosti;
- dostupnost usluge;
- naknade; i
- funkcije povezanih usluga povjerenja.

Važeća verzija i datum stupanja na snagu svakog javnog dokumenta objavljuju se putem primjenjivog kanala Identityuma.

Korisnici se o značajnim promjenama obavješćavaju putem registrirane adrese e-pošte, kanala obavijesti ID Walleta ili druge odgovarajuće elektroničke metode. U obavijesti se opisuju priroda promjene i, kada je primjenjivo, datum stupanja na snagu te sve radnje koje se zahtijevaju od Korisnika.

Promjena za koju je potrebna nova privola ili novi prihvati ne proizvodi učinak za zahvaćenu neobveznu funkciju dok Korisnik ne da potrebnu potvrdu. Ako se obvezna promjena usluge ne može prihvatiti, Korisnik može raskinuti ili opozvati Wallet u skladu s primjenjivim pravilima životnog ciklusa i čuvanja.

Hitne sigurnosne promjene mogu stupiti na snagu prije redovne obavijesti ako bi odgoda izložila Korisnike, Pouzdajuće strane ili uslugu značajnom riziku. Korisnik se naknadno obavješćava čim je to razumno moguće.

Uvjeti korištenja zahtijevaju elektroničku obavijest o značajnim promjenama usluge ili pravila i predviđaju objavu izmijenjenih ugovornih dokumenata.

Značajna promjena koja utječe na izradu Walleta, rezultate autentikacije bez identifikacije, upotrebu PID-a, posljedice životnog ciklusa ili odabire povezanih usluga povjerenja odražava



se u primjenjivim javnim dokumentima prije nego što promijenjena praksa stupi na snagu ili u trenutku njezina stupanja na snagu, uz pridržaj hitnih sigurnosnih mjera.





## Prilozi

### Prilog A — Matrica kanonskih funkcija i granica regulatornog statusa

| Komponenta ili mogućnost    | Kanonski funkcionalni status                                               | Tvrdnja o pouzdanosti ili regulatornom statusu                                                                                                |
|-----------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Prazan Wallet               | Osnovna funkcija Walleta                                                   | Samo kontekst autentikacije i autorizacije; bez PID-a, građanskog identiteta, tvrdnje o eID sredstvu ili eIDAS LoA-e.                         |
| Pseudonimna B2B prijava     | Funkcija Walleta za ugovorene integracije                                  | Identifikator Walleta specifičan za Pouzdajuću stranu i autentikacijski kontekst; nije elektronička identifikacija građanskog identiteta.     |
| Identyum PID                | Rezultat zasebne usluge Identify; opcionalno dostupan kroz Wallet          | Proizvodno specifičan strukturirani identitetski rezultat s LoIP-om koji dodjeljuje Identify; nije PID EUDI Walleta.                          |
| Predstavljanje PID-a        | Funkcija Walleta kada je PID dostupan kroz kopiju ili sigurnu referencu    | Odabrani atributi, podrijetlo, LoIP i informacije o svježini otkrivaju se nakon zasebne autorizacije Korisnika.                               |
| ANSign                      | Zaseban profil usluge povjerenja prema CP-u/TSPS-u                         | Dostupnost i prihvatljivost određuju CP/TSPS i vanjski uvjeti; pohrana PID-a ne izdaje certifikat.                                            |
| NAuth                       | Zaseban certifikacijski profil prema CP-u/TSPS-u                           | Autentikacijski certifikat nije samim time prijavljeno eID sredstvo niti mu Wallet dodjeljuje LoA-u.                                          |
| QNSign                      | Zaseban kvalificirani profil, podložen dovršetku svih vanjskih uvjeta      | Wallet može biti dio autentikacijskog/autorizacijskog sučelja; kvalificirani status i sole control dokazuju se mjerodavnim TSPS/SSAS opsegom. |
| COL-C / COL-D               | Mehanizmi usluge Identify; izvan normativnog opsega Wallet PS-a            | Njihovi use caseovi, dokazi i LoIP uređuju se dokumentacijom Identifyja/TSPS-om, ne ovim Pravilnikom.                                         |
| Identyum SMS / WEB / MOBILE | Zasebne eID vjerodajnice ili profili; izvan normativnog opsega Wallet PS-a | Dostupnost i eventualna LoA-a utvrđuju se vlastitim profilom i vanjskim odobrenjem, a ne iz Walleta.                                          |



| Komponenta ili mogućnost                 | Kanonski funkcionalni status                                | Tvrdnja o pouzdanosti ili regulatornom statusu |
|------------------------------------------|-------------------------------------------------------------|------------------------------------------------|
| Europski novčanik za digitalni identitet | Vanjski regulatorni status koji se ovim dokumentom ne tvrdi | Identyum ne tvrdi da ima status EUDI Walleta.  |



## Prilog B — Zahtjevi autentikacije prema radnji

| Radnja                                    | Zadana autentikacija Walletom                                                 | Važno ograničenje                                                         |
|-------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Izrada novog Walleta                      | AUTH-A + AUTH-D tijekom jedne valjane sesije upisa                            | AUTH-D ne dokazuje građanski identitet niti izdaje PID.                   |
| Pseudonimna B2B prijava                   | AUTH-A + odobreni drugi faktor                                                | Bez PID-a ili eIDAS LoA-e, osim ako su zasebno utvrđeni i objavljeni.     |
| Dodavanje ili izmjena podataka PID-a      | AUTH-A + AUTH-D; stroži režim može dodati AUTH-E                              | Provjera identiteta ili validacija odvojena je od autentikacije Walletom. |
| Predstavljanje atributa PID-a             | AUTH-A + AUTH-D ili AUTH-E, kako je dopušteno                                 | Potrebni su zaseban zahtjev za podatke i autorizacija Korisnika.          |
| Promjena faktora                          | Kako je definirano kontroliranom autentikacijskom politikom                   | Nedostupni faktori mogu zahtijevati suspenziju, oporavak ili zamjenu.     |
| Suspenzija Walleta                        | Odobrena autentikacija za suspenziju ili radnja Identityuma na temelju rizika | Status certifikata ostaje nepromijenjen samo zbog suspenzije Walleta.     |
| Ponovna aktivacija Walleta                | Odobrena kombinacija za ponovnu aktivaciju i svaki potrebni pregled           | Ne obnavlja istekli ili opozvani certifikat.                              |
| Trajno zatvaranje Walleta                 | Odobreni postupak trajnog ukidanja                                            | Opozivaju se vezani dugoročni ANSign, NAuth i QNSign.                     |
| Autorizacija QNSign/QES-a s pomoću AUTH-E | Mrežni push postupak izazov–odgovor                                           | Izvanmrežni TOTP nije dostupna metoda aktivacije QES-a.                   |



## Prilog C — Matrica životnog ciklusa Walleta, PID-a, certifikata i ključa

| Događaj                                                  | Učinak na Wallet/PID                                                                | Učinak na certifikat/ključ                                                                                             |
|----------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Izrada Walleta                                           | Prazan aktivni Wallet; bez PID-a, osim ako je zasebno izdan i pohranjen             | Bez certifikata, osim ako je zasebno zatražen, izdan i prihvaćen.                                                      |
| PID je izdan, ali je pohrana odbijena                    | Wallet ostaje prazan; PID se može upotrijebiti za trenutačnu transakciju            | Prihvatljivi certifikat i dalje se može zatražiti s pomoću zasebno zadržanih dokaza.                                   |
| PID je pohranjen                                         | PID postaje aktivni sadržaj Walleta                                                 | Nema automatskog izdavanja certifikata.                                                                                |
| PID je zastario                                          | Ponovna upotreba ili otkrivanje mogu zahtijevati osvježavanje ili pojačanu provjeru | Status postojećeg certifikata ostaje nepromijenjen; za novo izdavanje ili transakciju mogu se zahtijevati novi dokazi. |
| PID je uklonjen                                          | PID više nije dostupan kao sadržaj Walleta                                          | Status postojećih certifikata ANSign, NAuth i QNSign ostaje nepromijenjen samo zbog uklanjanja.                        |
| Wallet je suspendiran                                    | Radnje Walleta privremeno su blokirane                                              | Upotreba ključa utemeljena na Walletu blokirana je; status certifikata ostaje nepromijenjen.                           |
| Wallet je ponovno aktiviran                              | Nastavljaju se dopuštene radnje Walleta                                             | Upotreba se nastavlja samo ako su certifikat/ključ i sve druge ovisnosti i dalje valjani.                              |
| Wallet je trajno zatvoren                                | Wallet se ne može ponovno aktivirati                                                | Opozivaju se vezani dugoročni ANSign, NAuth i QNSign; ovaj događaj sam po sebi ne utječe na QLSeal.                    |
| Certifikat je istekao ili je opozvan                     | Wallet i PID mogu ostati aktivni                                                    | Prestaju zahvaćeni certifikat i njegova dopuštena upotreba ključa.                                                     |
| Upotreba upravljanog ključa blokirana je tijekom istrage | Wallet se može zasebno suspendirati kada je to primjereno                           | Radnja ključa je blokirana; status certifikata ostaje nepromijenjen do odluke o opozivu.                               |



## Prilog D — Matrica rezultata autentikacije bez identifikacije i otkrivanja PID-a

| Element rezultata                                         | Autentikacija bez identifikacije | Autentikacija uz otkrivanje PID-a                                               |
|-----------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------|
| Identitet izdavatelja Identityuma                         | Uključen                         | Uključen                                                                        |
| Namjeravana publika / Pouzdajuća strana                   | Uključena                        | Uključena                                                                       |
| Vezivanje uz transakciju i vrijeme                        | Uključeno                        | Uključeno                                                                       |
| Pseudonimni identifikator specifičan za Pouzdajuću stranu | Uključen kada je potreban        | Može biti uključen kada je potreban                                             |
| Autentikacijski režim Walleta                             | Uključen ili naveden upućivanjem | Uključen ili naveden upućivanjem                                                |
| Građansko ime ili nacionalni identifikator                | Nije uključen                    | Uključen samo ako je zatražen, dostupan i autoriziran                           |
| LoIP i podrijetlo PID-a                                   | Nisu uključeni                   | Uključeni u opsegu potrebnom za tumačenje i pouzdanje                           |
| Formalna eIDAS LoA                                        | Nije uključena                   | Nije uključena, osim ako je izričito pruža zasebna primjenjiva eID vjerodajnica |
| Drugi sadržaj Walleta                                     | Nije uključen                    | Nije uključen izvan autoriziranog opsega podataka                               |



## Prilog E — Matrica dokaza i čuvanja

| Događaj ili zapis                                     | Najmanja dokazna svrha                                                                                                     | Primjenjiva kategorija čuvanja                                                                    |
|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Izrada Walleta                                        | Identifikator računa, prihvata Uvjeta korištenja, uspostava faktora i aktivacija                                           | Ugovorni/sigurnosni zapis Walleta prema primjenjivom rasporedu čuvanja                            |
| Identify postupak i izdavanje PID-a                   | Izvori, provjere, povezivanje, odluka, LoIP i izdani rezultat; vodi ih Identify ili dokazni sustav QTSP-a, ne Wallet       | Kategorija dokaza Identifyja ili QTSP-a prema mjerodavnom TSPS-u; izvan aktivnog sadržaja Walleta |
| Odabir pohrane PID-a                                  | Prikazani podaci i radnja Korisnika „pohrani/preskoči”                                                                     | Dokaz Walleta; povezan s dokazom o identitetu kada je primjenjivo                                 |
| Zahtjev za povezanu uslugu povjerenja                 | Točan profil, upućeni dokumenti, radnja Korisnika i referenca transakcije; puni pretplatnički dokaz vodi usluga povjerenja | Dokaz QTSP-a o Pretplatniku/certifikatu — deset godina                                            |
| Prihvata ili aktivacija certifikata                   | Sadržaj certifikata, serijski broj/profil, radnja prihvata, vrijeme i rezultat                                             | Dokaz QTSP-a o certifikatu — deset godina                                                         |
| Autentikacija Walletom                                | Pouzdajuća strana, transakcija, kategorije faktora, ishod i metapodaci tvrdnje                                             | Opći zapis ili dokaz više kategorije prema svrsi                                                  |
| Predstavljanje PID-a                                  | Primatelj, svrha, opseg, autorizacija i dostavljeni atributi                                                               | Dokaz Walleta/privatnosti ili dokaz regulirane transakcije, ovisno o primjenjivosti               |
| Suspenzija, ponovna aktivacija ili zatvaranje Walleta | Inicijator, autentikacija, razlog, odluka, obavijest i rezultat                                                            | Dokaz životnog ciklusa/sigurnosti Walleta                                                         |
| Opoziv certifikata                                    | Zahtjev/prijava, verifikacija, odluka, objava statusa i obavijest                                                          | Dokaz QTSP-a o certifikatu — deset godina                                                         |

Ako isti zapis podupire više kategorija, primjenjuju se najdulje primjenjivo zakonito razdoblje čuvanja i najstroža primjenjiva kontrola pristupa, bez produljivanja dostupnosti aktivnog Walleta.



## Prilog F — Matrica primjenjivosti regulative i mjerodavnih dokumenata

| Izvor zahtjeva                                                                | Primarno područje i mjerodavni dokument                                                                                  | Odnos prema Wallet PS-u                                                                                                                                       |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Provedbena uredba Komisije (EU) 2015/1502                                     | Prijavljeni sustavi i sredstva elektroničke identifikacije; mjerodavna dokumentacija eID sustava                         | Odabrana načela služe dizajnu; Wallet ni autentikacijski režim nemaju LoA-u bez zasebnog formalno ocijenjenog eID sustava.                                    |
| ETSI TS 119 461                                                               | Identify/identity-proofing service; TSPS za uporabu u uslugama povjerenja i dokumentacija Identifyja za ostale kontekste | OVR-6.1-02/-03 i COL-8.2.1-06X ispunjavaju se identifikacijom use caseova, izvora dokaza i konteksta u mjerodavnoj praksi Identifyja/TSP-a, ne u Wallet PS-u. |
| ETSI EN 319 401                                                               | Opći zahtjevi za TSP i njegove prakse; TSPS i sustav upravljanja TSP-a                                                   | Na Wallet se odnosi samo kao na komponentu u opsegu određene usluge povjerenja; ne primjenjuje se na sve funkcije Walleta.                                    |
| ETSI EN 319 411-1 i ETSI EN 319 411-2                                         | Politike, registracija, izdavanje i životni ciklus certifikata; CP i TSPS/CPS                                            | Wallet uređuje korisničko sučelje i autentikaciju/autorizaciju; ne određuje profil, prihvatljivost ni status certifikata.                                     |
| ETSI TS 119 431-1                                                             | SSAS, SAD, sole control i udaljeno potpisivanje; TSPS i dokumentacija udaljenog QSCD/SSAS-a                              | Wallet može prenositi autentikacijski rezultat i potvrdu transakcije; sam nije QSCD niti sam dokazuje zahtjeve za QES.                                        |
| ETSI TS 119 472-2 i ETSI TR 119 462                                           | EUDI Wallet, EAA i EUDI PID/presentation kontekst                                                                        | Informativno za interoperabilnost kada se izričito primijeni; proizvodno specifični Identityum PID time ne postaje EUDI PID.                                  |
| Članak 5.a eIDAS-a i provedbeni akti EUDI Walleta, uključujući (EU) 2024/2979 | EUDI Wallet status, certificiranje i ekosustav Pouzdajućih strana                                                        | Ovaj Pravilnik ne tvrdi EUDI Wallet status; takva je tvrdnja dopuštena tek nakon svih propisanih vanjskih postupaka.                                          |



| Izvor zahtjeva              | Primarno područje i mjerodavni dokument                                       | Odnos prema Wallet PS-u                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Uredba (EU) 2016/679 (GDPR) | Obrada osobnih podataka; Pravila privatnosti i dokumentacija konkretne obrade | Uloge i pravne osnove određuju se prema stvarnoj svrsi i aktivnosti Walleta, Identifikacija, TSP-a i Pouzdajuće strane. |