



Konferencija Srce DEI

Europska digitalna lisnica i provjerljive vjerodajnice

Uvod i iskustvo iz Srca

Marko Ivančić

AAI@EduHr

Srce DEI 2026





Sadržaj

- (Fizička) Vjerodajnica, prednosti i nedostaci
- Digitalna provjerljiva vjerodajnica
- Digitalna lisnica
- Asimetrična kriptografija
- Iskustvo iz Srca kroz rad u GÉANTu
- Demo implementacije izdavatelja



Vjerodajnica (eng. Credential)

- Potvrda, dokaz o nekoj činjenici o nekom entitetu (tipično o osobi ili organizaciji) koju je izdala ovlaštena institucija (npr. ministarstvo, sveučilište, banka...)
- Primjeri:
 - Osobna iskaznica – potvrda identiteta, tipično na nacionalnoj razini
 - Putovnica – potvrda identiteta u međunarodnom kontekstu
 - Vozačka dozvola – potvrda o sposobnosti za upravljanjem vozilom
 - Diploma – potvrda o razini edukacije
 - ...
- Primjeri podataka:
 - Podaci o tipu potvrde (osobna iskaznica, putovnica...)
 - Podaci o subjektu, npr. ime i prezime, datum rođenja, fotografija, naziv institucije, identifikacijski broj...
 - Podaci o izdavatelju
 - Ograničenja, npr. datum izdavanja i isteka, trajanje, vrijeme “važenja”



Nedostaci fizičkih vjerodajnica

- Relativno teško za (re)izdati (dugotrajno i skupocjeno)
- Nemoguće ih je na siguran način provjeriti na daljinu
- Otkrivaju previše podataka pri svakom korištenju



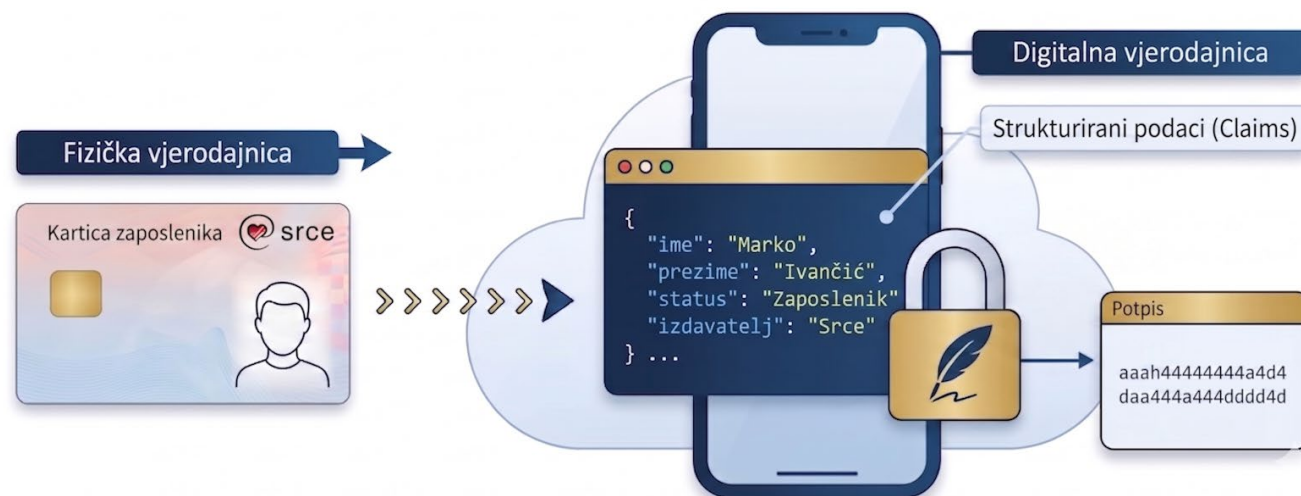
Digitalna vjerodajnica

- Struktura podataka sa skupom tvrdnji (eng. Claims) o:
 - entitetu, subjektu vjerodajnice
 - izdavatelju
 - metapodacima (npr. trajanje)

- Tvrdnja

- 'svojstvo': 'vrijednost'
- 'ime': 'Marko'
- 'izdavatelj': 'Srce'

- Strojno čitljiva
- Kriptografski potpisana





Vjerodajnica kao niz znakova





Provjerljiva vjerodajnica

- Moguća provjera autentičnosti i integriteta pomoću kriptografskog potpisa
- Provjerom se utvrđuje
 - tko je izdavalac
 - je li sadržaj promijenjen
 - je li još uvijek valjana (istek)
 - je li opozvana



Prednosti digitalnih vjerodajnica

- Brzo i relativno lako (re)izdavanje
- Sigurna provjera na daljinu (strojna čitljivost)
- Otkrivanje samo nužnih podataka za korištenje usluge (selektivna prezentacija)
- Standardizirani formati vjerodajnica
- Nema “središnjih servisa” ili “središnjih baza podataka”



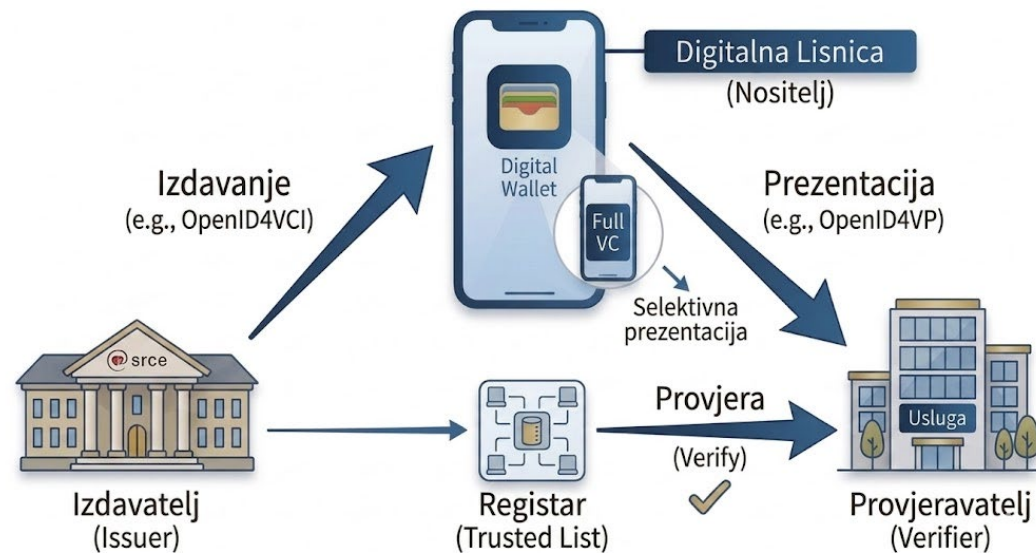
Digitalna lisnica (eng. Wallet)

- Aplikacija, servis za spremanje, čuvanje i korištenje digitalnih vjerodajnica
- Omogućuje sigurno dijeljenje podataka
- Korisnik kontrolira što i kada dijeli



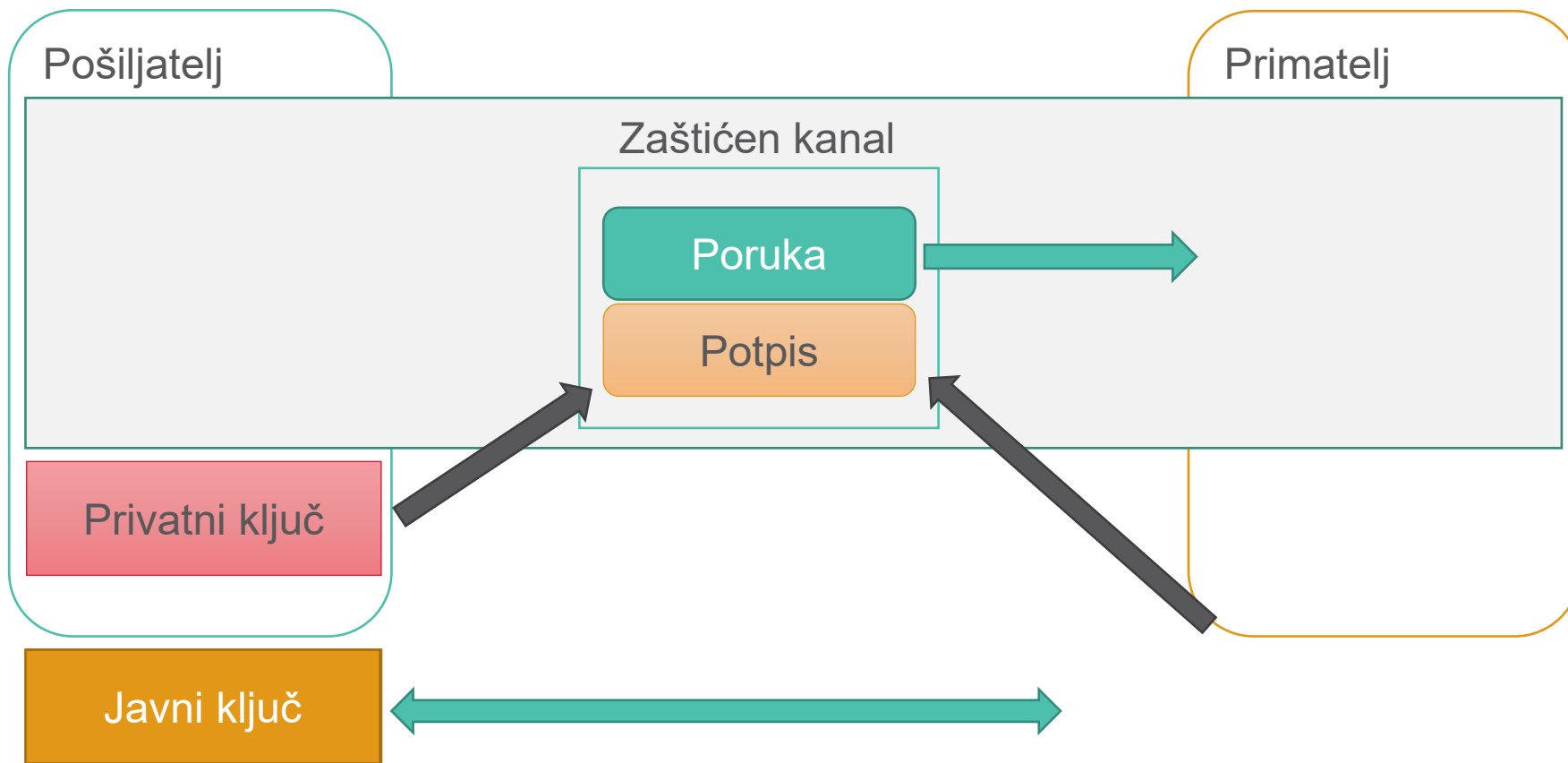
Trokut povjerenja

- Izdavatelj (Issuer)
 - organizacija, kreira i izdaje vjerodajnicu
- Nositelj (Holder)
 - osoba, organizacija, prima i sprema vjerodajnicu u digitalnu lisnicu
- Provjeravatelj (Verifier)
 - “strana” koja traži, prima i provjerava vjerodajnicu





Asimetrična kriptografija





Prednosti i izazovi ekosustava povjerljivih vjerodajnica

- Kontrola korisnika nad podacima
 - Brže omogućavanje digitalnih usluga
 - Selektivno otkrivanje podataka
 - Smanjenje prijevara
 - Otvoreni standardi
-
- Interoperabilnost
 - Upravljanje ključevima
 - Usklađivanje s aktima
 - Komplicirani standardi



Iskustvo Srca

- Sudjelovanje u projektu GÉANT Trust & Identity Incubator
- Aktivnost: “Implement OID4VCI/VP in SimpleSAMLphp and Shibboleth IdP”
- Uloga Srca: implementacija protokola “OpenID for Verifiable Credential Issuance OpenID4VCI” u alatu SimpleSAMLphp





Motivacija

- SimpleSAMLphp i Shibboleth su često korišteni open-source alati za uspostavu uloge “davatelja identiteta” u federacijama e-identiteta akademskih okruženja
- Akademске institucije davatelja e-identiteta tipično raspolažu mnoštvom provjerenih podataka o korisnicima, pa su dobar izbor i za ulogu izdavatelja vjerodajnica



Implementacija

- Autorizacijski tijekovi
 - Pre-authorized Code Flow (novi tijek definiran u specifikaciji OpenID4VCI)
 - Authorization Code Flow (OAuth2 autorizacijski tijek)
- Formati vjerodajnica
 - dc+sd-jwt (SD-JWT)
 - jwt_vc_json (VCDM v1.1 pomoću JWS)
 - vc+sd-jwt (VCDM 2.0 pomoću SD-JWT)
- Tipovi dokaza (eng. Proof Types):
 - jwt
- Mogućnost testiranja izdavanja vjerodajnica u admin sučelju SimpleSAMLphp modula
- API za dohvat ponuda vjerodajnica
- <https://github.com/simplesamlphp/simplesamlphp-module-oidc/tree/wip-version-7>

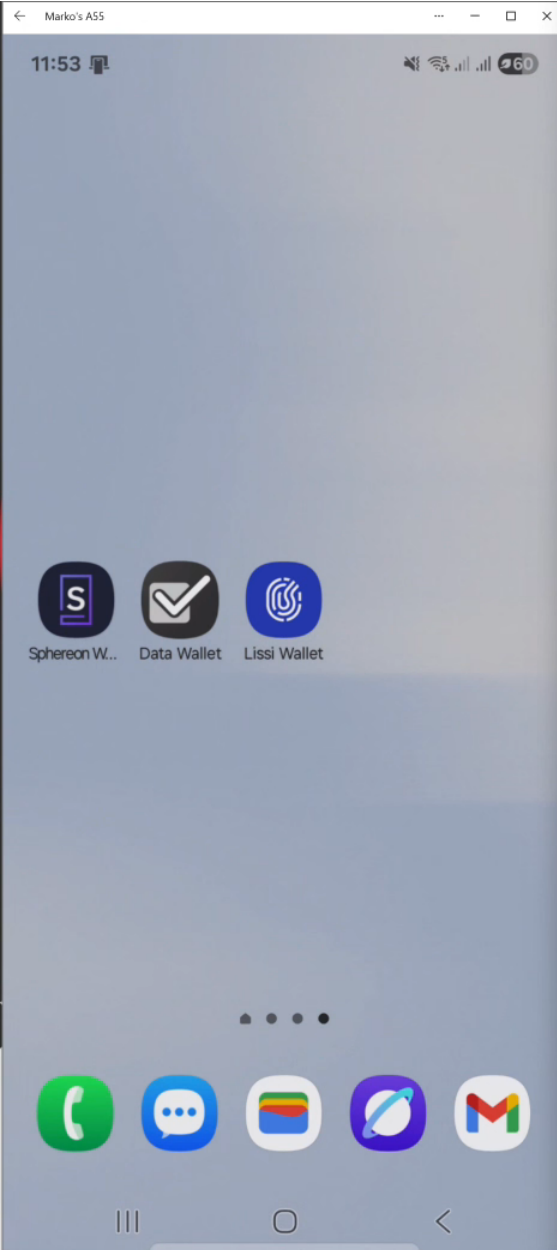


Podrška u lisnicama

Prosinac 2025.
Ožujak 2026.

Pre-authorized Code Flow			
Wallet / VC Format	jwt_vc_json	dc+sd-jwt	vc+sd-jwt
Sphereon	Da	Da	
Data	Da	Da	
Lissi		Da	
Paradym		Da	
Paradym			
Paradym		Da	

Authorization Code Flow			
Wallet / VC Format	jwt_vc_json	dc+sd-jwt	vc+sd-jwt
Sphereon			
Data			
Lissi		Yes	
Paradym		Yes	
Paradym			
Paradym		Da	



idp.mivanci.incubator.hexaa.eu/ssp/module.php/oidc/admin/test/verifiable-credential-issuance

SimpleSAMLphp

English

Configuration Test Federation **OIDC** Profile Page Log out

OIDC

- Database Migrations
- Client Registry
- Protocol Settings
- Federation Settings
- Test Trust Chain Resolution
- Test Trust Mark Validation
- Verifiable Credential Settings
- Test Verifiable Credential Issuance**


Test Verifiable Credential Issuance

You are currently authenticated with the following user data:

```
{
  "uid": [
    "testuserid"
  ],
  "eduPersonPrincipalName": [
    "testuser@example.com"
  ],
  "eduPersonTargetedID": [
    "abc123"
  ],
  "displayName": [
    "Test User"
  ],
  "givenName": [
    "Test"
  ],
  "sn": [
    "User"
  ],
  "mail": [
    "testuser@example.com"
  ],
  "eduPersonAffiliation": [
    "member",
    "guest"
  ],
  "o": [
    "Test Organization"
  ],
  "eduPersonScopedAffiliation": [
    "member@example.com",
    "guest@example.com"
  ]
}
```

Credential Offer:

```
openid-credential-offer://credential_offer={"credential_issuer":"https://\idp.mivanci.incubator.hexaa.eu","credential_configuration_ids":["ResearchAndScholarshipCredentialDc5d3wt"],"grants":{"urn:ietf:params:oauth:grant-type:pre-authorized_code":{"pre_authorized_code":"_a4e8139a2c416fc0a208e1b106322ff4688512dac2","tx_code":{"input_mode":"numeric","length":4,"description":"Please provide the one-time code that was sent to e-mail testuser@example.com"}}}}
```



Clear

idp.mivanci.incubator.hexaa.eu



11:53
22.09.2025.



Hvala na pažnji



Ovo djelo je dano na korištenje pod licencom Creative Commons *Imenovanje* 4.0 međunarodna.

Srce politikom otvorenog pristupa široj javnosti osigurava dostupnost i korištenje svih rezultata rada Srca, a prvenstveno obrazovnih i stručnih informacija i sadržaja nastalih djelovanjem i radom Srca.

www.srce.unizg.hr

creativecommons.org/licenses/by/4.0/deed

www.srce.unizg.hr/otvoreni-pristup

