Recommendation- step-by-step approach

Step-by-step план

1. Дефинирање на credential тип и claims

- Пример: `StudentIDCredential` со `studentId`, `fullName`, `faculty`, `enrolledUntil`.
- VC payload да личи на VC Data Model v2: `@context`, `type`, `issuer`, `validFrom`, `credentialSubject`.

1. Key management (Issuer + Holder)

- Генерирање ECDSA P-256 клуч (ES256) или Ed25519
- Issuer објавува јавен клуч како JWKS (за verifier да може да верификува потпис без hardcode).

1. Issuance (Issuer → Holder)

- `POST /issue` прима податоци за студент (или ги зема од mock база) и враќа VC како JWS/JWT.
- Во header се става `typ: "vc+jwt"` (препорачано во JOSE/COSE спецификацијата) и `kid` што реферира на клучот во JWKS.
- Во payload ставаш VC JSON (како „unsecured VC“) и се потпишува.

1. Wallet storage (Holder)

- `POST /store` зачувува добиениот VC JWT во SQLite (табела: `credentials(id, jwt, issuer, type, stored_at)`).
- Правење на едноставна UI страница за листа + „present“ копче (за screenshots во документација).

1. Presentation (Holder → Verifier) со challenge (анти-replay)

- `GET /challenge` на verifier враќа `nonce` (и рок на важност).
- Holder креира VP JWT: вметнува VC (или референца), додава `nonce`, `aud`, `iat/exp`, и го потпишува со свој клуч. VC Data Model

објаснува дека презентација е „subset of persona“ што holder ја користи за да презентира claims.

- `POST /verify` праќа VP (или директно VC ако сакаш simplest demo, но VP е поинтересно).

1. Verification (Verifier)

- Го верификува потписот на VP (holder key) и потписот на VC (issuer key преку JWKS fetch).
- Проверува: `exp`, `type`, `issuer`, `nonce` (да е свеж и да не е употребен).
- Важно: Треба да се одбие JWT ако `"alg":"none"`.

Сигурносни аспекти

- Интегритет/автентичност: потпис на VC/VP (JWS) според W3C JOSE/COSE насоки.
- Privacy: минимизација на податоци (пр. Verifier бара само `faculty` + „active enrollment“, не цела адреса); VC Data Model експлицитно зборува за privacy ризик од корелација и потреба од внимателен избор на идентификатори.
- Anti-replay: `nonce` + краток `exp` за VP.
- Key safety: приватните клучеви не се комитираат нели; ќе ги чуваме encrypted/во `.env`