IODM / WP-001

Interoperabilni dostopni medij

Odprta in interoperabilna kontrola dostopa

Različica: 0.4 · delovni osnutek
Datum: 25. november 2026
Spletno mesto: iodm.si

Povzetek
IODM je predlog odprtega tehničnega profila, ki ločuje dostopni medij, izdajatelja, čitalnik in sistem kontrole dostopa. Cilj je omogočiti neodvisne implementacije z javnimi ključi in preverljivim zaupanjem. Dokument je informativen; normativne zahteve določajo IODM-001 do IODM-007.

1. Od skupnih skrivnosti do individualnih ključev
Pri nekaterih tradicionalnih sistemih razkritje skupnega ključa ogrozi več naprav. Individualni neizvozljivi ključi omejijo posledice kompromitacije posameznega medija. Potrdilo X.509 omogoča preverjanje, kdo je izdal ključ. Svež izziv in podpis dokazujeta posedovanje ključa, ne pa pravice dostopa. Tudi PKI ima skupne točke tveganja, zato je zaščita CA bistvena.

2. Interoperabilnost brez vezanosti na čip
Enotni APDU in natančen profil potrdila omogočajo namenskim čipom in programirljivim karticam enako obnašanje. IODM ne zahteva proizvajalčevega SDK ali skupnih skrivnosti v čitalniku. Potrditev skladnosti posamezne izvedbe in neodvisni preskusi so potrebni pred trditvami o združljivosti.

3. Federativno zaupanje
Izdajatelji imajo lastne CA, javni podpisani register na iodm.si pa omogoča distribucijo potrjenih ključev. Upravljavec SKD izbere dovoljene izdajatelje; vpis v register sam po sebi ne omogoča dostopa. Čitalnik lahko deluje brez povezave, dokler ima sveže in veljavne podatke o zaupanju ter preklicu.

4. Identiteta in obstoječi sistemi
IODM-ID združuje 16-bitni identifikator izdajatelja in 32-bitni identifikator medija. Vrednost je v podpisanem subject.serialNumber potrdila. Obnova potrdila ne spremeni identitete istega medija. Za starejše sisteme je mogoča nadzorovana preslikava; statični UID sam ni varnostni dokaz. Podpisan manifest omogoča množični uvoz, medtem ko avtorizacija ostaja ločen korak.

5. Fizični in mobilni mediji
Pasivni mediji ne potrebujejo baterije ali omrežja. Mobilne poverilnice imajo drugačne možnosti in omejitve. IODM ne zahteva Aliro niti ne trdi združljivosti z njim ali z LEAF Verified. Skupna uporaba ECC in standardnih transportov omogoča delitev nekaterih komponent, ne pa samodejne protokolarne združljivosti.

6. Varnostne meje
Javno berljiva potrdila so lahko sledljiva. Osnovni profil ne zagotavlja zaupnosti, avtentikacije čitalnika ali zaščite pred relay napadi. Varovanje komunikacije do SKD, preklic, upravljanje pravic in fizična varnost vrat so nujni deli celotne rešitve.

7. Pot do ekosistema
Javne specifikacije, ločeni preskusi medijev in čitalnikov, potrditev izdajateljev ter register omogočajo pregledno vključevanje novih ponudnikov. Trenutna izdaja je razvojni osnutek; ni objavljenih potrjenih izdajateljev ali certificiranih izdelkov. Potrebni so fizični preskusi, strokovni pregled in vzpostavitev upravljanja registra.