IODM / 005

Interoperabilni dostopni medij

Register zaupanja vrednih izdajateljev

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

1. Namen

IODM-005 določa javni register potrjenih izdajateljev, CA in pooblaščenih ključev za manifeste. MORA označuje obveznost. Normativne osnove: IODM-001, 004, 006, 007; RFC 5280, RFC 5652, RFC 8259. Register ne dodeljuje pravic dostopa.

2. Distribucija

Pot na iodm.si	Vsebina
/trust/	Javni pregled
/trust/v1/manifest.json	UTF-8 JSON
/trust/v1/manifest.p7s	Ločeni DER CMS SignedData
/trust/v1/ca/	DER potrdila CA

HTTPS je obvezen, vendar ni nadomestilo podpisa. Podpisnik registra uporablja namenski P-256 ključ, javni ključ se namesti neodvisno in varno; menjava se odobri izven registra. Register se objavi najmanj vsakih 24 ur, veljavnost največ 7 dni. Zaporedna številka je naraščajoče pozitivno celo število največ 2^53−1; ponovna uporaba številke za različne bajte je prepovedana.

3. Podatkovni model

JSON brez BOM in podvojenih ključev. Vsa navedena polja so obvezna. Neznana polja se v različici 1 zavrnejo. Čas je RFC 3339 UTC v obliki YYYY-MM-DDThh:mm:ssZ. IID je 4-mestni veliki hex po IODM-006. SHA-256 je 64-mestni veliki hex nad DER. Polji issuers in certificates sta tabeli; identifikatorji so enolični. Veljavnost vpisa mora zajemati trenutek preverjanja. Status je active, suspended, withdrawn ali expired. Vloga potrdila je trustAnchor, intermediate ali manifestSigner; CA imajo obseg iz IODM-004. Vpis izdajatelja vsebuje vsaj eno aktivno sidro, kadar je aktiven. Vsa vmesna CA potrdila za odobrene poti morajo biti objavljena. Status in čas vpisa se preverjata poleg veljavnosti potrdil. Vloga trustAnchor zahteva samopodpisan CA; intermediate zahteva neposredno podrejenost registriranemu sidru istega IID. Isti prstni odtis ne sme biti dodeljen več IID. URL mora biti HTTPS na iodm.si, brez preusmeritev na drugo domeno. ManifestSigner je nekorensko potrdilo P-256 z digitalSignature, CA=FALSE, registrirano za točno določen IID; ne šteje kot sidro zaupanja.

```
{
  "schemaVersion": 1,
  "sequenceNumber": 42,
  "issuedAt": "2026-11-25T00:00:00Z",
  "nextUpdate": "2026-12-02T00:00:00Z",
  "issuers": [{
    "issuerId": "0001",
    "name": "Primer izdajatelja",
    "status": "active",
    "validFrom": "2026-11-25T00:00:00Z",
    "validUntil": "2027-11-25T00:00:00Z",
    "securityContact": "security@example.org",
    "certificates": [{
      "certificateId": "0001-01",
      "role": "trustAnchor",
      "status": "active",
      "url": "https://iodm.si/trust/v1/ca/0001-01.crt",
```

```
      "sha256": "<64 HEX>"
    }]
  }]
}
```

Primer je nenormativen in neveljaven kot produkcijski register. Omejitve: največ 10 MiB za JSON, največ 4096 B na potrdilo, največ 65534 izdajateljev. Polje certificateId je ASCII 1–64 znakov iz A–Z, a–z, 0–9, vezaja in podčrtaja. Naziv in kontakt sta neprazna niza največ 256 znakov.

4. Profil CMS

CMS ContentInfo vsebuje SignedData (OID 1.2.840.113549.1.7.2), eContentType id-data (1.2.840.113549.1.7.1), eContent odsoten. En SignerInfo, digestAlgorithm SHA-256 (2.16.840.1.101.3.4.2.1), signatureAlgorithm ecdsa-with-SHA256 brez parametrov. signedAttrs obvezno vsebuje natanko en content-type in message-digest, vezan na natančne bajte JSON; podpis se preveri po RFC 5652 nad DER SET OF signedAttrs. Potrdila podpisnika se lahko vdelajo; vdelano potrdilo ne vzpostavlja zaupanja. SignerIdentifier se mora ujemati s potrdilom podpisnika. Podpis mora biti veljaven ECDSA DER SEQUENCE. Podpis mora ustrezati neodvisno nameščenemu ključu registra. Čas veljavnosti izvira iz podpisanega JSON, ne iz nepreverjenega HTTP časa.

5. Aktivacija in preklic

Preveri velikost, CMS, JSON, čas, zaporedje, veljavnost vpisov in SHA-256 vseh potrebnih potrdil, nato atomsko aktiviraj. Najvišje sprejeto zaporedje se trajno shrani; enaka številka je dovoljena samo za identične bajte. Zavrni neveljaven paket; zadnji veljavni paket velja največ do nextUpdate. Pri izteku ali nedostopnem svežem registru dostop zavrni. Lokalna politika je lahko strožja. suspended/withdrawn/expired izdajatelj ali CA se izloči iz novih avtentikacij. Register ne nadomesti CRL/OCSP. Čitalnik mora vezati izbrano pot do sidra in IID na aktiven vpis; ne sme združevati poti med IID.

6. Preskusi

ID	Preskus	Merilo
TR-01	Veljaven paket	Atomska aktivacija
TR-02	Spremenjen JSON ali podpis	Zavrnitev
TR-03	Nepooblaščen podpisnik	Zavrnitev
TR-04	Staro zaporedje ali iztek	Zavrnitev
TR-05	Napačen hash CA ali podvojen IID	Zavrnitev
TR-06	Umik izdajatelja ali CA	Brez nove avtentikacije
TR-07	Izpad med zapisom	Stara veljavna ali nova celota
TR-08	Menjava CA	Samo odobreno prekrivanje

Produkcijski register še ni vzpostavljen; primeri niso dokaz potrditve.