IODM / 007

Interoperabilni dostopni medij

Elektronski manifest dostopnih medijev

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

1. Namen

IODM-007 določa prenos podatkov o izdanih medijih za množični uvoz v SKD. Uvoz ne dokazuje posedovanja ključa in ne dodeljuje dovoljenj. MORA označuje obveznost. Normativna osnova: IODM-001, 004, 005, 006, RFC 5652 in RFC 8259.

2. Oblika in podpis

Manifest je UTF-8 JSON brez BOM ali podvojenih ključev, največ 10 MiB; največ 10000 medijev v posameznem manifestu. Ločeni podpis DER CMS sledi IODM-005 § 4, le da se uporablja aktivni manifestSigner istega IID iz registra. Podpisni ključ ni ključ CA ali medija. Vsa navedena polja so obvezna, neznana polja se zavrnejo. Čas RFC 3339 UTC, identifikator manifestId UUID (RFC 9562), IID in IODM-ID kanonični hex. Veljavnost manifesta največ 30 dni. formFactor je card, fob ali other. certificateSha256 je 64 velikih hex znakov nad DER končnega potrdila.

```
{
  "schemaVersion": 1,
  "manifestId": "a9b5a3da-67c2-4cd0-9b23-a3e15ee5f8d2",
  "issuerId": "0001",
  "issuedAt": "2026-11-25T00:00:00Z",
  "expiresAt": "2026-12-25T00:00:00Z",
  "credentials": [{
    "iodmId": "000100001234",
    "formFactor": "card",
    "profile": "IODM-001/0.4",
    "certificateSha256": "<64 HEX>"
  }]
}
```

Primer je ilustrativen. Vsi IODM-ID znotraj manifesta morajo biti enolični in imeti IID iz glave. Ne sme vsebovati osebnih podatkov, zasebnih ključev ali PIN.

3. Distribucija in uvoz

Manifest se dostavi prek avtenticiranega kanala ali zaščitenega prevzema (QR povezava ni sama po sebi dokaz zaupanja). Prejemnik preveri velikost, podpis, pooblastilo podpisnika, aktivni IID, čas, strukturo, enoličnost in lokalno politiko; šele nato atomsko uvozi. Že uvožen manifestId z enakimi bajti se obravnava idempotentno, druga vsebina se zavrne. Konflikt identitete ali prstnega odtisa zahteva ročno presojo, ne samodejne prevezave. Ob prvi uporabi medija se preveri certifikat in svež podpis; če se prstni odtis ne ujema, se zahteva nadzorovana obnovitev evidence. Dovoljenja dodeli pooblaščeni administrator ločeno.

4. Preskusi

ID	Preskus	Merilo
MF-01	Veljaven podpis in zapis	Uvoz brez dodelitve pravic
MF-02	Napačen podpis ali drug IID	Zavrnitev
MF-03	Podvojen IODM-ID ali napačen hash format	Zavrnitev
MF-04	Ponovni uvoz identične datoteke	Brez podvajanja
MF-05	Enak manifestId, druga vsebina	Zavrnitev

MF-06	Iztek ali umik podpisnika	Zavrnitev
MF-07	Prekinitev uvoza	Atomska obravnava
MF-08	Medij s kopiranim potrdilom	Brez dostopa brez dokaza posedovanja