**IODM / 003**

# Interoperabilni dostopni medij

Ugotavljanje skladnosti čitalnikov

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

## 1. Predmet in področje uporabe

IODM-003 določa ugotavljanje skladnosti čitalnika in pripadajoče komponente za preverjanje. Če se PKI ali avtorizacija izvaja v zaledju, se preskuša celotna prijavljena kombinacija, vključno z varnostjo povezave. Čitalnik ne sme odobriti dostopa pred uspešno avtentikacijo in avtorizacijo.

Beseda **MORA** označuje obveznost, **NAJ** priporočilo. Normativna osnova je IODM-001, različica 0.3. Certificiranje v tem dokumentu pomeni predlagani postopek ugotavljanja skladnosti IODM, ne akreditiranega certificiranja ali certifikacije ISO.

## 2. Postopek in dokazila

Prijavitelj predloži model, različico strojne opreme, programske opreme, konfiguracijo, profil IODM in kontakt. Laboratorij evidentira datum, izvajalca, opremo, identifikatorje vzorcev, različico testnega okolja in uporabljeno politiko zaupanja. Uporabijo se namenski testni ključi in izolirano okolje. Produkcijski zasebni ključi se ne predložijo.

Za vsak preskus se evidentirajo ID, pričakovani in dejanski rezultat, sled APDU ali drugo dokazilo, ter izid USPEH / NEUSPEH / NI IZVEDENO. Vsi obvezni preskusi morajo uspeti; neizveden obvezni preskus pomeni, da skladnost ni dokazana. Neobvezne funkcije se označijo ločeno. Odstopanja se odpravijo in ponovno preskusijo. Poročilo vsebuje obseg, omejitve, podpis odgovorne osebe in enolično oznako poročila.

## 3. Preskusno okolje

Uporabite najmanj dve neodvisni izvedbi medija različnih proizvajalcev, najmanj dva testna izdajatelja z različnima CA ter programirljiv simulator za neveljavne odgovore. Vsaj en izdajatelj naj bo prisoten na obeh platformah; preskusite tudi dva izdajatelja na isti platformi. Uporabite nadzorovan čas, testni CRL/OCSP, politiko dovoljenih poverilnic in simuliran izhod za odpiranje vrat. Izvedite 100 veljavnih transakcij na vsaki kombinaciji medija in izdajatelja.

## 4. Kontrolni seznam čitalnika

Vsi preskusi so obvezni. Register se preskuša z lokalnim testnim podpisanim registrom po IODM-005. Negativni preskusi se izvajajo v izoliranem okolju; noben ne sme povzročiti signala za odpiranje.

| ID | Postopek | Merilo uspeha |
|---|---|---|
| B-01 | Izberi aplikacijo in EF | Natančni APDU iz IODM-001 |
| B-02 | DER dolžine 127, 128, 255, 256, 4096 B (kjer izvedljivo) | Pravilno branje in omejitve; neveljaven DER zavrnjen |
| B-03 | Neveljavna ali prevelika DER dolžina | Zavrnitev pred nevarno dodelitvijo pomnilnika |
| B-04 | Veljavna veriga in svež podpis, dovoljena pravica | Odobritev dostopa |
| B-05 | 100 izzivov na kombinacijo | Brez ponovitev, dokumentiran CSPRNG |
| B-06 | Ponovi prejšnji R-APDU | Zavrnitev |
| B-07 | Spremeni RndB, r, s ali OptsA | Zavrnitev vsake spremembe |
| B-08 | r ali s = 0 oziroma >= n | Zavrnitev |

| | | |
|---|---|---|
| B-09 | Napačna dolžina, podvojen TLV, dodatni bajti | Zavrnitev |
| B-10 | Zamenjaj potrdilo, ohrani ključ odgovora | Zavrnitev pri različnem ključu |
| B-11 | Neznan CA ali napačen podpis CA | Zavrnitev |
| B-12 | Poteklo ali še neveljavno potrdilo | Zavrnitev |
| B-13 | Neveljavne omejitve CA ali KeyUsage | Zavrnitev |
| B-14 | Preklicano potrdilo | Zavrnitev |
| B-15 | Zastarel CRL/OCSP ali nedosegljiv vir | Zavrnitev, če veljavnosti ni mogoče dokazati |
| B-16 | Veljavna poverilnica brez dovoljenja SKD | Zavrnitev dostopa |
| B-17 | Enak UID, drug ključ ali brez aplikacije | Brez odobritve na osnovi UID |
| B-18 | Napačen SW, timeout, prekinitev RF | Brez odpiranja; nov poskus z novim izzivom |
| B-19 | Dodaj drugega CA s konfiguracijo | Brez spremembe kode ali ukazov |
| B-20 | Dve platformi in dva izdajatelja | Vse veljavne kombinacije uspejo brez lastniških ukazov |
| B-21 | Odstrani dovoljeni CA | Poverilnice tega CA se ne sprejemajo več |
| B-22 | Neveljaven podpis registra, napačen hash | Paket se ne aktivira |
| B-23 | Starejši manifest, iztek ali umik CA | Ni povrnitve; iztek/umik se upošteva |
| B-24 | Prekinitev posodobitve registra | Atomska aktivacija ali zadnji veljavni paket |
| B-25 | Izpad zaledja ali ponovitev njegovega odgovora | Brez nepooblaščenega odpiranja |
| B-26 | Pregled dnevnikov in konfiguracije | Brez skrivnosti, najmanjši obseg osebnih podatkov |
| B-27 | Neznana različica profila | Zavrnitev, brez prehoda na UID |
| B-28 | Dve kartici v zaporedju | Ni prenosa certifikata, izziva ali odločitve med sejama |

## 5. Merila za integracijo

Čitalnik MORA uporabljati običajni APDU vmesnik brez prepoznavanja proizvajalca za izbiro protokola. Če se preverjanje izvaja zunaj čitalnika, mora povezava zagotavljati integriteto, avtentikacijo komponent in vezavo odločitve na konkretno sejo ter vrata. Časovna politika mora biti dokumentirana. Za preskuse B-22 do B-24 se uporabi lokalni testni podpisani register po IODM-005; produkcijski podpisni ključ se ne uporablja.

## 6. Odločitev in ponovna presoja

Poročilo določa različico čitalnika, firmware, zaledje, politiko PKI, transport in vse preskušene kombinacije. Spremembe APDU, parserja, kriptografije, upravljanja zaupanja ali povezave z zaledjem zahtevajo presojo vpliva in ponovitev preskusov. Skladnost ne pomeni zaščite pred relay napadi ali potrditve fizične varnosti vrat. Produkcijsko namestitev zaupanja vrednega ključa registra je treba preveriti pred uporabo.

## 7. Dodatni preskusi profila X.509

| ID | Postopek | Merilo uspeha |
|---|---|---|
| B-29 | Manjkajoč, podvojen ali napačno kodiran subject.serialNumber | Zavrnitev |
| B-30 | Mala črka, napačna dolžina, rezerviran IID/MID | Zavrnitev |
| B-31 | Veljavna veriga, vendar IID drugega izdajatelja | Zavrnitev |
| B-32 | Manjkajoč KU, BC, SKI, AKI ali CRL DP | Zavrnitev |
| B-33 | Napačna krivulja, neveljavna točka ali algoritem | Zavrnitev |
| B-34 | Obnovljeno veljavno potrdilo istega medija | Isti IODM-ID po avtentikaciji |
| B-35 | Različna IID, isti MID | Različni identiteti v SKD |
| B-36 | Napačen podpis, a pravilen IODM-ID | Brez posredovanja preverjene identitete |
| B-37 | Podpisan register: neustrezen IID, iztek, preklic, rollback | Zavrnitev po IODM-005 |