IODM / 002

Interoperabilni dostopni medij

Ugotavljanje skladnosti dostopnih medijev

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

1. Predmet in področje uporabe

IODM-002 določa ugotavljanje skladnosti dostopnega medija. Preskuša se kartica, obesek ali druga izvedba, ki implementira IODM-001. Preskus ne potrjuje avtorizacije konkretnega uporabnika ali odpornosti na vse fizične napade.

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

Najmanj trije personalizirani vzorci iste izvedbe, vsak z drugim ključem in potrdilom, dva neodvisna čitalnika ali referenčni implementaciji različnih proizvajalcev, testni CA, zapisovalnik APDU in orodje za preverjanje ECDSA. Za vsak vzorec izvedite 100 zaporednih veljavnih transakcij na vsakem čitalniku; vse morajo uspeti v dogovorjenih laboratorijskih pogojih. Beležite čas transakcije, vendar ta izdaja ne določa splošne časovne meje.

4. Kontrolni seznam medija

Vsaka vrstica je obvezen preskus, razen če je izrecno označena drugače. Izvedite ga za vsako prijavljeno konfiguracijo.

ID	Postopek	Merilo uspeha
M-01	Aktivacija ISO 14443-4	Standardna aktivacija brez lastniških ukazov
M-02	SELECT DF z AID iz IODM-001	9000, brez zahteve po skrivnosti
M-03	SELECT EF 0101	9000; javno berljiv EF
M-04	READ BINARY: glava in kosi 1–240 B	Vsebina je enaka izvirnemu DER
M-05	Branje čez mejo datoteke	Brez razkritja drugih datotek; skladno obravnavanje meje
M-06	Preveri DER, dolžino in polnilo	En veljaven DER, le ničelno polnilo
M-07	Preveri certifikat in javni ključ	X.509, P-256, veljavna testna veriga
M-08	INTERNAL AUTHENTICATE, predpisani OptsA	86 B podatkov, 9000, veljaven podpis
M-09	100 različnih izzivov	Vsak podpis ustreza trenutnemu izzivu

M-10	Zabeleži 100 RndB na vzorec	Brez ponovitev; dokumentiran varen RNG
M-11	Preveri podpis z drugim javnim ključem	Podpis se ne potrdi
M-12	Napačen P1, neobstoječ ključ	Napaka, brez veljavnega odgovora
M-13	Manjkajoč 7C ali 81, napačna dolžina	Napaka, brez veljavnega odgovora
M-14	Poskusi zapis EF brez pravic	Zapis zavrnjen, DER nespremenjen
M-15	Pregled zaščite zasebnega ključa	Neizvozljivost in varno ustvarjanje/vnos dokumentirana
M-16	Prekinitev RF med branjem ali podpisom	Po ponovni aktivaciji pravilno delovanje
M-17	Dva neodvisna čitalnika, vsi vzorci	Enaka semantika, brez prilagoditev protokola
M-18	Pregled personalizacije in preklica	Enolični ključi, sledljivost izdaje, postopek preklica
M-19	Drugačen OptsA (če ga medij sprejme)	Podpis vključuje natančno prejeti TLV; sicer napaka
M-20	Pregled podatkov v potrdilu	Brez nepotrebnih osebnih podatkov ali skrivnosti

5. Dodatna dokazila in omejitve

Če je prisoten EF 0102, preverite zaporedje DER vmesnih CA in mejo 8192 B. Pregled M-15 vključuje dokumentacijo platforme, politiko ključa in preverjanje razpoložljivih izvoznih ukazov; funkcionalni preskus sam ne dokazuje fizične neizvozljivosti. Neponavljanje RndB ni dokaz kakovosti RNG; potreben je pregled zasnove. Preizkusi invazivnih napadov in relay niso del osnovnega profila.

6. Odločitev in ponovna presoja

Poročilo se izda za natančno določeno izvedbo medija in konfiguracijo. Sprememba platforme, kriptografske knjižnice, politike ključa, personalizacije ali protokola zahteva presojo vpliva in ponovitev prizadetih preskusov. Vpis izdajatelja v register CA je ločen postopek po IODM-004 in IODM-005. Poročilo samo po sebi ne pomeni vpisa CA ali dovoljenja dostopa.

7. Dodatni preskusi profila X.509

ID	Postopek	Merilo uspeha
M-21	ASN.1 subject DN in IODM-ID	En PrintableString 12 znakov, veljavna IID in MID
M-22	Preveri vse obvezne razširitve in OID	Natančno po IODM-001 § 4
M-23	Primerjaj javne ključe in MID vzorcev	Različni ključi in MID za različne medije

M-24	Obnovi testno potrdilo	Isti IODM-ID, nova serijska številka potrdila
M-25	Preveri izdajo proti registriranemu IID	IID ustreza CA, dokazila o izdaji obstajajo