IODM / 004

Interoperabilni dostopni medij

Zahteve za izdajatelje dostopnih medijev

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

1. Namen in normativne osnove

IODM-004 določa pogoje za potrditev izdajatelja in vpis njegovih CA v register. MORA pomeni obveznost, NAJ priporočilo, LAHKO možnost. Uporabljajo se IODM-001, 002, 005 in 006, RFC 5280 ter RFC 3647. Potrditev izdajatelja ni certifikacija posameznega izdelka niti dovoljenje za dostop.

2. Vloge in odgovornosti

Izdajatelj MORA biti pravno identificiran, določiti odgovorno osebo in varnostni kontakt, objaviti politiko CP/CPS ter navesti obseg izdaje (lastna organizacija, komercialna ali proizvodna izdaja). Zunanji personalizator deluje pod nadzorom izdajatelja. Vsak IID dodeli upravljavec IODM; isti IID ostane pri menjavi CA. Izdajatelj vodi register MID in ne sme ponovno dodeliti že uporabljenega MID drugemu mediju.

3. Profil CA

Polje	Zahteva
Format	X.509 v3, DER, RFC 5280
Javni ključ	P-256, id-ecPublicKey, imenovana krivulja
Podpis	ECDSA s SHA-256; parametri odsotni
Serial	Pozitiven, enoličen pri nadrejenem CA, največ 20 B
BasicConstraints	Kritična; CA=TRUE, pathLen=0 za neposredni izdajateljski CA
KeyUsage	Kritična; keyCertSign in cRLSign, brez drugih bitov
SKI / AKI	Nekritična; SKI obvezen, AKI obvezen pri ne-samopodpisanem CA
CRL DP	Nekritična, obvezna za ne-korenski CA, HTTPS

Korenski CA je lahko neposredni izdajatelj ali nadrejen največ enemu vmesnemu CA (pathLen največ 1). Vsak CA v poti mora pripadati istemu IID in biti registriran; sidra različnih IID se ne smejo prekrivati. Uporaba javnega spletnega CA kot samodejnega sidra ni dovoljena. Ključi CA so namenski za IODM in zaščiteni s HSM ali enakovredno dokumentirano varnostno napravo. Korenski ključ naj bo brez povezave. Veljavnost CA ne sme presegati 25 let. Podpis manifestov se izvaja z ločenim namenskim ključem.

4. Izdaja in življenjski cikel

Pred izdajo izdajatelj preveri poročilo IODM-002 za konfiguracijo, edinstvenost ključa in MID ter dokaz posedovanja. Potrdilo MORA ustrezati IODM-001 § 4; identifikator je v subject.serialNumber. Evidenca vsebuje IID, MID, serijsko številko potrdila, prstni odtis, model, čas izdaje in status. Ob izgubi, kompromitaciji ali napačni izdaji se potrdilo prekliče; CRL se izda najmanj vsakih 24 ur in ob incidentu brez nepotrebnega odlašanja, nextUpdate največ 48 ur po thisUpdate. Ob kompromitaciji CA se upravljavca registra obvesti takoj. Menjava CA zahteva predhodno potrditev novega ključa in nadzorovano prekrivanje.

5. Postopek potrditve

Prijavitelj predloži pravno identiteto, CP/CPS, potrdila CA, podpis naključnega izziva z dokazom nadzora ključa (lahko nadzorovana ceremonija), preskusna poročila, CRL in opis zaščite ključev. Upravljavec preveri dokazila, zabeleži odločitev in obdobje potrditve (največ

eno leto), objavi potrjene vpise po IODM-005. Ob bistveni spremembi je potrebna ponovna presoja; ob incidentu se vpis lahko začasno ustavi ali umakne. Zasebnih ključev se nikoli ne predloži.

6. Kontrolni seznam

ID	Preverjanje	Merilo
ISS-01	Pravna identiteta in kontakt	Preverljiva
ISS-02	CP/CPS in odgovornosti	Dokumentirane
ISS-03	Dokaz nadzora CA	Veljaven
ISS-04	Profil CA	§ 3 izpolnjen
ISS-05	Zaščita ključev	Dokazila HSM ali enakovredno
ISS-06	Poročila medijev	IODM-002, vse konfiguracije
ISS-07	IODM-ID in evidenca	Enolična dodelitev
ISS-08	CRL in incident	Preskus preklica uspe
ISS-09	Menjava CA	Dokumentiran načrt
ISS-10	Podpis manifesta	Ločen ključ, pooblastilo

Vse obvezne točke morajo uspeti; poročilo vključuje dokazila, datum, obseg in podpis odgovorne osebe.