Cerfikattjänster / Kuusela Minna (MDB)

26.1.2026

Ändringar i MDB:s servicecertifikat år 2026

Kommande ändringar

26.1.2026

Innehållsförteckning

Ändringar i MDB:s servicecertifikat år 2026

Det kommer att ske flera betydande förändringar i servicecertifikaten år 2026, varav vissa kräver åtgärder från våra kunder. Vi rekommenderar att våra kunder bekantar sig med förändringarna i god tid och testar hur förändringarna påverkar deras egna miljöer genom att beställa testservercertifikat för detta ändamål.

1 Ändringar i servercertifikat år 2026

År 2026 medför flera förändringar för servercertifikat.

Alla ändringar som listas nedan kommer att genomföras under året 2026. I ACME har alla ändringar genomförts direkt från och med införandet:

- CN-fältet tas bort och ersätts av fältet SubjectAltName (SAN=DNS).
- Servercertifikat innehåller inte längre både Client auth och Server auth EKU. Under 2026 kommer DVV att differentiera de nuvarande servercertifikaten till två olika produkter: servercertifikat (Server Auth) och kundcertifikat (Client Auth).
- Fältet SerialNumber (OID 2.5.4.5) ersätts av fältet OrganizationIdentifier (OID 2.5.4.97).
- Basic Constraints CA: False tas ur bruk.
- Meddelandetexten (User Notice Explicit Text) i certifikatets Certifikatpolicyfält är inaktiverad: Notice text= Certifikatpolitika is available - Certifikatpoli-cy finns - Certifikatpolicy är tillgänglig http://www.fineid.fi/cps52.
- Expired Certs On CRL-tillägget läggs till blocklistfilen: för produktion den 14.1.2026, på testsidan har detta redan implementerats. Detta kommer bara att orsaka kompatibilitetsproblem för kunder om kunden använder en mycket anpassad CRL-implementering.

Giltighetstiden för servercertifikat reduceras:

- Från 15.3.2026 är den maximala giltighetstiden 6 månader
- Från 15.3.2027 är den maximala giltighetstiden 3 månader
- Från 15 mars 2029 kan servercertifikat endast vara giltiga i 47 dagar.

Vi rekommenderar ACME för våra kunder. MDB kommer att lansera ACME uppskattningsvis i mars 2026.

Några av våra kunder kan byta servercertifikatet till systemsignaturcertifikat vars giltighetstid är 24 månader.
Här är en sammanfattning av ändringarna i servicecertifikatprodukterna:

Servercertifikat (servercertifikat, servercertifikat för social- och hälsovården, servercertifikat för hälsoapplikationer, KaPa-autentiseringscertifikat): giltighetstiden förkortas, Client Auth tas bort, Basic Constraints CA inaktiveras. CN-fältet tas också bort och SerialNumber ersätts av fältet OrganizationIdentifier. Kunden kan byta till ACME.

Systemsignsturcertifikat, (BDS-gränssnitt) kundcertifikat: giltighetsperioden förblir oförändrad, inga ändringar. Kunden kan använda ACME om certifikatet innehåller ett domännamn.

KaPa-certifikat: betydande förändringar väntas för kunder. Det kommer detaljerade instruktioner separat senare.

E-postcertifikat: inga ändringar.

2 Nya produkter och ändringar på nuvarande produkter

På kommande 1.3.2026:

Kundcertifikat. Kundcertifikatet ersätter VTJ-gränssnittets kundcertifikat som tidigare endast var avsett för VTJ-användning. Det nya kundcertifikatet är tillgängligt för alla våra kunder. Om du redan nu behöver ett klientautentiseringscertifikat (Client auth) kan du beställa VTJ-gränssnittets kundcertifikat. Certifikatets tekniska specifikationer är identiska.

Omkring mars 2026 lanserar MDB ACME-protokollet. Läs mer om ämnet här: dvv.fi/sv/acme-sv.

3 Så här beställer du testservercertifikat

Vi rekommenderar att om det finns minsta misstanke om att de kommande förändringarna påverkar er verksamhetsmiljö och ni använder MDB:s servercertifikat (servercertifikat, KaPa autentiseringscertifikat, välfärdsapplikationscertifikat), att ni beställer testservercertifikat som redan har alla kommande ändringar inkluderade.

Gör beställningen som tidigare, men i fältet OU på certifikatbegäran (CSR) skrivs texten "Nytt 2026-certifikatsprofil". På så sätt kan vi på MDB skilja dessa testcertifikat från andra testcertifikat redan i beställningsfasen. Själva producerade testservercertifikatet kommer inte att innehålla något OU-fält.

Observera att även följande ändringar av Key Usage har genomförts i dessa testservercertifikat. För dessa ändringar har inga slutgiltiga beslut eller tidsplaner fastställts för produktionen, så de finns ännu inte med i den faktiska ändringslistan. Dessa KU har dock redan tagits bort från testservercertifikaten: i RSA-certifikat Key Encipherment och Data Encipherment, i ECC-certifikat Key Agreement.

4 Förberedelser inför kvantdatorerna

- Termerna PQC och PQ Cryptography (Post-Quantum Cryptography) och QSC (Quantum-Safe Cryptography) syftar på kvantsäkra, det vill säga kvantdatorresistenta kryptografiska algoritmer, det vill säga krypteringsmetoder.
- Algoritmerna RSA och ECC (ECDH/ECDSA), som för närvarande används mycket i krypteringssystem för publika nyckel, har en matematisk grund som en tillräckligt utvecklad kvantdator skulle kunna bryta på kort tid med Shors algoritm.

Schemakrav:

EU-kommissionen: "Skyddet av kritisk infrastruktur bör övergå till PQC så snart som möjligt, senast i slutet av 2030."

Traficom: "Den nationella kryptoarbetsgruppen rekommenderar att den nationella PQC-övergången genomförs i enlighet med de tidtabeller som presenteras av EU:

- *Högrisksystem bör göras kvantsäkra till 2030..*
- Alla offentliga nyckelmetoder bör vara kvantsäkra senast 2035.”

Checklista som vi rekommenderar alla våra kunder att gå igenom:

1. Se till att din organisation är medveten om den kommande PQC-övergången.

2. Skapa en kryptoinventering: skriv ner vilka kryptografiska algoritmer som används i din organisation och för vilka funktioner de används.

1. Mekaniska TLS- och SFTP-gränssnitt mot olika informationssystem eller intressenter.

2. Webbservrar (HTTPS/TLS) mot slutanvändaren.

3. Signerade/autentiserade meddelandegränssnitt, t.ex. SAML eller OIDC.

4. Signerade tokens, t.ex. JWT.

5. Certifikatkortsinloggning (mTLS).

6. Elektroniska signaturer.

7. Kryptering av databaser, säkerhetskopior etc. datareserver.

3. Sträva efter att främja kryptoagilitet i utvecklingsarbetet.

"Förmågan att snabbt anpassa kryptografiska system enligt nya hot eller standarder.” –VTT