

Fokozott biztonságú elektronikus aláírás (AES): megfelelőségi lap

Az aláírás szintje, a bizonyítékok megőrzése és a tárhely

Frissítve: 2026. október 12.

Az aláírás szintje

Fokozott biztonságú elektronikus aláírás a 910/2014/EU rendelet (eIDAS) 26. cikke értelmében. Az alábbi négy követelményen alapul.

- 1 Egyértelműen az aláíróhoz kötött: az aláíró böngészőjében személyes kulcspár jön létre, és az adott aláíráshoz tartozó tanúsítvány kerül kiállításra.
- 2 Az aláíró azonosítása: e-mailben küldött személyes aláírási hivatkozás, majd SMS-ben a mobiljára küldött egyszer használatos kód. Két külön csatorna.
- 3 Az aláíró kizárólagos ellenőrzése alatt áll: a privát kulcs nem exportálható, és soha nem hagyja el az aláíró böngészőjét.
- 4 Minden későbbi módosítás kimutatható: a dokumentum tartalmát aláírt SHA-256 ujjlenyomat és RFC 3161 időbélyeg pecsételi le.

Átadott bizonyítékok

Minden aláírt dokumentumhoz bizonyítéki tanúsítvány tartozik: időbélyeggel ellátott események (megnyitás, kapott kód, aláírás), IP-cím, a tanúsítvány száma és a dokumentum ujjlenyomata.

Megőrzés

Az aláírt dokumentumokat és az auditnaplókat 10 évig őrizzük, a választott csomagtól függetlenül.

Csak a teszt kulccsal (sandbox) létrehozott adatok törlődnek 30 nap után.

Tárhely és adatvédelem

Az alkalmazás, az adatbázis és a dokumentumtár saját infrastruktúránkon fut az Európai Unión belül (IONOS tárhelyszolgáltató). TLS 1.3 átvitel közben és AES-256 tárolás közben. A GDPR szerinti adatfeldolgozási megállapodás (DPA) online aláírható az ügyfélfiókból.

Jó tudni

A minősített aláírás (QES) aláírásonként érhető el egy partner minősített bizalmi szolgáltatón keresztül; ez a lap csak a fokozott biztonságú szintet írja le.

ISO 27001 tanúsítás: a tanúsítási audit folyamatban van, a tanúsítvány még nincs meg.