MICROSEC

eSign Day 2025
Aláírás ellenőrzés a 32. cikk szerint

2025/06/30

32. cikk szerinti aláírás ellenőrzés

- Miért van a fogalomra szükség?
  - A 32. cikk (3) bekezdése szerint a bizottsági végrehajtásiban hivatkozott szabványnak megfelelés esetén **feltételezett/presumed** az ennek a cikknek megfelelés.
  - Ez azt jelenti, hogy létezhetnek alternatív ellenőrzési módok, továbbra sem lesz egységes ellenőrzés.
  - Elkezdődött a szabványok és rendeletek felvizezése tagállami érdekek mentén:
    - RSA 2048 3 éves hosszabbítása,
    - Aláírás ellenőrzés végrehajtási tervezet az eIDAS rendelettel ellentétes tartalma,
    - Akkreditációról szóló végrehajtásiban tagállami jogkör szabályozása.

32. cikk szerinti aláírás ellenőrzés

- Miért jó a 32. cikk?
  - Ez a cikk egyszerűen megállapítja, hogy az aláírás érvényességét, ha megfelel az ebben megtalálható 8 jogi követelménynek.
    Ez egyértelmű és mindenkire vonatkozik.

    Egy-egy követelmény behivatkozza a 26. cikk és az 1. melléklet követelményeit, így ha ezeknek megfelelünk, akkor a minősített aláírásunk megfelelő.

Vonatkozó jogszabályok 1.

32. cikk
A minősített elektronikus aláírás érvényesítésére vonatkozó követelmények
(1) A minősített elektronikus aláírás érvényesítésére szolgáló eljárás megállapítja a minősített elektronikus aláírás érvényességét, amennyiben:
a) az aláírást igazoló tanúsítvány az aláírás időpontjában elektronikus aláírás olyan minősített tanúsítványa volt, amely megfelel az I. mellékletnek;
b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;
c) az aláírás-érvényesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;
d) a szolgáltatást igénybe vevő fél pontosan megkapja a tanúsítványban az aláírót azonosító egyedi adatokat;
e) amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;
f) az elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állították elő;
g) az aláírt adatok sértetlensége nem került veszélybe;
h) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények;

26. cikk
A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények
A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:
a) kizárólag az aláíróhoz köthető;
b) alkalmas az aláíró azonosítására;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Vonatkozó jogszabályok 2.

I. MELLÉKLET
AZ ELEKTRONIKUS ALÁÍRÁSOK MINŐSÍTETT TANÚSÍTVÁNYAIRA VONATKOZÓ KÖVETELMÉNYEK

Az elektronikus aláírások minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint — jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot, — természetes személy esetében a személy nevét;

c) legalább az aláíró neve vagy pedig egy álnév;. álnév használata esetén ezt egyértelműen jelezni kell;

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) információ a minősített tanúsítvány érvényességi állapotáról, vagy azoknak a szolgáltatásoknak a helye, amelyek segítségével arról felvilágosítás kérhető;

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában.

32. Cikk teljesülése – 1. adag követelmény

32. Cikk - A minősített elektronikus aláírás érvényesítésére vonatkozó követelmények	
(1) A minősített elektronikus aláírás érvényesítésére szolgáló eljárás megállapítja a minősített elektronikus aláírás érvényességét, amennyiben:	
a) az aláírást igazoló tanúsítvány az aláírás időpontjában elektronikus aláírás olyan minősített tanúsítványa volt, amely megfelel az I. mellékletnek;	Az **új** ETSI 319 412-2-nek megfelelő profilú tanúsítvány megfelel az 1 mellékletnek.
b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;	**Lásd később részletesen…**
c) az aláírás-érvényesítési adatok megfelelnek a szolgáltatást igénybe vevő fél számára megadott adatoknak;	Ha az aláírás nem sérült, teljesül.
d) a szolgáltatást igénybe vevő fél pontosan megkapja a tanúsítványban az aláírót azonosító egyedi adatokat;	Ez szabványos konténereket használva (XADES, PADES, CADES, ASIC) teljesül, mert a tanúsítvány átadásra kerül.
e) amennyiben az aláírás időpontjában álnév használatára került sor, az álnév használatának tényét egyértelműen feltüntették a szolgáltatást igénybe vevő fél számára;	Álneves tanúsítvány esetén az álnév pseudonym mezőbe foglalása ezt egyértelműen jelzi.
f) az elektronikus aláírást minősített elektronikus aláírást létrehozó eszközzel állították elő;	A tanúsítvány qcStatement mezője tartalmazza az SSCD statementet, akkor ez teljesül.
g) az aláírt adatok sértetlensége nem került veszélybe;	Ha az aláírás nem sérült, teljesül.
h) az aláírás időpontjában teljesültek a 26. cikkben foglalt követelmények;	PADES, XADES, CADES, ASIC konténer formátumú és 2015/1506 bizottsági végrehajtási határozata alapján megfelel a 26. cikkben foglalt követelmények, így ha ilyet használunk, akkor azt nem kell tovább vizsgálni.

32. Cikk b) teljesülése

b) a minősített tanúsítványt minősített bizalmi szolgáltató bocsátotta ki, és az az aláírás időpontjában érvényes volt;	
Minősített bizalmi szolgáltató bocsátotta ki	A minősített tanúsítványkiadó ellenőrzése az **EU bizalmi listán** úgy kell történjen, hogy az aláírás ellenőrzése során meg kell győződni arról, hogy a kibocsátó bizalmi szolgáltató tanúsítványa az aláíró tanúsítvány kibocsátásakor a bizalmi listán **„granted”** bejegyzéssel szerepelt, továbbá az aláírás időpontjában az nem „withdrawn” állapotú.
az aláírás időpontjában érvényes volt - lejárati idején belül van	A tanúsítványnak **a lejárati idején belül kell lennie.**
az aláírás időpontjában érvényes volt - nem volt visszavonva	Az aláírás időpontját követően kiadott OCSP vagy CRL válasz szerint a tanúsítvány nincs visszavonva. Az aláírás időpontja utáni CRL vagy OCSP válasz azért szükséges, mert az aláírás előtti CRL vagy OCSP válasz még **nem tartalmazhat** információt a tanúsítvány visszavonásáról/felfüggesztéséről adott időpontban, azt csak az aláírást követően kibocsátott visszavonási információ biztosíthatja. (Azaz az ETSI TS 119 172-4 szabvány szerinti RevocationFreshnessConstraints maximum értéke tehát 0 lehet csak.)
az aláírás időpontjában érvényes volt – a visszavonási információ elfogadhatóságának ellenőrzése	Amennyiben a visszavonási információ **nem tartalmazza az ArchiveCutoff (OCSP) vagy ExpiredCertsOnCRL (CRL) kiterjesztést,** akkor **azt csak a tanúsítvány érvényességi ideje alatt fogadhatjuk el.** **eIDAS 24. cikk (4) alapján kötelező az ArchiveCutoff (OCSP) vagy ExpiredCertsOnCRL (CRL) kiterjesztés.**
az aláírás időpontjában érvényes volt – a tanúsítvány nem rendelkezik releváns korlátozással	**Lásd még később részletesen…**

Visszavonás ellenőrzés – Az egyes szintek és ellenőrizhetőségük

Szint	Szint tartalma	Magyarázat	Tartós megőr-zésre alkalmas?	Kiegészítő információ beszerzése szükséges az ellenőrzéshez?	Az aláírás érvényesség megállapíthatósága
B	csak aláírás	Mivel ezen szint esetén sem időbélyeg, sem visszavonási információ nem szerepel az aláírásban, ezért az aláírás érvényessége alaphelyzetben nem állapítható meg.	Nem	Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az aláíró tanúsítvány (és annak lánca) érvényességi idején belül.
T	aláírás időbélyeggel	Mivel az időbélyeg ezen szinten hiteles információt ad az aláírás időpontjáról, ezért az aláírás érvényessége az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül állapítható meg.		Igen, CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** Nem megállapítható. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül. (Az időbélyegző tanúsítvány jellemzően sokkal tovább érvényes, mint az aláíró.)
LT	aláírás időbélyeggel és azt követően csatolt visszavonási információval	Mivel a csatolt visszavonási információt nem védi időbélyeg (azaz kvázi B szinten aláírt információként kerül csatolásra) ezért annak maximum elfogadási ideje a B aláírás szint alapján állapítandó meg.		Nem. Amennyiben a CRL vagy OCSP válasz érvényessége lejárt, új CRL vagy OCSP válasz beszerzése szükséges.	**Önállóan:** A visszavonási információ (és annak lánca) érvényességi idején belül. **Beszerzett kiegészítő információkkal:** Az időbélyegző tanúsítvány (és annak lánca) és a visszavonási információ (és annak lánca) érvényességi idején belül.
LTA	aláírás időbélyeggel és visszavonási információval, majd archív időbélyeg	Az archív időbélyeg az összes alatta található tartalmat védi, így azok érvényessége egészen addig megállapítható, amíg a legkülső archív időbélyeg (és annak lánca) érvényességi idején belül történik az ellenőrzés.	Igen	Nem.	Az archív időbélyegző tanúsítvány (és annak lánca) érvényességi idején belül.

Korlátozások vizsgálata

korlátozás	
privateKeyUsagePeriod	A kulcs használatának korlátozására használható a PrivateKeyUsagePeriod kiterjesztés. Ez aláíró tanúsítványok esetén nem szerepel, de időbélyegző tanúsítványok esetén szerepelhet. Amennyiben ezt a kiterjesztést tartalmazza egy tanúsítvány, akkor **hozzá tartozó kulccsal végzett aláírás csak akkor fogadható el, ha az aláírás időpontja a PrivateKeyUsagePeriod kiterjesztésbe foglalt időtartamon belül készült.** Ez időbélyegzők esetében azt jelenti, hogy az időbélyeg akkor érvényes, ha ezen időtartamon belül készült.
certificatePolicies:userNotice:Explicit text	A tanúsítvány használatára vonatkozó egyedi korlátozások jellemzően szövegszerű korlátozások, amelynek beírására helyet a certificatePolicies:userNotice:Explicit text mező biztosít. Amennyiben ez a mező megtalálható a tanúsítványban, akkor az ellenőrzés során az **RFC 5280 4.2.1.4 fejezete alapján meg kell jeleníteni a felhasználó számára**, és jelezni, hogy az aláírás csak akkor fogadható el, ha fenti mező nem tartalmaz korlátozást az elfogadhatóságra. **A 13. cikk (3) ebben a kérdésben további szabályozási lehetőséget biztosít a tagállamok számára.** Ez Magyarország esetében tiltó rendelkezést tartalmaz, **a Dáptv. 101. § (2) értelmében, az aláíró is kötelezett a korlátozások betartására.**

Érdekességek

- az ETSI EN 319412-2 4.2.4 fejezet előírja az ország (C) feltüntetését, habár kötelezősége nem vezethető le az eIDAS-ból (nincs az 1. mellékletben)
- az Adobe Reader helytelenül ellenőriz
- Subject:serialNumber, a 26. cikk 1. (a) és (b) implicit követelménye
- a 28. cikk 2. paragrafus tiltja a tanúsítványra vonatkozó további kötelező tartalom előírását, mint amit az 1. melléklet előír, így a tagállami tanúsítvány érvényességére vonatkozó előírások ellentmondásban vannak az eIDAS-szal

MICROSEC

Kérdések, hozzászólások

Kapcsolat

Contact

VARGA VIKTOR
PKI ARCHITECT & TRUST SERVICE MANAGER

Microsec zrt. | 1033 Budapest, Ángel Sanz Briz út 13.
varga.viktor@microsec.hu
microsec.hu