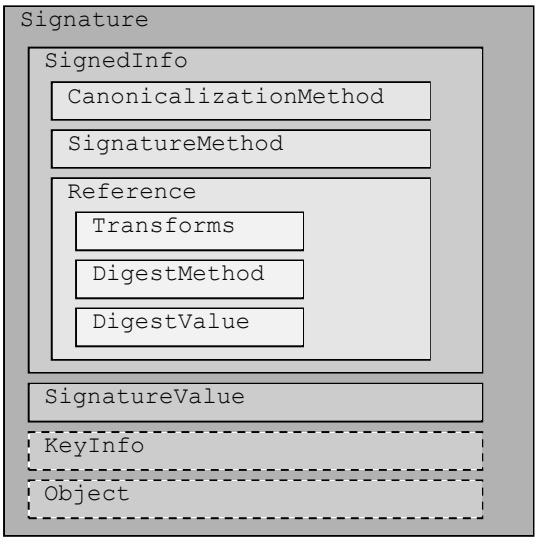
# MIRE JÓ AZ ARCHÍV ALÁÍRÁS?[1]

***Endrődi Csilla <csilla@microsec.hu>***
***Dr. Berta István Zsolt <istvan.berta@microsec.hu>***
***MICROSEC Kft.***

## 1. ELEKTRONIKUS ALÁÍRÁS EGYSÉGES FORMÁTUMA

Jelenleg úgy tűnik, hogy az RFC 3275 [RFC3275] által meghatározott *XML formátumú elektronikus aláírás* használata terjed el leginkább. Az ajánlás a következő struktúrát határozza meg:




Az aláírás gyökéreleme a `Signature` elem (ami bárhol lehet egy XML állományban). Ezen belül két kötelező (`SignedInfo` és `SignatureMethod`) és két opcionális (`KeyInfo` és `Object`) elem található. Aláírás készítésekor tulajdonképpen a `SignedInfo` elem tartalma kerül aláírása, a kiszámított aláírási értéket a `SignatureValue` elem tartalmazza. Az aláírni kívánt dokumentumra (vagy dokumentumokra) illetve egyéb aláírandó adatokra mutató referenciát és azok lenyomatát (illetve az ezek elkészítése során alkalmazott algoritmusok azonosítóját) a `Reference` elem tartalmazza (azaz az aláírói dokumentum kétszeres indirekcióval kerül aláírásra). A `KeyInfo` a használt tanúsítványt tartalmazza, míg az `Object` pedig tartalmát az ajánlás „nyitva hagyja".

Erre az ajánlásra építve került kidolgozásra az *XML formátumú fokozott biztonságú aláírásokkal* kapcsolatos követelményrendszer (XML Advanced Electronic Signature, XAdES), amelyet az ETSI TS 101 903 ajánlás tartalmaz [XAdES]. Ez meghatározza az aláíráshoz illetve aláírt dokumentumhoz kapcsolódó, az aláíráshoz csatolandó adatokat körét és ezek XML struktúráját, amelyeket az RFC 3275-ben definiált `Object` elemben helyez el a következőképpen:

A `QualifyingProperties` gyökérelem két nagy „konténert" tartalmaz: az aláírt adatokat tartalmazó `SignedProperties` elemet, és az aláírásra nem kerülő adatokat tartalmazó `UnsignedProperties` elemet. Utóbbiba az olyan adatelemek kerülnek, amelyek hitelességét valamely más aláírás védi (pl. időbélyegek, tanúsítványok, visszavonási információk). Az aláírt adatok is két részre oszlanak, a `SignedSignatureProperties` az aláírással kapcsolatos adatokat tartalmazza (pl. aláírás ideje, helye, aláírási szabályzat azonosítója), míg a `SignedDataObjectProperties` elem a dokumentumra vonatkozó információkat tartalmaz (pl. dokumentum formátuma, kötelezettségvállalás típusa).


A XAdES ajánlás meghatároz *nyolc egymásra épülő aláírási formát* is (XAdES-BES, -EPES, -T, -C, -X Type1, Type2, -X-L, -A), amelyek egyre több, az aláíráshoz kapcsolódó adatot tartalmaznak.

[1] Ez a cikk az alábbi konferencián jelent meg: Networkshop'2007, Eger, 2007. április 11-13.

Magyarországon a közigazgatásban alkalmazható elektronikus aláírás formátumokról szóló IHM ajánlás [IHM-AF] négy különböző aláírás formát definiál (*pillanatnyi, rövid távú, hosszú távú, archív*), amelyek mind megfelelnek valamely XAdES formának. Jelen cikkünkben az IHM ajánlás által definiált archív aláírást nevezzük *archív aláírásnak*, amely a XAdES ajánlás XAdES-A típusú aláírásának egy tovább specifikált változata.

## 2. KÜLÖNBÖZŐ ALÁÍRÁS FORMÁK

### 2.1. Alap aláírás: XADES-BES, -EPES

Az elektronikus aláírás elkészítése *alapszinten* az aláírandó dokumentum lenyomatképzését, majd a lenyomaton a titkos kulccsal való kriptográfiai művelet elvégzését jelenti[2], az így előálló értéket nevezzük szoros értelemben aláírásnak (vagy aláírási értékének). Az ellenőrzés során ennek megfelelően újból el kell készíteni az ellenőrzendő dokumentum *lenyomatát*, majd az aláírás értékén el kell végezni a *kriptográfiai művelet ellentettjét* az aláíró fél nyilvános kulcsának felhasználásával, és ezt *összehasonlítani* az újonnan képzett lenyomati értékkel. A kettő egyezése jelenti – szűk értelemben véve – az aláírás érvényességét.

Látható, hogy már a fenti folyamat elvégezhetőségéhez is szükség van pár információra, amelyeket ezért mindenképpen csatolni szükséges az aláíráshoz. Ismernünk kell az aláírás során használt *nyilvános kulcsot,* és az aláíró *tanúsítványát* (ez köti össze hitelt érdemlő módon a használt nyilvános kulcsot az aláíró nevével). Tudnunk kell, hogy mely *aláíró algoritmus* került alkalmazásra, valamint az aláírás elkészítése során alkalmazott *lenyomatkészítő* illetve *kanonizációs*[3] *algoritmusokat* is ismernünk kell. Ezen kívül, amennyiben az aláírás valamelyik *aláírási szabályzat* szerint került létrehozásra, akkor ennek azonosítójára is szükségünk van.
Ezeken kívül segíti az aláírt dokumentum értelmezését, ezért opcionálisan szerepeltethető az aláírt adatok között az aláíró által állított *hely*, *dátum*, *kötelezettségvállalás típusa*, *aláírói szerepkör* és a *dokumentum formátuma*.
A felsorolt adatokat[4] az aláíró a dokumentum aláírásával egyidejűleg, azzal egy lépésben aláírja, ezáltal biztosítva azok hitelességét is (az adatok a `SignedProperties` elembe kerülnek, ami meghivatkozásra kerül a `SignedInfo` egyik `Reference` eleme által).

A fenti adatokat tartalmazó aláírást a XAdES ajánlás *XAdES-BES-nek* (Basic Electronic Signature), ha tartalmazza az aláírási szabályzat azonosítóját, akkor *XAdES-EPES-nek* (Explicit Policy based Electronic Signature) nevezi.
Az IHM ajánlás szerinti *pillanatnyi aláírás* egy olyan XAdES-EPES aláírás, amely kötelezően tartalmazza az *aláírás időpontját* és a *dokumentum formátumát* (MIME típus) is. Alkalmazása az ajánlás szerint olyan esetekben javasolt, amikor az aláírás élettartama rövidebb az aláírást követő első visszavonási állapot információ kiadásánál[5].

### 2.2. Időbélyeget tartalmazó aláírás: XAdES-T

Ismeretes, hogy az aláírói tanúsítványok lejárhatnak, illetve visszavonhatják, felfüggeszthetik és visszaállíthatják őket, azaz állapotuk az időben változik. Az elektronikus aláírás érvényességének azonban feltétele, hogy az aláíró (aláíráskor használt) tanúsítványa *az aláírás létrehozásakor* érvényes legyen. Ennek ellenőrzéséhez nyilvánvalóan szükséges ismernünk az aláírás létrehozásának időpontját. Ezt nem rögzíthet maga az aláíró vagy az ő befolyása alatt álló program (hiszen tipikusan egy rossz szándékú fél a titkos kulcs ellopása – és a tulajdonos általi visszavonása – után egy, a visszavonás előtti időpontot tenne az aláírásba), hanem egy megbízható harmadik féltől, egy *Időbélyegzés szolgáltatótól* származó időbélyegre van szükség. Az *időbélyeg* nem más,

[2] Ennek matematikai illetve kriptográfiai hátterére jelen munkában nem térünk ki.
[3] Az XML szöveg egyértelmű formára hozására szolgáló algoritmus.
[4] A tanúsítvány értékén kívül, annak csak a lenyomati értékét írja alá az aláíró, az alapján azonosítható a tanúsítvány.
[5] Megjegyezzük, hogy ez a megfogalmazás értelmezhetetlen OCSP-s visszavonási információ használata esetében (lásd később), hiszen ilyenkor a visszavonási információ mindig aktuálisan rendelkezésre áll illetve beszerezhető.

mint az aláírás és az Időbélyegzés szolgáltató által biztosított hiteles időpont összekapcsolása az Időbélyegzés szolgáltató aláírásával.

Amennyiben egy aláírás *nem tartalmaz* ilyen időbélyeget, akkor a létrehozás időpontját *ismeretlennek* kell tekintenünk. Az általánosan elterjedt gyakorlat szerint ilyenkor feltételezzük, hogy amennyiben a tanúsítvány az ellenőrzés időpontjában érvényes, akkor érvényes volt az aláírás létrehozásakor is[6]. Viszont ha a tanúsítvány az ellenőrzés időpontjában nem érvényes (pl. lejárt), akkor az aláírást mindenképpen érvénytelennek kell tekinteni. Ez egyben azt is jelenti, hogy *az időbélyeget nem tartalmazó aláírás legkésőbb a tanúsítvány lejártakor érvényét veszti*. Egy végfelhasználói aláíró tanúsítványt jellemzően egy vagy két évre bocsátanak ki.

A XAdES ajánlás az olyan aláírásokat, amelyet a XAdES-BES által tartalmazott elemeken kívül tartalmazzák az aláírás értékéhez készített időbélyeget, *XAdES-T-nek* (XML Advanced Electronic Signature with Time) nevezi.
Az IHM ajánlás szerinti *rövid távú aláírás* egy XAdES-T-nek megfelelő aláírás. Az ajánlás szerint alkalmazása akkor javasolt, ha az aláírás ellenőrzése nem szükséges az aláíró tanúsítványának lejárta után[7].

### 2.3. Érvényesítési adat referenciát tartalmazó aláírás: XAdES-C

A következő problémát az okozhatja, hogy az aláírás ellenőrzéséhez szükséges tanúsítványok és visszavonási információk az eredeti helyen megváltozhatnak, elérhetetlenné válhatnak. Ezért szükséges legalább a *tanúsítványok* és *visszavonási információk* elérési helyét és lenyomati értékét hozzácsatolni az aláíráshoz, lehetőség szerint pedig érdemes magukat a tanúsítványokat és visszavonási információkat is beletenni az aláírásba[8].
Az ilyen aláírásokat a XAdES ajánlás *XAdES-C-nek* (XML Advanced Electronic Signature with Complete validation data references) nevezi.

Az IHM ajánlás szerinti *hosszú távú aláírás* egy olyan XAdES-C aláírás, amely kötelezően tartalmazza a tanúsítványok és visszavonási információk értékét is[9]. Az ajánlás szerint alkalmazás akkor javasolt, ha az aláírás ellenőrzése szükséges a tanúsítványlánc bármely elemének a lejárta után is.

Itt azonban felmerül egy további probléma, nevezetesen, hogy a CRL-es visszavonási információ használata esetében (részletesen lásd később) a CRL-ek szakaszos kibocsátása miatt az aláírásnál használt tanúsítvány aláíráskori állapotáról információt adó CRL csak később válik elérhetővé. Ez egyben azt is jelenti, hogy CRL-es visszavonási információ használata esetében XAdES-C aláírás nem készíthető el egyetlen lépésben. Ilyenkor azt lehet tenni, hogy az aláíró elkészít egy XAdES-T aláírást, majd a releváns CRL megjelenése után kibővíti azt XAdES-C aláírássá. Ez azonban a gyakorlati alkalmazást jelentősen megbonyolítja.

### 2.4. További időbélyeggel bővített aláírás: XAdES-X Type1, Type2

Maguk a tanúsítványok és a visszavonási információk (CRL-ek és OCSP válaszok) is tartalmaznak aláírást – amelyet a megfelelő szolgáltató készített –, amelyek szintén ellenőrzendők. Tekintve, hogy a szolgáltatók tanúsítványa is lejárhat illetve visszavonhatják őket, itt is meg kell vizsgálni,

---

[6] Ez akkor nem igaz, ha az aláíráskor a tanúsítvány még nem volt érvényes vagy éppen fel volt függesztve, de később visszaállították (lásd később).

[7] Megjegyezzük, hogy a fentebbi magyarázat szerint egy időbélyeget tartalmazó aláírás érvényes marad a tanúsítvány lejárta után is. Az IHM ajánlás nagy valószínűséggel azért nem tartja elfogadhatónak az időbélyeget tartalmazó aláírások hosszabb távú elfogadását, mert attól tartanak – egyébként megalapozottan, lásd később – hogy a tanúsítvány lejárta után a visszavonási információk már nem biztos, hogy beszerezhetőek.

[8] Az ajánlás nem teszi kötelezővé, hogy a tanúsítvány és visszavonási értékek belekerüljenek az aláírásokba, hiszen ezek érdemben megnövelik az aláírás méretét, és sok „hasonló” aláírás esetében javarészt ugyanazok az értékek kerülnének be mindenhova. Ezért hatékonysági okokból célszerű lehet ezeket egy helyen eltárolni és erre a helyre hivatkozni az aláírásokban. Ez természetesen csak valamilyen szempontból központosított rendszerben (pl. adott szervezeten belül) működő megoldás, teljesen elosztott rendszer esetében az említett adatokat csatolni érdemes az aláíráshoz.

[9] Az ilyen aláírásoknál az aláírás ellenőrzéséhez szükséges adatok biztosan rendelkezésre állnak (még akkor is, ha az eredeti helyen már nem találhatóak meg), így az ellenőrzés gyorsabban és Internet kapcsolat nélkül (pl. zárt hálózaton) is elvégezhető.

hogy az adott szolgáltató tanúsítványa érvényes volt-e az adott adategység kibocsátásakor. Ehhez a korábban elmondottaknak megfelelően szükség van az adott adategység (tanúsítvány, CRL, OCSP) felhasználásának időpontjára[10], amelyet egy újabb időbélyeg elhelyezésével tudunk biztosítani.
Ennek céljából vezette be a XAdES ajánlás a *XAdES-X* aláírást (eXtended signature with time form), amelynek két különböző típusa van. A *Type1* esetében a csatolt időbélyeg az aláírás értékét, az aláíráson levő időbélyeget, a tanúsítványok referenciáját és a visszavonási információk referenciáját írja alá, míg *Type2* esetében csak az utóbbi két adategységet.

### 2.5. További időbélyeggel bővített, hosszú távú aláírás: XAdES-X-L

A *XAdES-X-L* (eXtended Long electronic signature with time) az előbbi forma bővítése olyan módon, hogy ebben nem csak a tanúsítványok illetve visszavonási információk referenciáinak, hanem maguknak az értékeknek is szerepelnie kell – amelyek a XAdES-C-nél már opcionálisan megjelentek –, az időbélyeggel ellátott referenciáknak az XML állományon belülre kell mutatnia[11].

### 2.6. Archív aláírás: XAdES-A

További problémát vet fel, hogy természetesen az Időbélyegzés szolgáltatónak is lejár valamikor a tanúsítványa, illetve ennek kulcsa is visszavonásra kerülhet. Az Időbélyegzés szolgáltató által kibocsátott időbélyegeket a szolgáltató aláírása hitelesíti, amely létrehozásának időpontjáról kizárólag magától az Időbélyegzés szolgáltatótól van információnk (ő rögzíti az időpontot). Amennyiben az ellenőrzéskor érvényes az Időbélyegzés szolgáltató tanúsítványa, akkor elfogadottnak tekintjük az időbélyeg aláírását[12], azonban *a tanúsítvány lejárta vagy visszavonása után* – a fentebb tárgyalthoz hasonlóan – ezen aláírások (és így az időbélyegek) *érvényessége nem bizonyítható*. Ez a helyzet szintén a már ismertetetthez hasonló módszerrel előzhető meg: még a tanúsítvány érvényességének ideje alatt újabb, egy másik (hosszabb kulccsal, erősebb algoritmussal, vagy későbbi lejárati időponttal rendelkező) Időbélyegzés szolgáltató egységtől származó időbélyeget kell kérnünk, amely bizonyíthatja, hogy a korábbi időbélyeg(ek) a benne szereplő időpont előtt, azaz még az Időbélyegzés szolgáltató tanúsítványának érvényessége alatt keletkeztek.

Továbbá, hosszabb (évtizedes nagyságrendű) időtávlatban gondolkodva reálisnak kell tartani azt a veszélyforrást, hogy az aláírás létrehozása során használt *kriptográfiai algoritmusok elavulhatnak*, azaz a számítástechnika vagy a matematika, kriptográfia fejlődésével belátható időn belül megoldható feladattá válhat azok törése, és így az aláírás hamisítása. Ennek bekövetkezése esetén a korábban ezen algoritmus felhasználásával készített aláírásokban nem szabad többé megbíznunk – kivéve, ha bizonyítani tudjuk, hogy az adott aláírás biztosan az algoritmus meggyengülése előtt készült. Ez szintén egy újabb időbélyeg elhelyezésével oldható meg, amely aláírja az aláíráshoz csatolt összes olyan elemet, amely létrehozása (kiszámítása) során bármilyen kriptográfiai algoritmus felhasználására került sor.

A *XAdES-A* (Archival electronic signature) aláírás a fentiek értelmében tehát tartalmaz egy újabb, ún. *archív időbélyeget*, amely aláírja az összes olyan elemet, amely valamilyen kriptográfiai algoritmus felhasználásával készült. Tekintve, hogy ezzel bizonyos nem várt események ellen akarunk védekezni, illetve hogy az archív időbélyeget készítő Időbélyegzés szolgáltató tanúsítványa is biztosan lejár valamikor, időről időre szükséges újabb és újabb archív időbélyeg elhelyezése az aláíráson, azaz *egy XAdES-A aláírás folyamatos karbantartást igényel*. Ez ráadásul nagy felelősséggel is jár, hiszen egy hiba vagy mulasztás következtében rengeteg aláírt dokumentum

---

[10] Az említett adategységekből kiderül azok készítésének ideje, azonban ezeket az időpontokat maga a szolgáltató rögzíti, éppen ezért nem szabad ilyen célból felhasználni. Hiszen például ha egy Hitelesítés szolgáltató kulcsa kompromittálódik, a megszerzett kulccsal lehet olyan tanúsítványt vagy CRL-t készíteni, amiről úgy tűnik, hogy még a kompromittálódás előtt készült. Megoldás lehetne, ha a szolgáltatók minden tanúsítványt és visszavonási információt a létrehozásukkor maguk ellátnának időbélyeggel, de ennek híján a felhasználás időpontját kell megbízható módon rögzítenie az aláírónak.

[11] Megjegyezzük, hogy az IHM ajánlás által definiált *hosszú távú aláírás* is hasonló ehhez (hiszen ott is kötelezően megkövetelik ezen értékek megjelenését), azonban annál nem szükséges a XAdES-X-nél bevezetett időbélyeg, ezért nem XAdES-X-L-nek, hanem csak XAdES-C-nek lehet azt megfeleltetni.

[12] Időbélyegzés szolgáltató tanúsítványát nem szokás felfüggeszteni illetve visszaállítani, így megalapozott az a feltételezés, hogy ha egy adott időpontban érvényes a tanúsítvány, akkor korábban is végig érvényes volt.

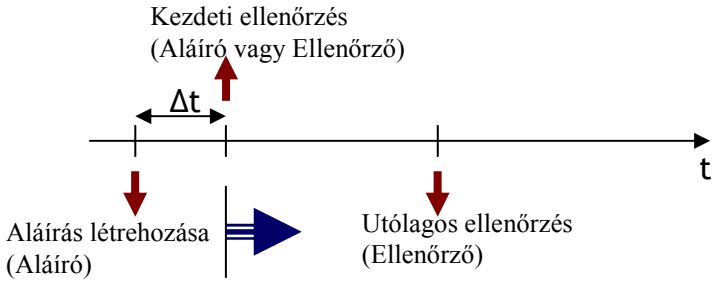
érvényessége válhat egyetlen csapásra bizonyíthatatlanná. Ezért az aláírt dokumentumok hosszú távú megőrzését sok esetben célszerű egy Archiválás szolgáltatóra bízni (lásd: [BE2007]).

Az IHM ajánlásban szereplő *archív aláírás* is egy XAdES-A aláírás.

### 2.7. Aláírás létrehozásának és ellenőrzésének fázisai

Már említettük, hogy előfordulhat, hogy a megcélzott aláírási forma létrehozáshoz szükséges összes adategység nem áll rendelkezésre az aláírás készítésekor, és így a kívánt forma csak több lépésben készíthető el. Elképzelhető az is, hogy az aláírás létrehozója nem kívánja elvégezni a szükséges adatokkal való kiegészítést, hanem azt helyette a befogadó fél végzi el. Ennek megfelelően a nemzetközi – és ennek megfelelően a hazai – ajánlások ([CWA14171], [IHM-AF], [IHM-ASZ]) három fázisra osztják egy aláírás létrehozását és ellenőrzését.

Az első fázis az aláírás létrehozása, amelyet az aláíró végez. A második fázist nevezzük *kezdeti ellenőrzésnek*, ekkor történik meg az aláírás kiegészítése a kívánt formára. Ezt akár az aláíró, akár az ellenőrző fél is elvégezheti, azonban lényeges, hogy az aláírás létrehozása és a kívánt formára való kiegészítés között minél kevesebb idő teljen el. A harmadik fázis az utólagos ellenőrzés, amikor már rendelkezésre áll az aláírás a végleges formájában, és így az ellenőrzés külső forráshoz való fordulás nélkül is elvégezhető.




### 2.8. Mikor melyik aláírás formát válasszuk?

A fentiekben láthattuk, hogy a felmerült újabb és újabb problémák elkerülése, kiküszöbölése érdekében elég sok adat csatolandó az aláíráshoz. Általánosságban igaz, hogy *minél magasabb aláírási formát választjuk, annál több tényező ellen biztosítunk védelmet, azonban egyúttal annál költségesebb és hosszadalmasabb az aláírás létrehozásának folyamata.*

Azaz a célforma meghatározásakor e kettőt kell mérlegelni. A választott aláírási formának mindenképpen ki kell elégítenie az elvárt biztonsági szintet, azonban nem szükséges (és nem is praktikus) mindenképpen a legmagasabb formához ragaszkodni, ha azt a helyzet nem indokolja.

## 3. PROBLÉMÁS HELYZETEK

### 3.1.Visszavonás, felfüggesztés, visszaállítás…

A gyakorlatban fel kell készülni arra a nem kívánt esetre, hogy az aláíró elveszíti a titkos kulcsát, vagy feltételezi, hogy mások is hozzáférhettek vagy hozzáférhetnek. Ekkor kérnie kell a tanúsítványának *visszavonását* az azt kibocsátó Hitelesítés szolgáltatótól, amely ilyenkor a megfelelő formában *publikálja a visszavonás tényét* (CRL vagy OCSP segítségével, lásd később).

Az életben viszonylag gyakran előfordul olyan eset, amikor az aláíró „nem találja” a kártyáját – nem biztos abban, hogy rossz kezekbe került a titkos kulcsa, azonban nem tudja kizárni ennek esélyét. A tanúsítvány visszavonása, majd helyette egy új igénylése időigényes és drága procedúra, ezért a gyakorlatban megszületett az igény a tanúsítványok ideiglenes *felfüggesztésére*, amely után – ha az aláíró mégis „megtalálja” elveszettnek vélt kártyáját – a tanúsítvány állapota *visszaállítható*. Ez a – gyakorlati alkalmazás szempontjából teljesen jogos – igény azonban rendkívüli módon meg tudja bonyolítania az aláírás ellenőrzés amúgy sem egyszerű feladatát, és szélsőséges esetekben vitatott helyzeteket is teremthet. A mai napig sem egyértelműen tisztázott, hogy *a tanúsítvány felfüggesztése és visszaállítása között keletkezett aláírásokat érvényesnek vagy érvénytelennek kell-e*

*tekinteni*. Az egyik megközelítés szerint *érvénytelennek*, hiszen a felfüggesztési időszak alatt keletkeztek, az ekkor beszerzett visszavonási információk mutatni fogják ezt a tényt. A másik megközelítés szerint pedig *érvényesnek*, hiszen azzal, hogy az aláíró visszaállított a tanúsítványát, tulajdonképpen azt jelenti ki, hogy a titkos kulcsát megtalálta, azzal nem történt semmi baj. És valóban, készíthető is olyan aláírás, amely a fent nevezett időszakban keletkezett, azonban a visszavonási információkat a visszaállítás után csatolták hozzá. Mivel *a visszaállítás után semmilyen nyoma nem marad a korábbi felfüggesztésnek*, így utólag az ilyen aláírásokról semmilyen módon nem lehet bizonyítani, hogy azok nem érvényesek. Mindez egyben azt is jelenti, hogy az aláíró tulajdonképpen utólag is el tudja dönteni, hogy aláírását érvényesnek vagy érvénytelennek szeretné beállítani, azaz a felfüggesztés és visszaállítás bevezetése az *aláírás letagadhatatlanságát ássa alá*.

Az említett probléma bizonyos esetekben egy megfelelő aláírási szabályzat alkalmazásával kezelhető, amely előírhatja például, hogy a visszavonási információkat az aláírás készítését követően mennyi időn belül kell csatolni[13] – ennek ellenőrzése azonban a befogadó fél feladata.

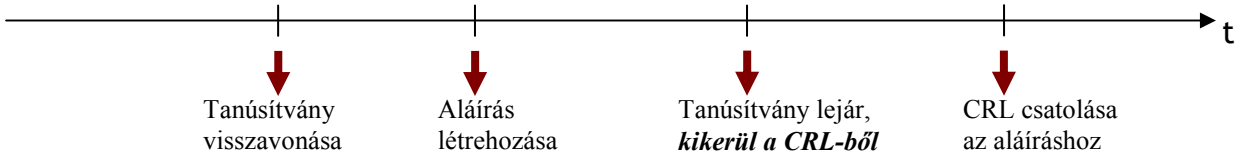
### 3.2. CRL-es technika problémái

A *Certificate Revocation List* (CRL, [RFC2527]) alapú visszavonás kezelés lényege, hogy a visszavont tanúsítványok (igazából a nyilvános kulcsok azonosítói) felírásra kerülnek a tanúsítvány visszavonási listára (CRL), amelyet a szolgáltató valamilyen közismert protokollon keresztül (jellemzően http, https vagy ritkán ldap) elérhetővé tesz.

A CRL egy *folyamatosan bővülő lista*, amelyet a szolgáltató alapesetben *rendszeresen*, *előre meghatározott időközönként* (pl. 24 óránként) publikál. Ez egyben azt is jelenti, hogy ha egy tanúsítványt visszavonnak, akkor az legrosszabb esetben csak 24 óra múlva derül ki, és az ez alatt készített aláírások még érvényesnek fognak „tűnni”. Lehetőség volna ún. *eseményvezérelt CRL* kibocsátására is, ami azt jelenti, hogy a szolgáltató nem csak előre megadott időnként, hanem minden visszavonást (felfüggesztést, visszaállítást) követően is kibocsát és publikál egy újabb CRL-t. Azonban az aláírás ellenőrző programok jellemzően nem kezelik az ilyen CRL-eket, hanem csak az előre megadott időpontok lejárta (ezt tartalmaznia kell a CRL-nek) után szerzik be a friss listát[14].

Egy másik probléma a CRL-ek folyamatos méretnövekedése, ami bizonyos szint fölött hatékonysági kérdéseket vet föl. Erre kínál bizonyos szintű megoldást az ún. *delta-CRL,* amely csak az előző teljes CRL-hez képesti változást tartalmazza. Azonban ekkor is időnként mindenképpen szükséges teljes CRL-t is kibocsátani. A delta CRL-eket sem kezeli minden aláírás ellenőrző program, valamint ez a technológia nem alkalmas a felfüggesztés utáni visszaállítás kezelésére.

Az előbbi problémát a gyakorlatban gyakran oldják meg úgy a szolgáltatók (amit egyébként az ajánlás megenged), hogy *a lejárt tanúsítványokat kiveszik a CRL-ből*, mondván, hogy egy lejárt tanúsítvánnyal úgysem lehet érvényes aláírást készíteni. Ez az állítás egyébként igaz, azonban azt az esetet teszik kezelhetetlenné ezzel, amikor egy korábban készített aláíráshoz később szerezzük be a visszavonási információkat. Így születhet meg az a problémás helyzet, amikor egy visszavont tanúsítvánnyal egy rossz indulatú fél a visszavonás és a lejárat időpontja között érvényesnek tűnő aláírást tud készíteni azzal, hogy a lejárat után szerzi be és csatolja a visszavonási információkat.




A CRL-es technika alkalmazása esetében további problémák is felmerülnek. Tudjuk, hogy nem csak az aláírói tanúsítványnak, hanem a megbízható hitelesítés szolgáltatóig felépített teljes

[13] Megjegyezzük, hogy a gyakorlatban éppen ennek ellenkezője szokott előfordulni: azt szokták előírni, hogy az aláírás létrehozása és a visszavonási információk csatolása között *legalább* mennyi időnek kell eltelnie, ami egy másik problémára nyújt megoldást, lásd később.

[14] Tegyük hozzá, hogy amennyiben az aláíró program mindig aktuálisan ellenőrizi, hogy esetleg nem érhető-e el friss visszavonási információ, akkor már sokkal praktikusabb (hatékonyabb) az OCSP-s megoldást alkalmazni (lásd később).

tanúsítvány-lánc minden elemének visszavonási állapota is ellenőrzendő. A végfelhasználói tanúsítvánnyal kapcsolatban az azt kibocsátó Hitelesítés szolgáltató bocsát ki CRL-t, míg a szolgáltató tanúsítványával kapcsolatban az ő tanúsítványát kibocsátó „felsőbb szintű" Hitelesítés szolgáltató által kibocsátott CRL ad információt, és így tovább... Azonban a lánc végén levő, megbízhatónak tekintett Hitelesítés szolgáltató tanúsítványáról nem szerezhető információ ilyen módon. Ez a feladat *nem oldható meg PKI alapon*, ilyenkor alternatív megoldásokat szoktak alkalmazni, például egy országos terjesztésű napilapban közzé teszik a kompromittálódás tényét.

Végül megemlítünk egy érdekes és nem nyilvánvaló problémát. A CRL-t a szolgáltató aláírásával látja el, amelyet szintén ellenőrizni kell. Jellemzően a szolgáltató ugyanazt a kulcsát használja a CRL aláírására, mint amelyikkel a végfelhasználói tanúsítványokat is aláírja. Ekkor az aláírás ellenőrző programok gyakran élnek azzal az egyszerűsítéssel, hogy a CRL-en levő aláírás ellenőrzését visszavezetik az aláírói tanúsítvány ellenőrzésére (hiszen mindkettőn ugyanannak a szolgáltatónak az aláírása szerepel). Pedig a két feladat nem teljesen ugyanaz, ugyanis a két aláírás *eltérő időpontokban* készült: az aláírói tanúsítványon levő szolgáltatói aláírásnak az *aláírás létrehozásának* időpontjában kell érvényesnek lennie, míg a CRL-en levő szolgáltatói aláírásnak a *CRL kibocsátásának* időpontjában. Amennyiben a szolgáltató kulcsa pont a kettő között kompromittálódik, akkor a kompromittálódás után készített (esetleg hamisított) CRL-t érvényesnek fogja találni ez a módszer. Ezért igazából a CRL-en levő aláírás ellenőrzésére egy újabb, az első CRL kibocsátásának időpontjára vonatkozóan releváns CRL beszerzésére volna szükség, és így tovább... Minél hosszabb az aláírói tanúsítvány-lánc, annál több további CRL beszerzésre és azon az aláírás ellenőrzésére van szükség, így az ellenőrzési feladat bonyolultsága és időigényessége rendkívüli mértékben megnőhet.

### 3.3. OCSP-s technika sajátosságai

Az *Online Certificate Status Protocol* (OCSP, [RFC2560]) alapú visszavonás esetében egy *adott tanúsítvány aktuális visszavonási állapotára* tudunk rákérdezni. Az *OCSP válasz* háromféle értéket tartalmazhat. Amennyiben „jó" értéket kapunk, az azt jelenti, hogy a tanúsítvány az OCSP válasz elkészítéséig nem lett visszavonva az adott OCSP válaszadó hatáskörébe tartozó Hitelesítés szolgáltató által – fontos azonban tudni, hogy mivel az OCSP válasz kizárólag erre a visszavonási állapotra vonatkozik, ettől még előfordulhat, hogy a tanúsítvány lejárt[15] és így esetleg nem érvényes az ellenőrzött aláírás. Amennyiben „visszavont" értéket kapunk, akkor a válasz mindenképpen tartalmazza a visszavonás időpontját is, és ez alapján meghatározható, hogy a vizsgált aláírás ez előtt vagy ez után készült-e – így előfordulhat, hogy egy „visszavont" OCSP válasz érkezésekor mégis az a helyes végkövetkeztetés, hogy a vizsgált aláírás érvényes. Az „ismeretlen" érték érkezésekor pedig – a visszavonási állapotra vonatkozó információ hiányában – befejezetlennek kell tekinteni az ellenőrzést.

Az OCSP-s technika alkalmazásának nagy *előnye*, hogy mindig az *aktuális állapotról ad információt*, azonban mindig szükséges hozzá *Internet kapcsolat*.

*OCSP alapú visszavonás-kezelés nyújtásakor* különböző *architektúrák* képzelhetőek el. Lehetséges például, hogy *ugyanaz az egység nyújtsa* az OCSP szolgáltatást, amelyik a végfelhasználói tanúsítványok aláírását is végzi. Ilyenkor azonban nem megoldott magának a Hitelesítés szolgáltatónak a tanúsítványával kapcsolatos visszavonási információk beszerzése, ezt más módon kell megoldani (CRL-lel vagy alternatív úton). Ha egy másik egység nyújtja az OCSP szolgáltatást, akkor ez már nyújthat OCSP szolgáltatást a Hitelesítés szolgáltató tanúsítványával kapcsolatban is, azonban ekkor ezen OCSP válaszadó a tanúsítványának az ellenőrzése marad megoldandó probléma. A rendszer természetesen tovább bonyolítható újabb OCSP válaszadók bevezetésével. Azonban a jó megoldást nem ezen az úton találjuk meg. Jelenlegi ismereteink szerint a legjobb és legbiztonságosabb megoldás az, amikor az OCSP *válaszadó rövid lejáratú tanúsítvánnyal* rendelkezik (ez alatt 10 perces nagyságrendet értve). Ilyenkor az OCSP válaszadó tanúsítványát

[15] Sőt, sajnos akkor is adható „jó" válasz, ha a tanúsítvány egyáltalán nem létezik (így nem is lett visszavonva), vagy esetleg egy másik szolgáltatónál kibocsátott és ott visszavont tanúsítványról van szó.

egyszerűen *nem kell ellenőrizni*, ugyanis egy esetleges kompromittálódás esetében az ő tanúsítványa nem visszavonásra kerül, hanem számára nem bocsátanak ki újabb tanúsítványt[16].

### 3.4. Kivárási idő

Korábban említettük, hogy a CRL-es visszavonási technika szakaszossága miatt egy tanúsítvány visszavonási állapotának változása nem derül ki azonnal. Azért, hogy ebben az időszakban ne az aláírónak kelljen viselnie a kockázatot (hogy az esetlegesen illetéktelen kezekbe került titkos kulcsával érvényes aláírást hoznak létre), bevezették a *kivárási idő* fogalmát. Ez azt jelenti, hogy az aláírás elkészítése és a visszavonási információk csatolása között el kell telnie a meghatározott kivárási időnek – ezt az előírást például az aláírási szabályzatban lehet rögzíteni. A kivárási idő hosszúságát két tényező befolyásolja. Az egyik, hogy az adott Hitelesítés szolgáltató mennyi idő alatt *dolgozza fel* a beérkező visszavonási kéréseket, a másik, hogy az új visszavonási állapotot mennyi időn belül *publikálja*.
Az OCSP-s visszavonási technika alkalmazása esetében a publikálás időtartam természetesen nulla, azonban a visszavonás feldolgozásának időtartamával itt is lehet számolni.
A MELASZ által kidolgozott MELASZ-Ready feltételrendszer [MELASZ] például 30 perces kivárási időt határoz meg OCSP használata esetében, CRL esetében pedig 24 órát. A közigazgatásban alkalmazható aláírási szabályzatokról szóló IHM ajánlás [IHM-ASZ] azonban mindkét esetre egységesen 4 órát ír elő.
A kivárási idő alkalmazása mindazonáltal egyértelműen azzal a következménnyel jár, hogy az aláírás nem készíthető el egyetlen lépésben.

### 3.5. Későbbi időbélyegzés kockázata

A közigazgatásban alkalmazható aláírási szabályzatokról szóló IHM ajánlás [IHM-ASZ] azt az elképzelést tartalmazza, hogy az ügyfelek időbélyegzés nélkül küldik be az aláírt dokumentumot a közigazgatás számára, az aláírások időbélyeggel (illetve egyéb adatokkal) való kiegészítését a befogadó fél végzi. Ezzel valószínűleg az ügyfeleket akarták tehermentesíteni, azonban ez a modell magában hordozza azt a veszélyt, hogy az aláírás készítése és a kezdeti ellenőrzés között eltelt idő megnőhet, és az ebben az időszakban a tanúsítvány állapotában bekövetkező változás (pl. lejár vagy visszavonják) a már beadott, de még fel nem dolgozott dokumentumok aláírásának érvényességét is befolyásolja.

## 4. HIVATKOZÁSOK


[RFC3275] RFC 3275: XML-Signature Syntax and Processing, 2002

[RFC2560] RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 1999

[RFC2527] RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, 1999

[XAdES] ETSI TS 101 903 XML Advanced Electronic Signatures, V1.3.2, 2006

[CWA14171] CWA 14171, General guidelines for electronic signature verification, 2004

[IHM-AF] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírás formátumok műszaki specifikációjára. 2005

[IHM-ASZ] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére, 2005

[MELASZ] MMM 001:2005. Egységes MELASZ formátum elektronikus aláírásokra, verzió1.0

[BE2007] Berta, I. - Endrődi, Cs.: Minősített archiválás szolgáltatás beindítása Magyarországon, Networkshop, 2007


[16] Megjegyezzük, hogy ez a megoldás *elvben* a végfelhasználói tanúsítványokra is működhetne (és akkor nem kellene „bajlódni" a visszavonási információkkal), azonban természetesen hatékonysági okokból ez a gyakorlatban nem megoldható.