Aláírási jogosultság igazolása elektronikusan

Dr. Berta István Zsolt

Microsec Kft.

1. Bevezetés

A nyilvános kulcsú infrastruktúra (PKI) minden szereplőjének van magánkulcsa és nyilvános kulcsa. A magánkulcsát mindenki titokban tartja, míg a nyilvános kulcsát nyilvánosságra hozza. Ha megszerezzük valakinek a nyilvános kulcsát, titkosított üzeneteket küldhetünk számára, illetve ellenőrizhetjük az általa létrehozott elektronikus aláírásokat. Lényeges, hogy az illető nyilvános kulcsa hitelesen kerüljön a birtokunkba, azaz biztosan tudjuk, hogy pontosan kinek a nyilvános kulcsát szereztük meg. A nyilvános kulcsú infrastruktúra arra épül, hogy egyes hitelesítés szolgáltatók nyilvános kulcsát már ismerjük, és mások nyilvános kulcsainak hitelességéről az ismert szolgáltatói kulcsok alapján győződünk meg. A hitelesítés szolgáltatók nyilvános kulcsú aláírói tanúsítványt[1] állítanak ki, ezzel igazolják, hogy egy adott nyilvános kulcs kihez tartozik.

Gyakran nemcsak arra vagyunk kíváncsiak, hogy az aláírói tanúsítvány alanya (akinek a hitelesítés szolgáltató kibocsátotta az aláírói tanúsítványt) pontosan ki, hanem azt is tudni szeretnénk, hogy az illető milyen szerepkörrel, jogosultsággal, tulajdonsággal rendelkezik, azaz milyen minőségben használja az aláírói tanúsítványát. Lehet, hogy az aláírói tanúsítványt egyszerűen magánszemélyként kívánja használni, de az is lehet, hogy valamely szervezet tagjaként vagy munkatársaként, egy vállalat képviselőjeként, valamilyen hivatással (ügyvéd, közjegyző) rendelkező személyként, vagy egy szolgáltatás előfizetőjeként.

2. Hogyan állapítható meg egy tanúsítvány alanyának szerepköre, jogosultsága?

Attól függően, hogy az alany aláírói tanúsítványát a hitelesítés szolgáltató milyen módon bocsátja ki, milyen információkat hol és hogyan tüntet fel, illetve az alany milyen módon, esetleg milyen aláírási szabályzat szerint használja az aláírói tanúsítványt, szerepkörei, jogosultságai, tulajdonságai (együttesen: attribútumai) más és más módon állapíthatóak meg az aláírói tanúsítvány vagy az aláírás alapján. Ez gyakran interoperábilitási problémákhoz vezet: előfordulhat, hogy egy rendszer nem engedi be a jogosult felhasználót, de az is lehet, hogy jogosulatlan felhasználót enged be, vagy nem a megfelelő jogosultságokkal enged be valakit.

A fejezet hátralévő részében azt írjuk le, hogy ma milyen megoldások terjedtek el az attribútumok feltüntetésére. Egyúttal azt is megmutatjuk, hogy ezek a megoldások milyen korlátokkal rendelkeznek, miért nem skálázhatóak, miért nem működnek nagy rendszerekben, ahol sok hitelesítés szolgáltató, sok felhasználó és sok attribútum van jelen. Úgy látjuk, azért van szükség attribútum tanúsítványokra, mert a ma használt megoldások nem, illetve nem jól oldják meg a felmerülő problémákat.

---

[1] Jelen dokumentumban a nyilvános kulcsú tanúsítványok közül kizárólag az aláírói tanúsítványokkal (elektronikus aláíráshoz használható tanúsítványokkal) foglalkozunk, ezen tanúsítványokra „aláírói tanúsítvány” vagy „nyilvános kulcsú tanúsítvány” névvel hivatkozunk. Igyekszünk kerülni az önmagában álló „tanúsítvány” szót, nehogy összekeverhető legyen az „attribútum-tanúsítvány” fogalmával.

A következő alfejezetek a jelenleg használt műszaki megoldások részleteit, és korlátait írják le.

2.1. Implicit kapcsolat

Implicit kapcsolatról akkor beszélünk, ha valamilyen rendszerben csak a „jogosult" személyek rendelkeznek tanúsítvánnyal. Ekkor, ha valakinek tanúsítványa van, az egyben azt is jelenti, hogy az illető rendelkezik a rendszer használatához szükséges szerepkörrel, jogosultsággal.

Tegyük fel, hogy egy baráti társaság saját mini hitelesítés szolgáltatót hoz létre, és ez a szolgáltató kizárólag a baráti társaság tagjainak bocsát ki tanúsítványt. Ha érvényesnek találunk egy tanúsítványt vagy aláírást a baráti társaság gyökértanúsítványa alapján, akkor nemcsak arról győződünk meg, hogy az aláírói tanúsítványhoz tartozó magánkulcsot az illető személy birtokolja, hanem egyben arról is, hogy ő a baráti társaság tagja.

Azzal, hogy a letagadhatatlanság (aláírás) és az azonosítás fogalmát összemossuk, egyszerű és könnyen kezelhető rendszerhez jutunk. Elegendő az aláírói tanúsítvány érvényességét ellenőriznünk, az érvényes tanúsítvány egyben a baráti társaság tagsági viszonyát is igazolja, így az alanyt feljogosítja arra, hogy a társaság erőforrásait használja.

Az alany jogosultságai az aláírói tanúsítványával együtt, egy helyen visszavonhatóak.

Ennek a megoldásnak a következő hátrányai vannak:

a) Egyrészt ilyen módon csak egyetlen szerepkör[2], **csak egyetlen attribútum kezelhető**,

b) másrészt e megoldás **nehezen kapcsolható más rendszerekhez**, ezért elsősorban zárt közösségben használható.

Hogyan fogadhatja el az egyik közösség egy másik közösség tanúsítványát, és hogyan biztosítható ilyen esetekben a rendszerek együttműködése?

A következő felsorolás néhány megoldási lehetőséget mutat az implicit kapcsolat problémáinak kezelésére, figyelemmel a hátrányos következményekre is:

1. **Az egyes közösségek megbíznak egymás gyökértanúsítványaiban. Így minden egyes közösség és minden egyes jogosultság egy-egy gyökértanúsítványt jelent.**

   Ezáltal nagyon nehézzé válik egy új közösség/jogosultság bevezetése, mert az adott gyökértanúsítványt minden egyes végfelhasználó gépére telepíteni kell. A megszűnt vagy kompromittálódott gyökértanúsítványok eltávolítása is problémákhoz vezet, mert azokat külön-külön minden egyes végfelhasználónál törölni kell a rendszerből.

   A megoldás hátrányos tulajdonsága még, hogy a gyökértanúsítványok számának növekedésével egyenes arányban a felmerülő problémák száma is növekszik.

2. **Az egyes közösségek gyökértanúsítványaival rendelkező CA-k kereszthitelesítik egymást (tanúsítványokat bocsátanak ki egymás számára).**

   Ezáltal az egyes közösségeken kívüli személyek tanúsítványait is lehet majd ellenőrizni a közösség gyökértanúsítványa alapján.

[2] A példa szerint a tagsági viszony.

A megoldás hátrányos tulajdonsága, hogy a fent ismertetett módszerrel nem lehet megállapítani, hogy ki milyen szerepkörrel, jogosultsággal rendelkezik, hiszen a kereszthitelesítés miatt több PKI közösségnek is tagjává válik.

3. **A közösségek új, közös CA-t hoznak létre, amely tanúsítványt bocsát ki az egyes közösségi CA-k számára.**

   Ebben az esetben a jogosultságok, illetve szerepkörök a tanúsítványláncokban fellelhető köztes CA-k tanúsítványai alapján vezethetők le.

   A megoldás hátrányos tulajdonsága, hogy ekkor az egyes alkalmazásokba „bele kell drótozni" a köztes tanúsítványokat is azért, hogy az alkalmazások meg tudják állapítani a megfelelő szerepköröket, illetve jogosultságokat. A köztes tanúsítványok lejárta, visszavonása, cseréje az alkalmazásokat is érinti, ezáltal a művelet biztonságos elvégzése nagyon körülményessé válik. Az is előfordulhat, hogy valaki több közösségnek is tagja, ezért az egyes közösségektől továbbra is külön-külön tanúsítványokat kell beszereznie. Ráadásul a megoldás nem szabványos, a tanúsítványlánc jellegzetességeiből kívülálló nem tud az alany jogosultságaira következtetni.

Összefoglalva: Nagy rendszerekben – ahol több közösség, több jogosultság jelenik meg – az implicit kapcsolaton alapuló megoldás nem alkalmazható.

2.2. Az attribútum a nyilvános kulcsú aláírói tanúsítványban szerepel

Másik lehetőség, hogy az alany aláírói tanúsítványa tartalmaz olyan mezőket, amelyekből az alany szerepköre vagy jogosultsága megállapítható.

Az alany szerepköre vagy jogosultsága általában a következő helyeken szerepelhet az aláírói tanúsítványban:

1. az alany megnevezésében (DN, distinguished name): Ekkor a jogosultság általában a „title" (emellett esetleg az „organization", „organization unit" stb.) mezőben jelenik meg. Például, az aláírói tanúsítványban lévő Subject DN title elemének értéke „ügyvezető".

   A megoldás hátrányos tulajdonsága, hogy a szöveges leírásokat nehéz géppel automatizáltan feldolgozni[3], és az ott feltüntetett adatok csak egy adott nyelvterületen belül értelmezhetőek. Minél több hitelesítés szolgáltató és regisztrációs szervezet működik egy PKI közösségben, a Subject DN használata annál több interoperábilitási problémát eredményezhet.

2. Az aláírói tanúsítványra vonatkozó valamely hitelesítési rendben (certificate policies): A nyilvános kulcsú tanúsítvány tartalmazza a rá vonatkozó hitelesítési rendek azonosítóját. A hitelesítési rend pedig szövegesen tartalmazhatja, hogy az adott rendnek megfelelő aláírói tanúsítvány alanya mely attribútummal rendelkezik. A megoldás előnyös tulajdonsága, hogy a hivatkozás OID alapján történik, így számítógép is könnyen fel tudja dolgozni.

   A megoldás hátrányos tulajdonsága, hogy amennyiben gépi feldolgozásra nincs lehetőség, természetes személy nagyon nehezen tudja az OID-be kódolt adatokat értelmezni. Másfelől pedig túlságosan körülményes minden szerepkörhöz, jogosultsághoz, tulajdonsághoz külön-külön hitelesítési rendet felvenni.

[3] A tanúsítványban „ügyvezető" helyett szerepelhet „Ügyvezető", „ÜGYVEZETŐ", „ügyvezető igazgató", „vezérigazgató" stb. is. Ráadásul, a szöveg akár különböző (latin-2, UTF-8) kódolással, vagy ékezet nélkül is szerepelhet.

3. A szerepkör, illetve jogosultság egyéb helyeken (pl. subjectDirectoryAttributes kiterjeszés) van feltüntetve.

   A megoldás hátrányos tulajdonsága, hogy nagyon kevés szolgáltató, és így nagyon kevés alkalmazás támogatja a megoldást.

A magyar közigazgatásban az 1. és 2. megoldás keverten jelentkezik, mert:

a) a hitelesítési rend alapján el lehet dönteni, hogy az alany közigazgatási szerepkört tölt-e be[4],

b) további finomítás pedig az alany DN-je alapján lehetséges.

Ha az aláírói tanúsítványt több célra is szeretnénk használni, várhatóan többféle szerepkört, illetve jogosultságot is fel kell tüntetni a tanúsítványban. (Például, valaki egy cég ügyvezetője, de emellett egy egyesület elnökségi tagja, és egyúttal ügyvéd is.)

E megoldás hátrányos következményei:

- Nehéz megállapítani, hogy az alany éppen melyik szerepében, melyik jogosultsága szerint használja/használta az aláírói tanúsítványát.
- Ha egy tanúsítványban szereplő bármely jogosultság megváltozik, az aláírói tanúsítványt vissza kell vonni, és helyette újat kell kibocsátani.
- Az aláírói tanúsítvány lecserélését a hitelesítés szolgáltatónak kell végeznie, aki jellemzően nem ugyanaz a fél, mint aki az alany szerepköreiről, jogosultságairól dönt. Ez már önmagában is jelentősen megnehezíti, megdrágítja a folyamatot.
- Az aláírói tanúsítvány lecserélésére – elsősorban minősített tanúsítvány esetén – összetett szabályok vonatkoznak. Az új tanúsítványt jellemzően másik magánkulcshoz kell kibocsátani, és esetleg a teljes – a személyes találkozót is igénylő – regisztrációs eljárást meg kell ismételni.
- Az adatvédelmi szabályok miatt egy tanúsítványból közvetlenül[5] nem határozható meg, hogy az alany kicsoda. Ezért a célrendszerekben valamilyen „másodlagos regisztrációt" kell használni, nyilvántartásba kell venni az alany tanúsítványát, és fel kell jegyezni, hogy az melyik alanyhoz tartozik. Ha az alany tanúsítványa gyakran változik, ezt a körülményes műveletet is gyakran meg kell ismételni.
- Ha az alany sok attribútummal (szerepkörrel, jogosultsággal) rendelkezik, nem szeretné feltétlenül, hogy az aláírói tanúsítványából kiderüljön, hogy pontosan milyen attribútumai vannak[6].

[4] A közigazgatás számára más hitelesítési rendek szerint lehet tanúsítványt kibocsátani, mint a közigazgatás ügyfelei számára.

[5] A tanúsítvány alanyának személyazonosságának meghatározásához a hitelesítés szolgáltató által felvett, nem nyilvános regisztrációs adatok is szükségesek.

[6] A tanúsítványt kibocsátó hitelesítés szolgáltató tanúsítványtárából esetleg még visszamenőleg is megállapítható lehet, hogy kinek mikor milyen attribútumai voltak, melyiket mikor szerezte, és mikor veszített el.

2.3. Az attribútum az alany állításából derül ki

Elsősorban papír alapú rendszerekben gyakori, hogy amikor valaki aláír egy dokumentumot, ő maga nyilatkozik róla, hogy milyen szerepkörben írja alá. A dokumentumot felhasználó fél elfogadhatja az aláíró állítását, de úgy is dönthet, hogy – egy esetleg igen körülményes eljárás keretében – utánajár az aláíró szerepkörének, jogosultságának.

E megoldásnak kockázata, hogy az aláíró hazudhat, olyan attribútumot is állíthat magáról, amellyel nem rendelkezik. Ekkor a dokumentumot felhasználó fél bíróság előtt felelősségre vonhatja az aláírót a hamis állítást tartalmazó aláírt dokumentum alapján.

2.4. Az attribútumot más informatikai rendszer tartalmazza

Elektronikus dokumentumokat kezelő rendszerekben a papír alapú rendszerekhez hasonlóan kézenfekvőnek tűnik az a megoldás, amikor az aláíró szerepköreit, jogait nem az aláíró elektronikus aláírásának tanúsítványa, hanem valamilyen más, az elektronikus aláíráshoz csatolt elektronikus dokumentum tartalmazza.

Ebben az esetben az elektronikus aláírás tanúsítványa egyedül azt igazolja, hogy az alany valóban birtokolja az aláírói tanúsítványhoz tartozó magánkulcsot[7].

Ebből az következik, hogy az aláírói tanúsítvány ellenőrzését követően valamilyen más rendszertől származó bizonyítékok alapján kell ellenőrizni, hogy az alany valóban rendelkezik-e a megfelelő jogosultsággal, illetve szerepkörrel.

A megoldás vitathatatlan előnye, hogy az aláíróknak elegendő egyetlen aláírói tanúsítványt birtokolniuk, és azt minden célra, minden szerepkörben felhasználhatják. Nem kell az aláírói tanúsítványt visszavonni és újat kibocsátani, ha az alany valamely attribútuma megszűnik, vagy ha az alany új attribútumhoz jut. Az aláírói tanúsítványt kibocsátó hitelesítés szolgáltatónak nem kell nyilvántartania, hogy az egyes alanyok milyen attribútumokkal rendelkeznek. A szerepkörök, jogosultságok kiosztása, illetve megszüntetése ott történik, ahol az attribútumok használatáról döntenek, és arról megfelelő nyilvántartást vezetnek.

A megoldás szerint a dokumentum elektronikus aláírásának folyamatában ugyanakkor kapcsolatba kell lépni azokkal a rendszerekkel is, amelyek az alany kérdéses attribútumait nyilvántartják, és az adott szerepkört, jogosultságot bizonyító, a szervezet elektronikus aláírásával ellátott igazolásokat 'online' szolgáltatnak ahhoz, hogy azokat megfelelő módon az aláírásokhoz lehessen csatolni[8].

Az attribútum-tanúsítványok használata ennek a feladatnak a megoldásához nyújt rugalmas és szabványos megoldást.

3. Mit nevezünk attribútum-tanúsítványnak?

Az attribútum-tanúsítvány olyan igazolás, amely egy nyilvános kulcsú tanúsítványhoz, vagy a nyilvános kulcsú tanúsítvány alanyához kapcsolódik, és alkalmas a nyilvános kulcsú tanúsítvány alanyához tartozó egy vagy több szerepkör, jogosultság, tulajdonság (együttesen: attribútum) igazolására.

[7] Érvényes tanúsítvány esetén kizárólag ő birtokolja a kulcsot, az érvénytelen tanúsítvány esetén ez már nem garantálható.

[8] Fontos, hogy a szervezetekkel felvett kapcsolat is szabványos, egységes és biztonságos (hiteles) legyen.

Nyilvános kulcsú aláírói tanúsítvány esetén az attribútum-tanúsítvány az aláírói tanúsítványhoz kapcsolódik. Az alany nyilvános kulcsát és „kilétét[9]" az aláírói tanúsítvány alapján lehet megállapítani[10], az alany szerepköreit, jogosultságait, tulajdonságait (attribútumait) pedig attribútum-tanúsítványai tartalmazzák.

Az attribútum-tanúsítvány hivatkozást tartalmaz a nyilvános kulcsú aláírói tanúsítványra (vagy annak alanyára), így egy adott attribútum-tanúsítványról és egy adott nyilvános kulcsú aláírói tanúsítványról megállapítható, hogy a két tanúsítvány alanya megegyezik.

Az alany nyilvános kulcsát a nyilvános kulcsú aláírói tanúsítvány tartalmazza. **Az attribútum-tanúsítvány nem tartalmaz kulcsot**. Mivel az attribútum-tanúsítványban nincs kulcs, az attribútum-tanúsítvány **használatához intelligens kártyára sincs szükség.**

3.1. Nemzetközi specifikációkban

3.1.1. Főbb mértékadó specifikációk

Az attribútum-tanúsítványok szintaxisát az X.509 ajánlás tartalmazza (így az „X.509 tanúsítvány" fogalom nyilvános kulcsú tanúsítványt és attribútum-tanúsítványt is jelent). Az attribútum-tanúsítványok profilját, kezelését az RFC 3281 is meghatározza [RFC3281]. Az RFC 3281 egyúttal az attribútum-tanúsítóra és az ő aláírói tanúsítványra vonatkozó követelményeket is meghatároz:

> 4.5 Profile of AC issuer's PKC
>
> The AC issuer's PKC MUST conform to [PKIXPROF], and the keyUsage extension in the PKC MUST NOT explicitly indicate that the AC issuer's public key cannot be used to validate a digital signature. In order to avoid confusion regarding serial numbers and revocations, an AC issuer MUST NOT also be a PKC Issuer. That is, an AC issuer cannot be a CA as well. So, the AC issuer's PKC MUST NOT have a basicConstraints extension with the cA BOOLEAN set to TRUE.

Vagyis az attribútum-tanúsítvány aláírásához használt tanúsítvány nem lehet hitelesítés szolgáltatói tanúsítvány. Így az attribútum-tanúsítványt nem hitelesítés szolgáltató, hanem a hitelesítés szolgáltatás végfelhasználója bocsátja ki, és elektronikus aláírással látja el. Ezért az attribútum kibocsátó végfelhasználó tanúsítványának alkalmasnak kell lennie elektronikus aláírás létrehozására.

Az ETSI TR 102 044 [ETSI_ACREQ] az RFC 3281-re hivatkozva, az attribútum-tanúsítványokra vonatkozó általános követelményeket írja le. Ismerteti az attribútum-tanúsítványokra vonatkozó európai gyakorlatot, valamint javaslatot tesz az egyes főbb általános attribútumok szabványos megnevezésére (OID segítségével történő jelzésére).

Az ETSI TS 102 158 [ETSI_ACPREQ] olyan szabályozási követelményeket határoznak meg attribútum-tanúsítók (attribute authority, AA) számára, amelyek a minősített tanúsítványokéval egyenszilárdságú biztonságot jelentenek.

[9] A személyazonosság megállapításához a nyilvános kulcsú tanúsítvány nem elegendő, a hitelesítés szolgáltató által felvett regisztrációs adatok is szükségesek hozzá. Jogvita estén a hitelesítés szolgáltató segítségével állapítható meg a nyilvános kulcsú tanúsítvány alanyának személyazonossága.

[10] Ahogy azt az előző fejezetekben leírtuk, a nyilvános kulcsú tanúsítvány is tartalmazhat attribútumokat.

Az ETSI 101 903 [XAdES] az XML aláírások formátumát határozza meg. A dokumentum leírja, hogy az XML aláírásban hogyan lehet attribútum-tanúsítványt szerepeltetni[11]. Itt az aláíráshoz csatolt, az aláíró által is aláírt – esetleg harmadik féltől származó – igazolás bizonyítja az aláírónak azt a szerepkörét, jogosultságát (attribútumát), amelyet az aláírás idejében használt.

3.1.2. Általános attribútum-tanúsító

Az ETSI dokumentumai – elsősorban az [ETSI_ACPREQ] – a hitelesítés szolgáltatáshoz hasonló, általános attribútum-tanúsítás szolgáltatást képzelnek el, ahol az attribútum-tanúsító olyan megbízható harmadik fél (TTP, trusted third party), amely az egyes felhasználók attribútumaira a hitelesítés szolgáltatókhoz hasonló módon ad ki igazolást. A TTP-jellegű általános attribútum-tanúsító többféle – akár tetszőleges – attribútumot tanúsíthat, és az érintett felek hasonlóan a minősített tanúsítványban igazolt állításhoz hasonlóan "komolyan veszik" az attribútum-tanúsító állításait, és megbíznak abban.

Mivel az általános attribútum tanúsító bármilyen attribútumot tanúsíthat, legalább olyan szintű biztonsággal kell működnie, amely a legérzékenyebb attribútum esetén szükséges. Ez magyarázza az [ETSI_ACPREQ] erős követelményeit. Ugyanakkor, számos attribútum esetén közel sincs szükség ilyen erős bizonyítékokra. Annyira, hogy az ETSI TR 102 044 ún. „claimed role"-t is megenged, ahol valaki saját maga számára állít ki attribútum tanúsítványt – saját attribútumairól nyilatkozik a 2.3. fejezetben leírt gondolatmenet szerint. Bizonyos attribútumok esetén vagy bizonyos helyzetekben ilyen szintű garancia is elegendő. Így nyilvánvaló, hogy egyes esetekben túlzó követelményeknek számítanak azok az előírások, amelyeket az attribútum-tanúsítókkal szemben az ETSI TR 102 044 magában foglal.

A specifikációkban elkülönül, hogy ki rendelkezik a felhasználók attribútumairól (AGA, attribute granting authority vagy AIA, attribute issuing authority), illetve ki az attribútum-tanúsítványt kibocsátója, aláírója (AA, attribute authority).

Ha AA és AGA elkülönülnek egymástól, akkor AA pontosan olyan helyzetben van, mint egy hitelesítés szolgáltató: harmadik féltől származó igazolásokra támaszkodva kell igazolnia az attribútumokat.

Egy AA – a hitelesítés szolgáltatók esetén elfogadott megoldáshoz hasonlóan – több AGA-val is kapcsolatban lehet.

3.2. Jogi szempontok

3.2.1. Milyen joghatással rendelkezik az attribútum-tanúsítvány?

A hazai jogszabályok nem definiálják az „attribútum-tanúsítvány" fogalmát, így az attribútum tanúsítvány az elektronikus aláírásról szóló törvény (Eat.) szerint értelmezhető. Az Eat. a következő módon definiálja a „tanúsítvány" fogalmát:

> *Eat., 2. §, „21. Tanúsítvány: a hitelesítés-szolgáltató által kibocsátott igazolás, amely az aláírás-ellenőrző adatot a 9. § (3), illetőleg (4) bekezdése szerint egy meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget."*

[11] Az attribútum-tanúsítvány az aláírt elemek közé kerül, így aláírásával az alany megerősíti, hogy éppen melyik szerepkörében, melyik attribútuma szerint ír alá.

A fent ismertetett – ajánlások szerinti – attribútum-tanúsítvány nem fér bele az Eat. szerinti tanúsítvány fogalmába, hiszen nem tartalmazza az aláírás-ellenőrző adatot, így nem kapcsolja azt meghatározott személyhez sem. Az attribútum-tanúsítványokat merőben másképp kell kibocsátani vagy felhasználni, mint az Eat. szerinti nyilvános kulcsú aláírói tanúsítványokat. Az attribútum-tanúsítvány önmagában – egy az Eat. szerinti nyilvános kulcsú aláírói tanúsítvány nélkül – nem használható.

A 3.1. fejezetben megmutattuk, hogy az attribútum-tanúsítványt **nem hitelesítés szolgáltató**, hanem aláírásra képes végfelhasználó **bocsátja ki**. Ebből következik, hogy az Eat. értelmében az attribútum-tanúsítvány mindössze egy elektronikus aláírással ellátott **elektronikus dokumentum**, amelyen egy végfelhasználó – az Eat. fogalmai szerint egy aláíró – helyez el fokozott biztonságú vagy minősített elektronikus aláírást. Ez a dokumentum egy szabványos, géppel is értelmezhető formátumú igazolás, amely az igazolást kérő személy szerepkörét, jogosultságát, illetve tulajdonságát igazolja.

Az attribútum-tanúsítványon elektronikus aláírás van, így – fokozott biztonságú elektronikus aláírás esetén – egyenértékű lehet egy írásba foglalt igazolással, amely például a következőket tartalmazza:

> *„Alulírott Gipsz Jakab (szig. szám: XY123456), a Kókler Kft. ügyvezetője igazolom, hogy Nagy Zebulon, az 01234567890123456789...01234567890123456789 SHA-256 lenyomatú tanúsítvány alanya a Kókler Kft. munkatársa, aki jogosult a Kóker Kft. címére érkező küldeményeket átvenni. Jelen igazolás 2008 január 7. és 2008. január 8. között érvényes.*
>
> *[dátum, aláírás]”*

Így egy attribútum tanúsítvány a fenti igazolással azonos joghatással rendelkezik.

3.2.2. Ki jogosult attribútum-tanúsítványt kiállítani, és milyen attribútumokat jogosult valaki igazolni?

A fenti papír alapú igazolással egyenértékű attribútum-tanúsítványt az állíthat ki, és olyan attribútumokról, amelyről a fentihez hasonló igazolást egyébként papíron is jogában áll kiadni.

3.2.3. Összefoglalva

- **A hatályos jogszabályok szerint semmi akadálya annak, hogy valaki attribútum-tanúsítvány formájában állítson ki igazolást olyan tényről, amelyről papír alapú igazolást is kiadhat**. Ez esetben AA és AGA megegyezik. Az attribútum-tanúsítvány szabványos, számítógéppel is értelmezhető ellenőrizhető szerkezettel rendelkező, írásba foglalt igazolásnak minősül.
- **Általános célú, TTP-jellegű,** az [ETSI_ACPREQ] specifikációban elképzelt **attribútum tanúsító megjelenése ugyanakkor nehezen képzelhető el Magyarországon.**

  Ennek oka, hogy ha AA és AGA nem esik egybe, akkor az AA által aláírt igazolásokat, attribútum-tanúsítványokat nem lehet megbízható módon ellenőrizni – legalábbis nem egyszerű[12] AGA-ra visszavezetni, következésképpen az attribútum-tanúsítványokban feltüntetett szerepköröket, jogosultságokat sem könnyű elfogadni.

[12] Az ellenőrzési eljárásban azt kellene bizonyítani, hogy AA jogosult egy adott attribútummal kapcsolatban igazolást kiállítani. Ez történhetne ugyan egy AGA által AA számára kiállított attribútum tanúsítvány alapján is, de AA szerepe éppen az volna, hogy AGA-nak ne kelljen attribútum tanúsítványokkal foglalkoznia.

4. Modell az attribútum-tanúsítványok felhasználására

Az alábbiakban egy olyan rendszert körvonalazunk, amelyben több, független hitelesítés szolgáltató, és több, független attribútum-tanúsító (AA) működik. Modellünk az attribútum-tanúsítványokra vonatkozó specifikációk szűkítéséből, pontosításából, illetve a hazai helyzethez történő illesztéséből származik.

A körvonalazott rendszerben hitelesítés szolgáltatók adják ki a végfelhasználók (köztük az attribútum-tanúsítók) aláírói tanúsítványait, az AA-k pedig a végfelhasználók aláírói tanúsítványaihoz kapcsolódó szerepkör, jogosultság igazolásokat (attribútum-tanúsítványokat) bocsátanak ki.

Azok a szervezetek működnek attribútum-tanúsítóként, amelyek jogosultak a végfelhasználók attribútumainak igazolására, és ismerik az adott attribútummal rendelkező végfelhasználók valamelyik nyilvános kulcsú aláírói tanúsítványának kriptográfiai lenyomatát (objectDigestInfo).

Az egyes attribútum-tanúsítók kizárólag saját hatáskörükben bocsátanak ki attribútum-tanúsítványokat, és kizárólag olyan attribútumokat igazolnak, amelyekkel kapcsolatban papíron is kiadhatnak igazolásokat.

Ha egy végfelhasználó valamelyik szerepkörében szeretné a nyilvános kulcsú aláírói tanúsítványát használni, akkor az adott szerepkörének igazolására jogosult attribútum-tanúsítóhoz fordul. Az attribútum-tanúsító online bocsátja ki az attribútum-tanúsítványt.

Az attribútum-tanúsítvány rövid élettartammal rendelkezik (pl. 10 percig érvényes), így nem kell vizsgálni a visszavonási állapotát. Ha egy felhasználótól megvonnak egy attribútumot, akkor az attribútum-tanúsító a visszavonást követően már nem ad ki tanúsítványt.

Ha egy felhasználó nyilvános kulcsú aláírói tanúsítványához tartozó magánkulcsa kompromittálódik, a hitelesítés szolgáltató visszavonja az aláírói tanúsítványt, így a nyilvános kulcsú aláírói tanúsítványhoz tartozó attribútum-tanúsítványok sem használhatóak többé.

4.1. A modell jellemzői

1. A végfelhasználóknak elég egyetlen nyilvános kulcsú aláírói tanúsítványt vásárolni, azt több célra is felhasználhatják.
2. A rendszer elosztott, decentralizált. A jogosultságok, szerepkörök (attribútumok) kezelését nem hitelesítés szolgáltató végzi, hanem a szerepkört, jogosultságot kezelő szervezet.
3. A rendszer nyitott, könnyű hozzá csatlakozni. Az attribútum-tanúsítványok érvényességét könnyű ellenőrizni.
4. A rendszer nem fogalmaz meg felesleges követelményeket az attribútum-tanúsítókra. Az igazolt attribútumok jellege, érzékenysége határozza meg, hogy az adott attribútum esetén milyen biztonsági követelmények (pl. [ETSI_ACPREQ]) indokoltak[13].
5. A rendszer skálázható, sok hitelesítés szolgáltató, sok attribútum-tanúsító, sok felhasználó és sok attribútum esetén is működőképes.

[13] Túl szigorú követelmények általános előírása költségessé teszi az attribútum-tanúsítványok elterjedt használatát.

6. A rendszer elveiben hasonlít a jelenleg működő, papír alapú ügyvitelhez.
7. A jelenlegi jogszabályi környezetnek megfelel.
8. A rendszer szereplői csak olyan információkhoz jutnak hozzá, amelyek kezelésére jogosultak. Az érintett fél csak olyan ismeretekhez jut az aláíró tulajdonságaival, attribútumaival kapcsolatban, amelyeket közvetlenül az aláíró juttat el neki.

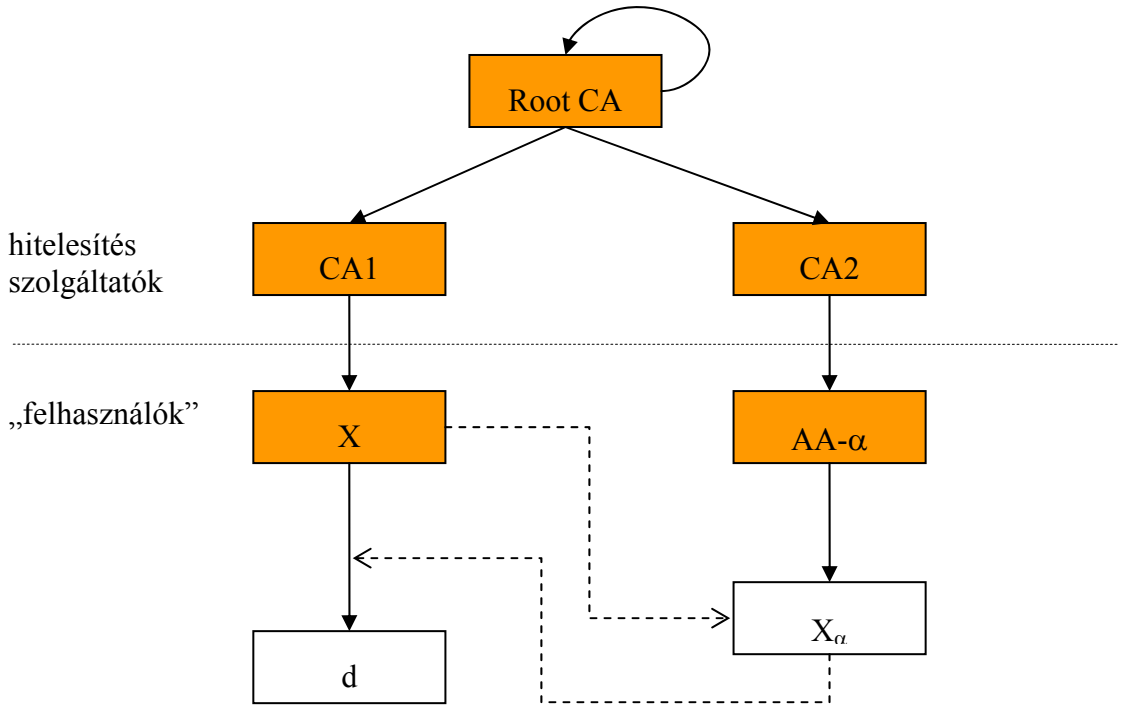
4.2. Végfelhasználók: aláírás létrehozása, ellenőrzése

A következők azt részletezik, hogy hogyan használhatóak az attribútum-tanúsítványok elektronikus aláírás létrehozására alkalmas nyilvános kulcsú aláírói tanúsítványok mellett.

Más célra szolgáló nyilvános kulcsú tanúsítványok esetében is ehhez hasonló megoldások alkalmazhatók.

Az ábrákon szereplő jelöléseket a 7. fejezet magyarázza meg.

4.2.1. Aláírás létrehozása



2. ábra: Az X felhasználó aláírja a d dokumentumot. Ez az aláírás tartalmazza az X felhasználó tanúsítványához kapcsolódó (annak lenyomatát tartalmazó) X_α attribútum tanúsítványt. Az attribútum tanúsítványban AA-α igazolja, hogy az X felhasználó rendelkezik az α szerepkörrel.

Tegyük fel, hogy X felhasználó az α szerepkörével szeretne aláírni egy dokumentumot. X rendelkezik egy nyilvános kulcsú aláírói tanúsítvánnyal, és AA-α (az α szerepkör igazolására jogosult attribútum szolgáltató) ismeri X ezen nyilvános kulcsú tanúsítványát.

Az eljárás lépései a következők:

1. X felhasználó üzenetet küld AA-α-nak, amelyben igazolást kér arról, hogy ő rendelkezik α szerepkörrel. (Ennek részleteit a 4.5. fejezet írja le.)
2. AA-α kiállítja az X_α igazolást (attribútum-tanúsítvány). Nyilvántartásában megnézni X tanúsítványát, és annak lenyomatát beleírja az X_α igazolásba. Az attribútum-tanúsítványt rövid távra (kb. 10 percre) állítja ki.
3. AA-α elküldi X_α-t X-nek.
4. Amikor X aláírja a d dokumentumot, egyúttal aláírja saját X aláírói tanúsítványát, és az X_α attribútum-tanúsítványt is.
5. X időbélyeget helyez el az elkészült aláíráson.

Példa: Dr. Gipsz Jakab ügyvédként szeretne ellenjegyezni egy dokumentumot, ehhez igazolnia kell, hogy ő ügyvéd. A Magyar Ügyvédi Kamarától ezért igazolást (attribútum-tanúsítványt) kér arról, hogy ő valóban ügyvéd, majd ezt az igazolást csatolja a [XAdES] aláírásához.

Megjegyzés:

- AA-α-nak nem kell vizsgálnia X aláírói tanúsítványának érvényességét. Visszavont, lejárt tanúsítványhoz is kiállíthat X_α attribútum-tanúsítványt, mert az attribútum-tanúsítvány (igazolás) érvényes aláírói tanúsítvány nélkül amúgy sem használható. [ETSI_ACPREQ]
- AA-α bárkinek elküldheti, az X_α attribútum-tanúsítványt, mivel azt úgyis csak az X tanúsítványhoz tartozó magánkulccsal lehet használni.

  AA-α egyébként kérheti a kérelmezőket arra, hogy azonosítsák magukat, mert:

  - nem szeretné, hogy akárki lekérdezze, hogy kik rendelkeznek α szerepkörrel,
  - védekezni kíván a szolgáltatás leterhelésére irányuló támadások ellen,
  - díjazáshoz kívánja kötni az attribútum-tanúsítványok kiállítását.
- Ha valakinek fontos, hogy különböző szerepkörben elkészített aláírásairól ne lehessen megállapítani, hogy ugyanaz a személy hozta őket létre, ezt az általunk körvonalazott modellben is meg tudja valósítani. Az X aláírói tanúsítvány alanya rendelkezhet további X' vagy X'' stb. aláírói tanúsítványokkal is, esetleg másik hitelesítés szolgáltatótól is beszerezheti azokat. Ezek az aláírói tanúsítványok más lenyomattal rendelkeznek, így az X_α attribútum-tanúsítvány nem használható velük. Ha X nem szeretné a δ szerepkörben ugyanazt a kártyát vagy magánkulcsot használni, beszerezhet egy X' aláírói tanúsítványt, és ehhez kérheti az X_δ' attribútum-tanúsítványt. Ekkor X aláírói tanúsítványát (és a hozzá tartozó magánkulcsot) α szerepkörben, X' aláírói tanúsítványát δ szerepkörben használhatja. Aki nem tudja, hogy X és X' aláírói tanúsítványok alanya megegyezik, nem tudja megállapítani, hogy X_α és X_δ' attribútum-tanúsítványok ugyanahhoz a személyhez tartoznak. Így nem tudja megállapítani, hogy e személy α és δ szerepkörrel is rendelkezik, és így nem tudja összekapcsolni az α és a δ szerepkörben létrehozott aláírásait sem.

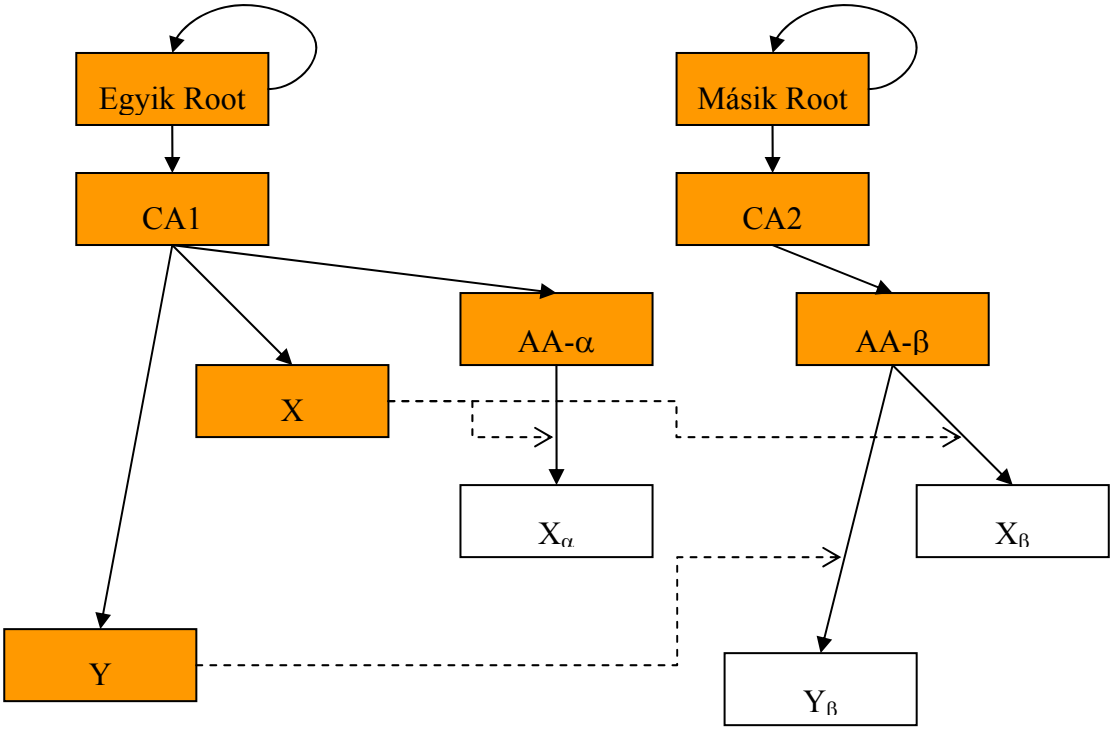
4.2.2. Egy érintett fél ellenőrzi az aláírást

Tegyük fel, hogy az Y érintett fél megkapja a fent létrehozott d dokumentumot, és ellenőrizni szeretné az aláírást, valamint meg szeretné állapítani, hogy az aláíró rendelkezik-e az α szerepkörrel.

A következőket kell tennie:

1. Ellenőrzi az aláírt d dokumentumon lévő időbélyeget, vagy más módon megállapítja, hogy X aláírása mikor készült. (Ennek lépéseit itt nem részletezzük.) [B2006elf]
2. Ellenőrzi, hogy X aláírása érvényes-e az aláírt (d, X, X_α) adatokon.
    a. Ellenőrzi, hogy az aláírás X aláírói tanúsítványához tartozó magánkulccsal készült-e.
    b. Visszavezeti X aláírói tanúsítványát valamely megbízható, és az adott célra elfogadott gyökér hitelesítés szolgáltatóra, azaz felépíti a tanúsítványláncot.
    c. Ellenőrzi a tanúsítványlánc minden elemének a visszavonási állapotát (kivéve a gyökértanúsítványét).
    d. Megvizsgálja, hogy az aláírás tartalmaz-e attribútum-tanúsítványt. Ekkor megtalálja X_α-t.
3. Ellenőrzi, hogy AA-α aláírása érvényes-e X_α-n. Ezen az ellenőrzést ahhoz hasonlóan végzi el, mint amikor X aláírását ellenőrizte.
    a. Ellenőrzi, hogy az aláírás az AA-α aláírói tanúsítványához tartozó magánkulccsal készült-e.
    b. Visszavezeti AA-α aláírói tanúsítványát valamely megbízható, és az adott célra elfogadott gyökér hitelesítés szolgáltatóra, azaz felépíti a tanúsítványláncot.
    c. Ellenőrzi a tanúsítványlánc minden elemének a visszavonási állapotát (kivéve a gyökértanúsítványét).
4. X_α rövid ideig érvényes, így nem kell ellenőriznie, hogy AA-α visszavonta-e X_α-t.
5. Ellenőrzi, hogy X_α érvényes volt-e (nem járt-e már le) az aláírás létrehozásának pillanatában.
6. Ellenőrzi, hogy AA-α jogosult-e az α szerepkör igazolására (lásd: 4.6. fejezet).

4.3. Elosztott rendszer



3. ábra: Az X felhasználó egyaránt rendelkezik α és β szerepkörrel, mindkét szerepkörében ugyanazt a tanúsítványt használja. Abból derül ki, hogy melyik szerepkörében ír alá, hogy X_α vagy X_β attribútum tanúsítványát csatolja az aláírásához. Az Y felhasználó csak β szerepkörrel rendelkezik.

A fenti ábra azt mutatja be, amikor több szerepkör is megjelenik a rendszerben. A felhasználóknak (alanyoknak) elég egyetlen tanúsítvánnyal rendelkezniük, ezt használhatják valamennyi szerepkörükben. Ugyanakkor, aki kívánja, megteheti, hogy különböző szerepköreiben más és más tanúsítványt és magánkulcsot használ.

A jelen dokumentumban körvonalazott rendszerben az [RFC3281] szerinti „push” modellt használjuk az attribútum-tanúsítványok továbbítására. E modell szerint az attribútum-tanúsítványok beszerzése az aláírói tanúsítvány alanyának feladata. Szintén az aláírói tanúsítvány alanya kell, hogy eljuttassa az attribútum-tanúsítványt az aláírást ellenőrző érintett félnek. (Mindez úgy zajlik le, hogy az attribútum-tanúsítvány az aláírt elemek közé kerül.)

A „push” modell előnye, hogy az érintett félnek nem kell kapcsolatba kerülnie AA-α-val, nem kell ismernie AA-α elérhetőségét, és nem kell adatokat (attribútum-tanúsítványokat) lekérdeznie az egyes AA-któl. Így az érintett fél kizárólag azon információkhoz jut hozzá, amelyeket az aláírói tanúsítvány alanya a rendelkezésére bocsát. Így nem jelentkeznek olyan problémák, hogy mely érintett fél jogosult lekérdezni az egyes felhasználók α, β, χ stb. attribútum tanúsítványait, és így nem kezelni a felhasználók adott attribútumaival kapcsolatos adatait.

4.4. Az attribútum-tanúsítók

4.4.1. Ki tanúsíthat attribútumot?

Az attribútum-tanúsítók – a PKI közösség szempontjából – olyan végfelhasználók, akik elektronikus aláírással látják el az online kibocsátott rövid élettartamú attribútum-tanúsítványokat[14]. Az attribútum-tanúsítványokon jellemzően automata segítségével helyeznek el **fokozott biztonságú elektronikus aláírást**.

Az általunk körvonalazott modellben az, aki az attribútum kiosztására jogosult (AGA) és az, aki az attribútum-tanúsítványt kibocsátja (AA) ugyanaz a szereplő.

Bármelyik végfelhasználó felléphet attribútum-tanúsítóként, pontosan ugyanolyan jogosultságot, felhatalmazást (igazolást) adhat ki elektronikusan, mint amilyet papíron, kézzel írott aláírással is kiadhat. Aki elektronikusan olyan szerepköröket, jogosultságokat igazol, amelyekre nincs meg a megfelelő felhatalmazása, pontosan olyan következményekkel számolhat, mintha azt papír alapon adta volna ki.

Az [ETSI_ACREQ] szellemében a végfelhasználó saját attribútumairól is nyilatkozhat „claimed role”-t tartalmazó attribútum-tanúsítvány formájában.

Az attribútum-tanúsító egy kulccsal több szerepkört is igazolhat.

4.4.2. Hogyan történik az attribútum-tanúsítvány kibocsátása?

AA-α nyilvántartásba veszi azoknak a felhasználóknak az aláírói tanúsítványát[15], akik rendelkeznek az α attribútummal.

AA-α-nak csak a saját nyilvántartását kell megnéznie; azt kell ellenőriznie, hogy az X tanúsítvány alanyához valóban tartozik-e az α szerepkör. Ha igen, kiadhatja a tanúsítványt. Ha X már nem rendelkezik α szerepkörrel, AA-α nem ad ki több X_α attribútum-tanúsítványt. Más teendője ezen kívül nincs[16].

4.4.3. Attribútum-tanúsítványok visszavonásának közzététele

Az attribútum szolgáltató „rövid” lejáratú attribútum-tanúsítványokat ad ki. Az attribútum-tanúsítványok élettartama olyan rövid, hogy nem szükséges, illetve nincs értelme a rájuk vonatkozó attribútum-visszavonási listát közzétenni[17].

Jelen dokumentumban a 10 perces attribútum-tanúsítvány élettartamot javasoljuk, de egyes esetekben ennél hosszabb élettartam is elég rövid lehet. Például, ha egy AGA-υ működéséből adódóan csak hetente egyszer születhet olyan döntés, amely a υ attribútumot személyekhez rendeli (és esetleg megfoszt valakit a υ attribútumától), akkor nem sok értelme van egy hétnél rövidebb élettartamú attribútum tanúsítványokat kibocsátani. AA-α felelőssége olyan rövid lejáratot meghatározni, amely az adott attribútummal kapcsolatban minimalizálja a visszaélés kockázatát, egyúttal használható szolgáltatást eredményez.

---

[14] Az attribútum-tanúsítványok elektronikus aláírással aláírt igazolások

[15] A tanúsítvány lenyomatát is elegendő nyilvántartásba venni.

[16] AA-α-nak nem kell vizsgálnia a nyilvános kulcsú tanúsítvány lejártát, visszavonási állapotát.[ETSI_ACPREQ]

[17] OCSP válaszadó tanúsítványokkal kapcsolatban terjedt el ehhez hasonló gyakorlat. [OCSP10p]

AA-α az [RFC3281, 4.3.6] szerinti szabványos módon jelöli, hogy az adott attribútum tanúsítvánnyal kapcsolatban nincs elérhető visszavonási információ.

4.4.4. Biztonság

Egy attribútum-tanúsítónak olyan fizikai, logikai és szabályozási biztonságot kell megvalósítania, amely az adott attribútumhoz indokolt. Például, valamely cég képviseletére vonatkozó jogosultság érzékeny attribútum, ahol erős biztonsági követelmények alkalmazása is indokolt. Ezzel szemben, egy evezősklub-tagság kevésbé érzékeny attribútum, ahol felesleges szigorú követelményeket támasztani.

AA-α (vagy AGA-α) dönt arról, hogy az α attribútum mennyire érzékeny, és hogyan állapítja azt meg, hogy az X felhasználó valóban rendelkezik-e a kérdéses attribútummal. Ő dönti el, hogy milyen adatbázisok adataira támaszkodik, találkozik-e személyesen X-szel, és miként bizonyosodik meg arról, hogy X valóban birtokában van az aláírói tanúsítványához tartozó magánkulcsnak. AA-α felel az általa kibocsátott igazolásokért is.

Az attribútum-tanúsító végfelhasználók sok helyen a magánkulcsot – a hitelesítés szolgáltatóknál megszokotthoz képest – gyenge biztonsági környezetben őrzik, így mindenképpen biztosítani kell az attribútum-tanúsítók aláírói tanúsítványainak felfüggesztési, illetve visszavonási lehetőségét.

Nagyobb szervezetek várhatóan szabályozni fogják, hogy az általuk tanúsítható attribútumokat milyen módon lehet tanúsítani, és saját szervezetükön belül követelményeket fognak megfogalmazni attribútum-tanúsítóik működésére.

4.4.5. Felelősség

AA-α felelős az általa aláírt attribútum-tanúsítványokért, mint ahogy az X felhasználó is felelős az általa aláírt dokumentumokért, nyilatkozatokért.

4.4.6. Hogyan jelenik meg az attribútum az attribútum-tanúsítványban?

Az attribútumokat az X.509, az [ETSI_ACREQ] és az [RFC3281] által meghatározott szintaxis szerint tüntethetjük fel az attribútum-tanúsítványban. Az attribútumokat célszerű olyan módon jelölni, hogy azokat automaták segítségével is fel lehessen dolgozni. Így célszerű őket URI vagy OID segítségével jelölni. Ugyanakkor előnyös, ha az attribútumok szövegesen is megjelenjenek az attribútum-tanúsítványban, így akkor is fel lehet dolgozni azokat, ha a feldolgozó által használt alkalmazás nem tudja értelmezni az adott URI-t vagy OID-et.

Azt javasoljuk, hogy az attribútum-tanúsítvány mindkét módon tartalmazza az attribútumot. Ilyenkor az attribútum-tanúsító felelőssége, hogy a szöveges és az automaták által feldolgozható megjelölés konzisztens legyen, és ne lehessen az attribútumot kétféleképpen értelmezni.

Az [ETSI_ACREQ] specifikáció javaslatot tesz a szerepköröket jelentő attribútumok feltüntetésére.

A cég képviseleti jogosultságot jelentő szerepkör feltüntetésére a **Hiba! A hivatkozási forrás nem található.**. fejezet mutat példát.

4.5. Hogyan szerzi be a felhasználó az attribútum-tanúsítványt?

4.5.1. Az attribútum-tanúsító címe

Az alany tudja, hogy milyen attribútumokkal rendelkezik, és minden α attribútumához ismeri azt az URL-t, amelyről AA-α-tól tanúsítványt kérhet.

4.5.2. Protokoll az attribútum-tanúsítvány beszerzésére

- Az attribútum-tanúsítványt HTTPS kapcsolaton keresztül kell letölteni. A HTTPS szervere SSL tanúsítvány segítségével azonosítja magát, amit a kliens ellenőriz.
- AA dönti el, hogy a kliensnek kell-e azonosítani magát. AA vagy tanúsítvány-alapú, vagy basic (felhasználónév és jelszó alapú) authentikációt írhat elő a kliens számára.
- A kliens elküldi az attribútum-tanúsítvány kérelmet AA-nak. A kérelemnek kell tartalmaznia az alany nyilvános kulcsú tanúsítványának lenyomatát, a használt lenyomatképzési algoritmus megnevezését, és annak az attribútumnak vagy attribútumoknak a megnevezését is, amelyekre attribútum-tanúsítványt kér.
- AA megvizsgálja, hogy a kliens rendelkezik-e a kívánt attribútumokkal, és AA jogosult-e ezeknek az attribútumoknak a tanúsítására. Ha igen, AA elkészíti a rövid lejáratú attribútum-tanúsítványt.
- AA elküldi az attribútum-tanúsítványt a kliensnek a HTTPS kapcsolaton keresztül.
- A kliens ellenőrzi az attribútum-tanúsítványt, és ellenőrzi, hogy valóban azok az attribútumok szerepelnek-e benne, amelyeket kért.

Ezt az eljárást a felhasználó aláírás-létrehozó alkalmazása végzi el, az emberi felhasználó mindebből annyit érzékel, hogy egy listából ki kell választania, hogy éppen milyen szerepkörben szeretne aláírni.

4.6. Hogyan ellenőrzi az érintett fél, hogy ki milyen attribútumot jogosult tanúsítani?

A 3.1. és 3.2. fejezetekben leírt gondolatmenet szerint, az attribútum-tanúsító végfelhasználó (az Eat. terminológiája szerint „aláíró”), aki legalább fokozott biztonságú elektronikus aláírással lát el elektronikus dokumentumokat, és a dokumentumokban igazolásokat bocsát ki az egyes aláírói tanúsítványok alanyainak attribútumaival kapcsolatban. Jogi szempontból nincsen kitüntetett szerepe, műszaki szempontból pedig csak elektronikus aláírás létrehozására alkalmas tanúsítvánnyal kell rendelkeznie.

Az [RFC3281] szerint a befogadónak közvetlenül meg kell bíznia AA tanúsítványában. Ez a gondolat szintén TTP-jellegű AA-t tételez fel.

```
5. Attribute Certificate Validation
[...]
   4. The AC issuer MUST be directly trusted as an AC issuer (by
      configuration or otherwise).
```

Nem tudunk olyan szabványos lehetőségről, amely szerint egy aláírói tanúsítványban feltüntethetnénk, hogy az egy attribútum-tanúsító aláírói tanúsítványa. Amennyiben lenne is ilyen lehetőség, ez is legfeljebb általános célú, TTP-jellegű attribútum tanúsító megjelölésére lenne alkalmas. Olyan modellben, ahol sok attribútum-tanúsító van jelen, de egy-egy tanúsító

csak egy-egy szerepkört jogosult tanúsítani, azt kellene megjelölni az attribútum-tanúsító aláírói tanúsítványában, hogy az adott attribútum-tanúsító mely attribútumokkal kapcsolatban jogosult attribútumokat kibocsátani.

A fentiek alapján az attribútum-tanúsító tanúsítványát „közönséges" aláírói tanúsítványnak kell tekinteni, és az attribútum-tanúsító aláírását ennek megfelelően kell ellenőrizni. A következő két megoldást javasoljuk annak eldöntésére, hogy egy attribútum-tanúsító jogosult-e egy adott attribútumot tanúsítani:

- **Ha automata dönt, vagy a papír alapú rendszereknél jelentősen magasabb szintű biztonságot követelünk meg, akkor kizárólag az ismert tanúsítvánnyal rendelkező attribútum-tanúsítókat szabad elfogadni**.

  Ekkor jellemzően nagy mennyiségű aláírásról, attribútum-tanúsítványról kell dönteni, és az attribútum-tanúsítványok az attribútum-tanúsítók zárt halmazától származnak. Az [RFC3281] szerint közvetlenül meg kell bízni az attribútum-tanúsítókban, tehát nyilvántartást kell vezetni az egyes attribútumok tanúsítására jogosult attribútum-tanúsítók aláírói tanúsítványairól.

  Például, kizárólag ügyvédek, közjegyzők, és jogtanácsosok küldhetnek be a cégbíróságra elektronikus cégbejegyzési kérelmet. A cégbejegyzési kérelmeket befogadó automaták elég, ha e három attribútumot (szerepkört) ismerik, mert csak ezeket kell ellenőrizniük. Ha az ellenőrzés attribútum-tanúsítvány alapján történik, az automatáknak az AA-ügyvéd, AA-közjegyző és AA-jogtanácsos aláírói tanúsítványokat kell ismerniük. Így az „ügyvéd" szerepkör tanúsítását kizárólag az AA-ügyvéd attribútum-tanúsítótól fogadják el, stb.

- **Ha ember dönt, a papíron alkalmazott eljáráshoz hasonlóan kell eljárni, és az attribútum-tanúsító nevéből kell megállapítani, hogy az jogosult-e egy adott attribútum tanúsítására**.

  Papír alapú ügyintézés során az emberi ügyintézők – megfelelő képzés, vagy csak „józan ész" alapján – az igazolást kibocsátó neve alapján döntik el, hogy az jogosult-e egy adott igazolást kibocsátani. Amennyiben kétség merül fel, a papír alapú rendszerekben már kialakult szabályok vannak, hogy hogyan kell a megfelelő bizonyítékokat beszerezni.

  Például elfogadjuk, ha „Budapesti Műszaki és Gazdaságtudományi Egyetem" igazolja, hogy Gipsz Jakab „okleveles villamosmérnök". Azt is elfogadjuk, ha a „Fővárosi Cégbíróság" igazolja, hogy Gipsz Jakab jogosult a „Kókler Bt-t" képviselni. Ezzel szemben, rögtön kétség merül, ha ezeket az igazolásokat „Nagy Zebulon" magánszemély bocsátja ki.

  A megoldás előnyös tulajdonsága, hogy nem kell nyilvántartást vezetni az elfogadott attribútum-tanúsítók aláírói tanúsítványairól. Nem kell foglalkozni azzal sem, ha az attribútum-tanúsítók aláírói tanúsítványai megváltoznak, vagy új attribútum-tanúsító jelenik meg.

  Egyedül az álneves tanúsítványok (amelyek nem az alany valódi nevét tartalmazzák) jelenthetnek problémát: álneves tanúsítvány esetén az attribútum-tanúsító megnevezéséből (DN) nem következtethetünk annak kilétére.

  Megoldásunkban ezért nem fogadhatunk el olyan attribútum-tanúsítókat, amelyek álneves tanúsítvánnyal rendelkeznek. Az Eat. szerint egyértelműen jelölni kell egy tanúsítványban, ha az álnevet tartalmaz, így e probléma kivédhető.

4.7. A hitelesítés szolgáltatók szerepe a modellben

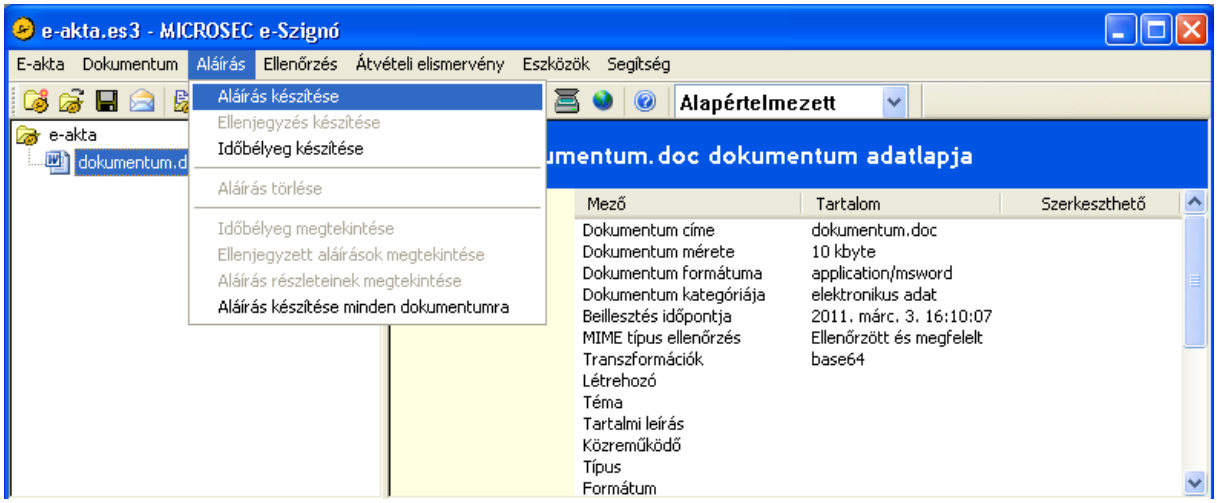
A modell nem érinti a hitelesítés szolgáltatókat, nem támaszt követelményeket velük szemben. A hitelesítés szolgáltatóknak továbbra is aláírói tanúsítványokat kell kibocsátani, ahogyan ezt most is teszik. Várhatóan csökken a nyilvános kulcsú aláírói tanúsítványokban szereplő attribútumok jelentősége, és e tanúsítványok az alany nevén kívül – hasonlóan a kézzel írott aláíráshoz – a jövőben mást már nem fognak tartalmazni[18].

Ha egy nyilvános kulcsú aláírói tanúsítványt több célra, több szerepkörben is fel lehet használni, akkor várhatóan többen találják majd gazdaságosnak a nyilvános kulcsú infrastruktúra használatát, így mindez elősegíti majd az elektronikus aláírásra szolgáló nyilvános kulcsú tanúsítványok terjedését.

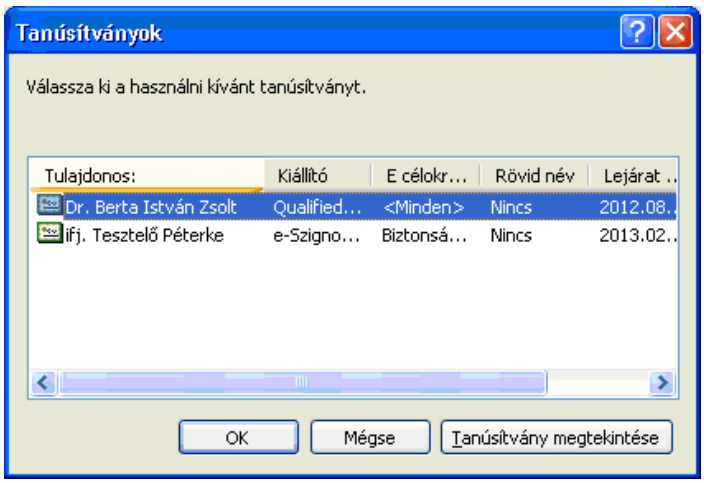
E modellben semmilyen megkötést nem támasztunk az aláírói tanúsítványokra nézve, mert lenyomat alapján hivatkozunk rájuk, így modellünkben valamennyi hitelesítés szolgáltató tanúsítványa használható.

5. Attribútum tanúsítványok használata a gyakorlatban

Válasszuk ki, hogy melyik dokumentumot szeretnénk aláírni!

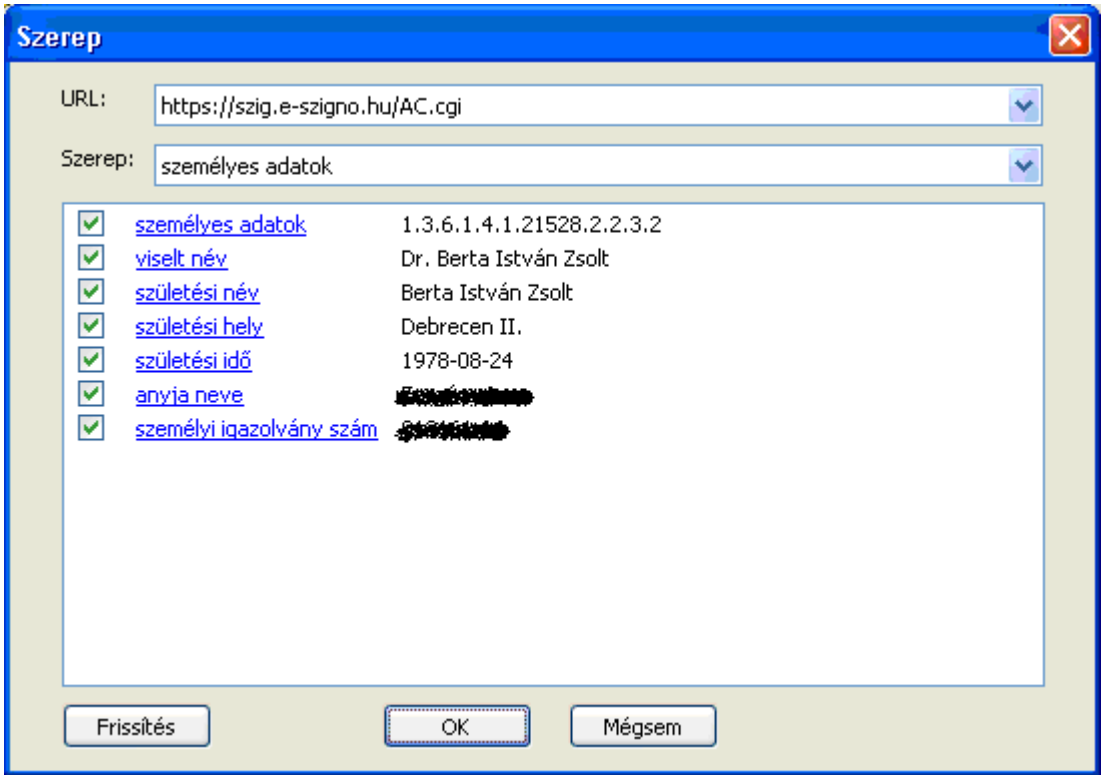


Válasszuk ki a tanúsítványunkat!

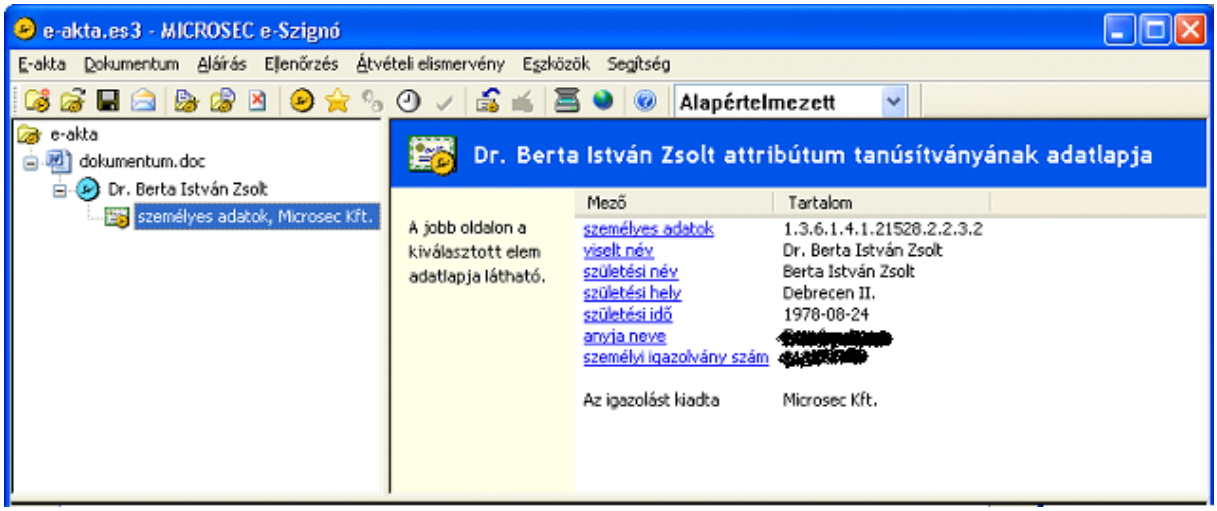


[18] Tartalmazhatnak még egy-két kötelező elemet (pl. „HU”), illetve a DN egyediségét biztosító számot vagy megkülönböztetést.

Az aláírás-létrehozó alkalmazás lekérdezi a beállított attribútum-tanúsítótól, hogy milyen attribútumokat szeretnénk, ha igazolna. Az alábbi példában az attribútum-tanúsító megegyezik a hitelesítés szolgáltatóval, akitől az aláíró személyes adatainak igazolását kérjük.



Az aláírás-létrehozó alkalmazás lekéri az attribútum tanúsítványt, majd az aláíráshoz szükséges PIN kód begépelését követően létrejön az aláírás, és megtekinthetjük a csatolt attribútum-tanúsítványt.



6. Hivatkozások

[RFC3281] RFC 3281 – An Internet Attribute Certificate Profile for Authorization

[RFC5280] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[XAdES] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES)

[ETSI_ACPREQ] ETSI TS 102 158 – Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates

[ETSI_ACREQ] ETSI TR 102 044 – Electronic Signatures and Infrastructures (ESI); Requirements for role and attribute certificates

[Eat] 2001. évi XXXV. törvény az elektronikus aláírásról

[OCSP10p] Berta István Zsolt, Endrődi Csilla Éva, Vanczák Gergely – Miért fontos a rövid lejáratú OCSP válaszadó tanúsítvány? http://www.e-szigno.hu/wp_ocsp_10perc.html

[PKIX_ACRMF] Attribute Certificate Request Message Format, PKIX Working Group Internet Draft http://tools.ietf.org/html/draft-ietf-pkix-acrmf-01

[ETSI_ALGO] ETSI TS 102 176-1 – Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

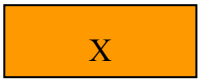
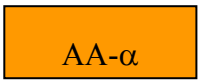
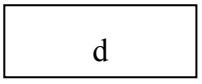
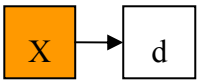
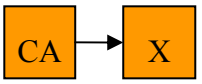
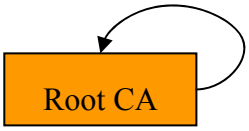
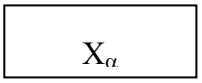
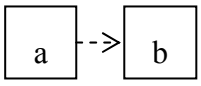
[CTV] 2006. évi V. törvény a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról

[B2006elf] Berta István Zsolt – Mi alapján fogadhatunk el egy elektronikus aláírást? (How to accept an electronic signature?) Híradástechnika, 2006, vol. LXI, 2006, in Hungarian, 2006.

http://www.e-szigno.hu/anyagok/Berta2006eaelf.pdf

[JBT] 2007. évi LXIV. törvény a jogügyletek biztonságának érdekében szükséges törvénymódosításokról

7. Jelölések

X, Y, Z, CA, CA2	Az „X”, „Y”, „Z”, illetve „CA” és „CA2” elnevezésű személyek, szervezetek
α, β, χ, δ, ...	Szerepkörök, jogosultságok.
	Az „X” nevű személy vagy szervezet, illetve annak tanúsítványa
	Az a felhasználó / attribútum-tanúsító, aki az α attribútum igazolására jogosult
	A „d” elnevezésű bitsorozat, amely lehet például elektronikus dokumentum.
	„X” a tanúsítványához tartozó magánkulccsal aláírja a „d” elektronikus dokumentumot. A nyíl az aláírást, mint bitsorozatot jelenti.
	A „CA” hitelesítés szolgáltató az „X” felhasználó tanúsítványát írja alá. A nyíl a tanúsítványt, mint bitsorozatot jelenti.
	Root CA nevű szervezet, aki a saját tanúsítványát írja alá. A nyíl jelenti az önhitelesített gyökértanúsítványt.
	Állítás, miszerint az „X” felhasználó az α szerepkörrel rendelkezik, vagy rendelkezett. Az attribútum tanúsítvány is egy ilyen állítás.
	A „b” bitsorozat/dokumentum tartalmazza az „a” bitsorozatot/dokumentumot vagy annak kriptográfiai lenyomatát.