

Hosszútávú hiteles archiválás elektronikus aláírás segítségével

Krasznay Csaba
BME Informatikai Központ
krasznay@ik.bme.hu

Bevezetés

Előadásom célja az elektronikus archiválás szempontjából „megfelelő” alkalmazás bemutatása. Ennek megválaszolásához először egy szabályozott környezetet kell létrehozni. Az elektronikus aláírás használatát rengeteg jogszabály keretei között kell kidolgozni. Jelen előadásban a viszonylag egyszerűbb irányt választottam, az üzletfelek közötti (B2B), valamint a munkatársak közötti kapcsolattartást kívánjuk elektronikus alapokra helyezni.

Ennek érdekében először ki kell dolgozni egy elektronikus aláírás szabályzatot. Ebben először meghatározzuk a tipikus (mű)egyetemi szervezet által használt dokumentumok körét. Ez már önmagában komoly feladat, hiszen mindezt a meglehetősen általánosan megfogalmazott egyetemi iratkezelési szabályzat árnyékában kellett megtenni.

A második lépésben össze kellett foglalni az iratkezelés szabályait. Ez tipikusan papíralapú ügyintézésre van kitalálva. Foglalkozni kellett tehát az elektronikus iratmozgással is. Ezért a szabályzatban az elektronikus levelezésre vonatkozó előírások is bekerültek, mely röviden és mindenki számára érthetően próbálja meghatározni az elektronikus levelezés során megkövetelt szabályokat.

Csak ezután kerülhetett sor az elektronikus aláírás használatának szabályozására. Ehhez először röviden vázoltuk a jelenleg rendelkezésre álló eszközökből és szolgáltatásokból eredő lehetőségeket, majd az iratok köréhez rendeltük azt, hogy mikor lehet elektronikus iratot létrehozni, ki írhatja alá elektronikusan az iratot és milyen peremfeltételek mellett. Ez gyakorlatilag a jelenlegi szabályok és szokások átfordítása az elektronikus világra.

Az utolsó fejezet az elektronikus aláírás legkritikusabb kérdésére próbál szabályozást adni. Ez az archiválás problémája. A szabályozás során figyelembe vettük a jelenlegi technológiai és jogi lehetőségeket, illetve (sajnos jelentősebb számú) hátrányokat. Az archiválást ezért csak viszonylag rövid ideig érvényes iratokra kívántuk kiterjeszteni, nyitva hagyva a további szabályozást a megfelelő feltételek megteremtésének időpontjára.

A dokumentum annak ellenére, hogy egy az egyben használható egyetemi környezetben, inkább egy hiánypótló sablonnak tekintendő. Célja, hogy megkönnyítse az elektronizálás, a „papírmentes iroda” bevezetését mindazoknál, akik ódzkodnak ettől a technológiától.

Elektronikus aláírási szabályzat

Fogalmak, általános rendelkezések

Ez a dokumentum szabályozza az Egyetemi Szervezetben belül keletkezett elektronikus iratok elektronikus aláírásának rendjét és használati szabályait. A Szabályzat érvényes a Szervezet minden dolgozójára, illetve mindazon partnerekre, akik szerződésben vállalják a Szervezettel való hiteles elektronikus kapcsolattartást.

A Szabályzat rendelkezései támaszkodnak az **1995. évi LXVI törvényre**, mely a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szól, a **2001. évi XXXV törvényre** és annak módosítására, melyek az elektronikus aláírásról szólnak, valamint a Budapesti Műszaki és Gazdaságtudományi Egyetem **Iratkezelési Szabályzatára**.

Irat minden olyan szöveg, számadatsor, térkép, tervrajz és vázlat - a megjelentetés szándékával készült könyv jellegű kézirat kivételével -, amely valamely szerv működésével, illetőleg személy tevékenységével kapcsolatban bármilyen anyagon, alakban, bármely eszköz felhasználásával és bármely eljárással keletkezett. Elektronikus irat minden olyan irat, mely számítógép által feldolgozható formában áll rendelkezésre.

Ügyirat a szerv rendeltetésszerű működése, illetve ügyintézése során keletkező irat, amely az ügy valamennyi ügyintézési fázisában keletkezett ügyiratdarabokat tartalmazza.

Ügyiratdarab az ügyiratnak az a része, amely az ügy intézésének valamely, egy-egy fázisában keletkezett iratokat tartalmazza.

Kiadmány a jóváhagyás után letisztázott és a kiadmányozásra jogosult részéről hiteles aláírással ellátott, lepecsételt irat.

Az iratok az alábbi pontok szerint sorolhatók csoportokba:

1. Kimenő számla
 - a. Külső partnernek
2. Kifizetés engedélyezése bejövő számla vagy egyéb dokumentum alapján
 - a. Belső munkatársnak
 - b. Egyetemi partnernek
 - c. Külső partnernek
3. Bejövő teljesítési igazolás attól a partnertől, akinek a munka készült
 - a. Külső partnertől
4. Kimenő teljesítési igazolás annak a partnernek, aki a munkát végezte
 - a. Egyetemi partnerek
 - b. Külső partnerek
5. Bejövő levél, pályázat, elkészült munka, előterjesztés, javaslat, jegyzőkönyv, stb. érkeztetése
 - a. Belső munkatárstól
 - b. Egyetemi partnertől
 - c. Külső partnertől
6. Kimenő levél, pályázat, elkészült munka, előterjesztés, javaslat, jegyzőkönyv, stb.
 - a. Belső munkatársnak
 - b. Egyetemi partnernek

- c. Külső partnernek
- 7. Bejövő vagy kimenő árajánlat
 - a. Egyetemi partnertől
 - b. Külső partnertől
- 8. Szerződés
 - a. Belső munkatárssal
 - b. Egyetemi partnerrel
 - c. Külső partnerrel
- 9. Rendelés
 - a. Külső partnertől
- 10. Kinevezés
 - a. Belső munkatársat
- 11. Igazgatói utasítások
 - a. Belső munkatársak felé

A fenti csoportosításban a **belső munkatárs** megnevezés alatt minden olyan személyt kell érteni, aki az Egyetemi Szervezet alkalmazásában áll. **Egyetemi partner** minden olyan egyén vagy szervezet, aki a Budapesti Műszaki és Gazdaságtudományi Egyetem szervezeti keretein belül működik. **Külső partner** minden olyan szervezet illetve személy, aki a Budapesti Műszaki és Gazdaságtudományi Egyetem keretein kívül működik.

Ügyiratkezelés

Az iratkezelés feladata az irat készítése, az irat átvétele, vagy elektronikus úton történő fogadása, iktatása, használatra bocsátása, nyilvántartása, továbbítása, rendszerezése, a selejtezhetőség szempontjából történő válogatása, segédletekkel való ellátása, szakszerű és biztonságos őrzése, selejtezése, illetve levéltári őrizetbe adása.

A beérkező postai, kézbesítő által személyesen átadott és elektronikus küldemények közül

- az Igazgató nevére szóló iratokat az Igazgató által megbízott dolgozó bontja fel, majd az Igazgató szignálja,
- a Szervezet nevére érkező küldeményeket a Titkárságvezető bontja fel és szignálja,
- az egyes munkacsoportokhoz, projektekhez címzetten érkező postát a munkacsoport vezetői vagy a projektvezetők bontják, szignálják és a titkárságra továbbítják az iratokat iktatásra.

Elektronikus úton érkező levél a Titkárságra, a projektek elektronikus levél címeire vagy a munkatársak névre szóló elektronikus postaládájába. A Titkárságra érkező elektronikus leveleket tovább kell küldeni az illetékesnek, utána archiválni kell. A projektek elektronikus levelezését a projektdokumentációval együtt kell tárolni, melyet a projektvezető szignál. A munkatársak elektronikus postafiókjába érkező levelek közül azokat, melyek valamilyen formában projektet érintenek, vagy kapcsolatban vannak a Szervezettel, a munkatársnak aláírással kell ellátnia, és a projektdokumentációba vagy a Titkárságnál archiválnia kell.

A beérkező, illetve a helyben keletkező (hivatalból kezdeményezett, intézkedést igénylő) ügyiratokat iktatni kell. Iktatni kell az elektronikus rendszeren kapott vagy küldött iratokat is. Az elektronikus levelezésen keresztül érkező vagy küldött iratok iktatása a Titkárságon vagy a projektdokumentációban történik, legfeljebb egy nappal az irat kézhezvétele után. Az elektronikus formában létező irat iktatási rendje megegyezik a hagyományos, papíralapú iratokéval.

Az elektronikus aláírás szabályai

Az Elektronikus Aláírás Törvény szerint „elektronikus aláírás, illetve dokumentum elfogadását – beleértve a bizonyítási eszközként történő alkalmazást – megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni nem lehet kizárólag amiatt, hogy az aláírás, illetve dokumentum elektronikus formában létezik.”. A törvény szellemének megfelelően a Szervezet törekszik a papírmentes ügyintézés bevezetésére, tehát ésszerű korlátok között a lehető legtöbb iratát elektronikus formában előállítani, hitelesíteni, közlekedtetni és tárolni.

Egyes családjogi eseteken, bírósági eljárásokon (bizonyítékként való felhasználáson kívül), valamint az engedélyezettéken kívüli államigazgatási eljárásokon túlmenően mindenhol, ahol a jogszabály írásba foglalást ír elő, az elektronikus aláírás felhasználható, amennyiben az elektronikus iratot legalább fokozott biztonságú elektronikus aláírással látták el. Ha az elektronikusan aláírt elektronikus dokumentumon minősített elektronikus aláírás szerepel és az aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott. A fokozott biztonságú, illetve minősített elektronikus aláírással ellátott elektronikusan aláírt elektronikus dokumentum kinyomtatott változatához azonban nem fűződnek az ugyanezen dokumentum elektronikus változatának bizonyító ereje tekintetében előírt szabályok.

A hitelesítés érdekében a Szervezet munkatársai fokozott biztonságú személyes elektronikus tanúsítvánnyal rendelkeznek, az Igazgató és az Igazgató-helyettesek, valamint a projektvezetők minősített személyes elektronikus tanúsítvánnyal, az Igazgató és az Igazgató-helyettesek ezen felül minősített szervezeti tanúsítvánnyal. A tanúsítványokhoz kapcsolódó felhasználói szerződés szerint az elektronikus aláírásokkal ellátott iratok esetén a következő értékekig vállal felelősséget a hitelesítés-szolgáltató:

- fokozott biztonságú személyes tanúsítvány: 0 Ft,
- minősített személyes tanúsítvány: 50.000 Ft,
- minősített szervezeti tanúsítvány: 5.000.000 Ft.

Elektronikus aláírással emiatt csak a fenti értékhatárokig lehet elektronikus iratokat hitelesíteni. Amennyiben az elektronikus aláírás használatával kapcsolatba hozható káresemény történik, a hitelesítés-szolgáltató Általános Szerződési Feltételeinek és a Hitelesítés-szolgáltatási Szabályzatnak megfelelően kell a kártérítési igényt kezelni.

Az irattípusok közül az alábbiak láthatók el elektronikus aláírással, a feltételek teljesítése mellett:

1. Kimenő számla

- a. Külső partnernek: hosszú távú cél az elektronikus számlázás bevezetése, mely az **Igazgató** vagy az **Igazgató-helyettesek** együttes **minősített szervezeti tanúsítványával**, valamint a **Projektvezető minősített személyes tanúsítványával** kell hitelesíteni, **időbélyegző** felhasználásával, maximum **5.000.000 Ft** értékig. Az elektronikus számlázás a külső partner előzetes, írásos beleegyezésével történhet meg. Amennyiben a külső partner nem egyezik bele az elektronikus számla fogadásába, a számla értéke több mint 5.000.000 forint, illetve az Egyetem Gazdasági Osztálya nem készült fel az

elektronikus számla fogadására, az **Igazgató** vagy a két **Igazgató-helyettes** együttesen, a **Projektvezetővel** együtt szignálhatja a számlát.

2. Kifizetés engedélyezése bejövő számla vagy egyéb dokumentum alapján
 - a. Belső munkatársnak: a Szervezet nem függetlenedhet az Egyetem Gazdasági Osztályától, ezért a belső munkatársnak történő kifizetések engedélyezése egészen addig papíralapú marad, ameddig az Egyetem nem készül fel a hiteles elektronikus ügyintézésre. A kifizetéseket az **Igazgató** vagy a két **Igazgató-helyettes**, valamint a **Projektvezető** együttes aláírással engedélyezheti.
 - b. Egyetemi partnernek: a Szervezet ebben az esetben is az Egyetem Gazdasági Osztályától függ, így az elektronikus ügyintézés csak az Egyetemmel párhuzamosan vezethető be. A kifizetéseket az **Igazgató** vagy a két **Igazgató-helyettes**, valamint a **Projektvezető** együttes aláírással engedélyezheti.
 - c. Külső partnernek: a külső partnerekkel való szerződések megkötésekor törekedni kell arra, hogy a szerződési feltételek közé fel lehessen venni az elektronikus kapcsolattartást is, amennyiben a szerződő fél erre felkészült. Ekkor a külső partnertől érkező elektronikus számlát az **Igazgató** vagy a két **Igazgató-helyettes**, illetve a **Projektvezető** együttes **minősített személyes tanúsítványával** ellátott elektronikus aláírása után lehet elfogadni, amennyiben a számla összege nem magasabb az aláíró tanúsítványához kapcsolódó felelősségvállalás mértékénél. Papíralapú számla esetben az **Igazgató** vagy a két **Igazgató-helyettes**, illetve a **Projektvezető** együttes aláírással engedélyezhet egy kifizetést. Mindaddig papíralapú számlázást kell használni, ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus számla fogadására.
3. Bejövő teljesítési igazolás attól a partnertől, akinek a munka készült
 - a. Külső partnertől: a külső partnerekkel való szerződések megkötésekor törekedni kell arra, hogy a szerződési feltételek közé fel lehessen venni az elektronikus kapcsolattartást is, amennyiben a szerződő fél erre felkészült. Ebben az esetben a teljesítési igazolást a megbízó elektronikus aláírással ellátva küldi át a Szervezetnek. Az **Igazgató** vagy a két **Igazgató-helyettes minősített személyes tanúsítvány** felhasználásával veszi tudomásul az abban foglaltakat. Egyéb esetben az **Igazgató** vagy a két **Igazgató-helyettes** együttes aláírásával láttatja az igazolást. Ez a megoldás az Egyetem Gazdasági Osztályának felkészüléséig kötelező.
4. Kimenő teljesítési igazolás annak a partnernek, aki a munkát végezte
 - a. Egyetemi partnerek: az egyetemi partnerek felé a teljesítési igazolást előzetes beleegyezés esetén lehet elektronikusan kiadni. Ekkor a **projektvezető minősített személyes tanúsítványa** kell, hogy szerepeljen az elektronikus aláírásban, valamint egy **időbélyegző**. Papíralapú igazolásnál a **Projektvezető** aláírásának kell szerepelnie. Ez érvényes az Egyetem Gazdasági Osztályának felkészüléséig.
 - b. Külső partnerek: a külső partnerekkel való szerződések megkötésekor a szerződési feltételek közé fel kell venni az elektronikus kapcsolattartást is, amennyiben a szerződő fél ebbe beleegyezik. Ekkor a **Projektvezető minősített személyes tanúsítványa** kell, hogy szerepeljen az elektronikus aláírásban, valamint egy **időbélyegző**. Papíralapú igazolásnál a **Projektvezető** aláírásának kell szerepelnie. Ez érvényes az Egyetem Gazdasági Osztályának felkészüléséig.
5. Bejövő levél, pályázat, elkészült munka, előterjesztés, javaslat, jegyzőkönyv érkeztetése

- a. Belső munkatárstól: a munkatárstól érkező bármilyen küldemény érkeztetése a **Titkárságvezető** feladata, a dátum pontos megadásával. Az érkeztetés elektronikus esetben a **Titkárságvezető fokozott biztonságú személyes tanúsítványával** történik, **időbélyegző** felhasználásával. Rövidtávú cél az, hogy minden belső levelezés elektronikus formában történjen. A levelezés tartalmában a munkatárs (feladó) és a Szervezet (címezett) közötti hivatalos kapcsolatról szól.
 - b. Egyetemi partnertől: Amennyiben a Szervezet címére érkezik a küldemény, annak érkeztetése a **Titkárságvezető** aláírásával történik, a dátum megadásával. Elektronikus esetben a **Titkárságvezető fokozott biztonságú személyes tanúsítványával** és **időbélyegzővel** érkezteti a küldeményt, majd továbbítja azt a címezettnek. Amennyiben a Szervezet munkatársának érkezik a Szervezetet is érintő küldemény, abból egy másolatot **fokozott biztonságú elektronikus** aláírással ellátva köteles a titkárságnak küldeni, ahol a **Titkárságvezető** a fent leírt módon jár el.
 - c. Külső partnertől: Amennyiben a Szervezet címére érkezik a küldemény, annak érkeztetése a **Titkárságvezető** aláírásával történik, a dátum megadásával. Elektronikus esetben a **Titkárságvezető fokozott biztonságú személyes tanúsítványával** és **időbélyegzővel** érkezteti a küldeményt, majd továbbítja azt a címezettnek. Amennyiben a Szervezet munkatársának érkezik a Szervezetet is érintő küldemény, abból egy másolatot **fokozott biztonságú elektronikus** aláírással ellátva köteles a titkárságnak küldeni, ahol a **Titkárságvezető** a fent leírt módon jár el.
6. Kimenő levél, pályázat, elkészült munka, előterjesztés, javaslat, jegyzőkönyv
- a. Belső munkatársnak: a munkatárssal történő levelezését akkor szükséges aláírással ellátni, amennyiben az a szervezetet is érinti. Elektronikus esetben a küldő munkatársnak **fokozott biztonságú** vagy **minősített személyes tanúsítványával** kell hitelesítenie a küldeményt, melyből egy példányt a titkárságnak is el kell küldenie. Rövidtávon ezt a kommunikációt teljesen elektronikussá kell tenni. A levelezés tartalmában a Szervezet (feladó) és a munkatárs (címezett) közötti hivatalos kapcsolatról szól.
 - b. Egyetemi partnernek: az egyetemi partnernek szóló levelezés esetén a küldő személy írja alá a küldeményt. Elektronikus esetben minden, a Szervezetet érintő levelet vagy küldeményt a küldő **személyes fokozott biztonságú** vagy **minősített elektronikus tanúsítványával** kell hitelesíteni. A küldemény egy példányát továbbítani kell a titkárságnak. Rövidtávú cél az, hogy a jelenlegi elektronikus levelezés minden olyan esetben hiteles legyen, amikor a munkatárs a Szervezet nevében küld iratot.
 - c. Külső partnernek: a külső partnernek szóló levelezés esetén a küldő személy írja alá a küldeményt. Elektronikus esetben minden, a Szervezetet érintő levelet vagy küldeményt a küldő **személyes fokozott biztonságú** vagy **minősített elektronikus tanúsítványával** kell hitelesíteni. A küldemény egy példányát továbbítani kell a titkárságnak. Rövidtávú cél az, hogy a jelenlegi elektronikus levelezés minden olyan esetben hiteles legyen, amikor a munkatárs a Szervezet nevében küld iratot.
7. Bejövő vagy kimenő árajánlat
- a. Egyetemi partnertől: az ilyen iratokat a **Projektvezető** ellenjegyzzi, az **Igazgató** vagy a két **Igazgató-helyettes** együttesen hitelesíti. Amennyiben az árajánlat elektronikus formában érkezik, az aláíró tanúsítványának ellenőrzése utána a **Projektvezető személyes minősített tanúsítványával** ellenjegyez, az

Igazgató vagy a két **Igazgató-helyettes** együttesen a **személyes minősített tanúsítványával** elfogadja az árajánlatot. Egy példány a titkárságra kerül.

- b. Külső partnertől: az ilyen iratokat a **Projektvezető** ellenjegyzi, az **Igazgató** vagy a két **Igazgató-helyettes** együttesen hitelesíti. Amennyiben az árajánlat elektronikus formában érkezik, az aláíró tanúsítványának ellenőrzése után a **Projektvezető személyes minősített tanúsítványával** ellenjegyez, az **Igazgató** vagy a két **Igazgató-helyettes** együttesen a **személyes minősített tanúsítványával** elfogadja az árajánlatot. Egy példány a titkárságra kerül.

8. Szerződés

- a. Belső munkatárssal: a munkatárssal kötött szerződést a **Munkatárs** és az **Igazgató** vagy a két **Igazgató-helyettes** együttesen, valamint a **Projektvezető** írja alá. Elektronikus esetben a szerződésen szerepelnie kell a **Munkatárs fokozott biztonságú személyes tanúsítványának**, az **Igazgató** vagy a két **Igazgató-helyettes minősített szervezeti tanúsítványának**, a **Projektvezető minősített személyes tanúsítványának**, valamint **időbélyegzőnek**. A Szervezet részéről maximum 5.000.000 forint kifizetési vállalásig lehet egy szerződést elektronikusan aláírni. Ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus szerződések fogadására, a szerződéskötés minden esetben papíralapon történik.
- b. Egyetemi partnerrel: az egyetemi partnerrel kötött szerződést a **Partner** és az **Igazgató** vagy a két **Igazgató-helyettes** együttesen, valamint a **Projektvezető** írja alá. Elektronikus esetben a szerződésen szerepelnie kell a **Partner tanúsítványának**, az **Igazgató** vagy a két **Igazgató-helyettes minősített szervezeti tanúsítványának**, a **Projektvezető minősített személyes tanúsítványának**, valamint **időbélyegzőnek**. A Szervezet részéről maximum 5.000.000 forint kifizetési vállalásig lehet egy szerződést elektronikusan aláírni, illetve a partner részéről a tanúsítványát alátámasztó felelősségvállalásig lehet kifizetési kötelezettséget elfogadni. Ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus szerződések fogadására, a szerződéskötés minden esetben papíralapon történik.
- c. Külső partnerrel: a külső partnerrel kötött szerződést a **Partner** és az **Igazgató** vagy a két **Igazgató-helyettes** együttesen, valamint a **Projektvezető** írja alá. Elektronikus esetben a szerződésen szerepelnie kell a **Partner tanúsítványának**, az **Igazgató** vagy a két **Igazgató-helyettes minősített szervezeti tanúsítványának**, a **Projektvezető minősített személyes tanúsítványának**, valamint **időbélyegzőnek**. A Szervezet részéről maximum 5.000.000 forint kifizetési vállalásig lehet egy szerződést elektronikusan aláírni, illetve a partner részéről a tanúsítványát alátámasztó felelősségvállalásig lehet kifizetési kötelezettséget elfogadni. Ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus szerződések fogadására, a szerződéskötés minden esetben papíralapon történik.

9. Rendelés

- a. Külső partnertől: a rendeléseket a rendelést végző személy és felettese együttesen írja alá, amennyiben a rendelési érték kisebb, mint 50.000 forint. Más esetben a rendelést végző személy mellett az **Igazgató** vagy a két **Igazgató-helyettes** együttesen ellenjegyzi a rendelést. Elektronikus esetben a rendelésen szerepelnie kell a rendelést végző **Munkatárs fokozott biztonságú személyes tanúsítványának**, a felettes **Munkatárs fokozott biztonságú** vagy **minősített tanúsítványának**, amennyiben a rendelési érték kisebb, mint 50.000 forint. Ha a rendelési érték nagyobb, mint 50.000 forint, az iraton

szerepelnie kell a rendelést végző **Munkatárs fokozott biztonságú személyes tanúsítványának**, valamint az **Igazgató** vagy a két **Igazgató-helyettes minősített személyes tanúsítványának**. Ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus iratok fogadására, a rendelések kizárólag papíralapon készülhetnek.

10. Kinevezés

- a. Belső munkatársat: a kinevezési okirat saját részre elektronikusan, a Gazdasági Osztály részére papíron készül el. Az elektronikus változatot az **Igazgató minősített személyes tanúsítványával** és **időbélyegzővel** látja el. A papíralapú változatot az **Igazgató** szignálja. Ameddig az Egyetem Gazdasági Osztálya nem készült fel az elektronikus iratok fogadására, a kinevezések papíralapon készülnek.

11. Igazgatói utasítások

- a. Belső munkatársak felé: az igazgatói utasítások mindig elektronikus formában kerülnek kiosztásra a munkatársak között. A körlevelet az **Igazgató minősített szervezeti tanúsítványával** és **időbélyegzővel** ellátva írja alá. Ezután minden munkatárs **fokozott biztonságú személyes tanúsítványával** és **időbélyegzővel** láttatja azt.

Az archiválás szabályai

Az archiválás általános szabályait a Budapesti Műszaki és Gazdaságtudományi Egyetem Iratkezelési Szabályzata tartalmazza. Ennek 45.§ szerint „Az ügyiratokat az ügyiratkezelést ellátó szervezeti egység kezeli és irattárában öt évig őrzi. Az öt évnél hosszabb őrzési idejű, illetve nem selejtezhető iratokat az egyetemi levéltárnak kell átadni.”.

Az Egyetem szabályzata a következő táblázatban foglalja össze az irattárolás szabályait:

Tétel	T á r g y*	Megőrzési idő	Levéltárba adás ideje
1.	Jogszabályban rögzített megőrzési idejű iratok	jogszabály előírása szerint	5 év
2.	Az Egyetem által kiállított közokiratok, címek, kitüntetések, díszoklevelek iratai	nem**	5 év
3.	Egyetemi és kari szabályzatok	nem**	5 év
4.	Egyetemi tanácsi, kari tanácsi ülések, illetve szabályzatban említett testületek üléseinek dokumentumai	nem**	5 év
5.	Egyetemi Értesítő	nem**	5 év
6.	Iratselejtezési jegyzőkönyvek	nem**	5 év
7.	Igazgatási Szabályzat szerinti, rektor által aláírt szerződések	nem**	5 év

8.	Szabályzatokban nem selejtezhetőként nevesített dokumentumok	nem**	5 év
9.	A 1.-8.pontba nem sorolható iratok	legfeljebb 15 év	-

* A „nem selejtezhető” megjelölésű iratok azokban a szervezeti egységekben minősültek nem selejtezhetőnek, ahol keletkeztek. Más szervezeti egységek a 9. tételszám szerinti iratként kezelhetik ezen iratokat.

** nem selejtezhető

A Szervezet dokumentumait archiválási szempontból négy csoportba lehet osztani:

- egyszeri elolvasásra szánt iratok,
- egy éven belül selejtezendő iratok,
- öt évig tárolandó iratok,
- öt évnél hosszabb ideig tárolandó iratok.

Az egyszeri olvasásra szánt iratok és az egy éven belül selejtezendő iratok körét azon dokumentumok teszik ki, melyek **nem minősülnek ügyiratnak**, így nem érvényes rájuk az Egyetem Iratkezelési Szabályzata. Minden olyan iratot, melyet a munkatárs, mint a Szervezet dolgozója ír vagy fogad, kötelező a Titkárságnak továbbítani, ahol a **Titkárságvezető** feladata eldönteni, hogy az irat melyik kategóriába tartozik.

A jelenlegi technológiai feltételek mellett csak az egyszeri olvasásra szánt anyagok és az egy éven belül selejtezendő iratok teljes elektronizálása oldható meg. Az egyszeri olvasásra szánt anyagok iktatása és archiválása nem szükséges. Az egy éven belül selejtezendő iratok iktatása úgy történik, hogy a **Titkárságvezető** a felelős által már megfelelően kezelt elektronikus iratot ellátja a saját **fokozott biztonságú elektronikus tanúsítványával**, valamint **időbélyegzővel**, ha azt az érkeztetés során még nem tette meg. Az így előállított elektronikus iratot a Szervezet megfelelő biztonsági szintet elérő állományszerverén tárolja, az irat iktatási számának megfelelő hivatkozással.

Az öt évig tárolandó iratok iktatása akkor lehetséges, ha megteremtődnek a megfelelő feltételek, azaz rendelkezésre áll a hosszú távú elektronikus archiváláshoz szükséges szoftver. Ebben az esetben a **Titkárságvezető** saját **fokozott biztonságú elektronikus tanúsítványával** és **időbélyegzővel** archiv elektronikus aláírást állít elő, melyet a megfelelő állományszerveren tárol. A hosszú ideig tárolt elektronikus iratokról minden év decemberében biztonsági másolatot kell készíteni, valamint ellenőrizni kell azok olvashatóságát.

A levéltárba adandó iratok kizárólag elektronikus úton történő előállítására és tárolására nem megengedett egészen addig, ameddig az erre vonatkozó törvényi szabályozás meg nem születik.

Az elektronikus aláírás felhasználása a Szervezetben

A szervezeten belül minden dolgozó rendelkezik fokozott biztonságú elektronikus tanúsítvánnyal. Az igazgatóság és a projektvezetők emellett minősített elektronikus tanúsítványnak is a birtokosai. A szervezet vezetőinek pedig szervezeti minősített elektronikus tanúsítványa is van, amivel a szervezet hivatalos dokumentumait is aláírhatják.

A felhasználás elsődleges célja a minél kevesebb papírt felhasználó iroda. Első körben a kevésbé fontos, archiválásra nem kerülő dokumentumok aláírása a cél, amivel minden munkatárs megismerheti a technológiát. Második körben a tanúsítvány lejáratí idejénél nem hosszabb ideig tárolandó dokumentumok elektronizálása a cél. Végül a hosszútávú digitális archiválás is elérhető. A teljes sikerhez először belső használatra, majd a kiválasztott partnerekkel való kapcsolattartásra is felhasználható az elektronikus aláírás.

A dolgozóknak kötelessége a vezetőség által kijelölt dokumentumok körét elektronikusan fogadni és az előírásoknak megfelelő elektronikus aláírással ellátni, illetve az elektronikusan aláírt dokumentumokat megfelelően ellenőrizni. Ezen dokumentumokat kinyomtatása nem megengedett. Az elektronikusan kezelendő dokumentumok körét, illetve az elektronikus aláírás használatának részletes leírását az Elektronikus Aláírási Szabályzatról szóló igazgatói körlevél szabályozza.

Az elektronikus archiválás megvalósítása

A hosszútávú elektronikus aláírás legfőbb problémája az, hogy a hitelesítő adatok az évek múlásával gyakorlatilag elérhetetlenné válnak. Hitelesítő adat a teljes tanúsítványlánc, illetve a visszavonási listák. Ahhoz, hogy minden hitelesítő adat biztosan rendelkezésre álljon a jövőben, legkésőbb az aláíráshoz tartozó időbélyeg időpontja után kiadott első visszavonási lista lejáratá előtt el kell tárolni minden hitelesítő adatot. Mivel ez nyilvánvalóan az esetek nagy részében kivitelezhetetlen (pl. egy köztes hitelesítés-szolgáltató visszavonási listája ritkán frissül), bizonyos kompromisszumokkal kell élni.

Amiben nem lehet kompromisszum, az az archivált állomány formátuma. A hosszútávú elektronikus aláírás formátumát legjobban az ETSI TS 101 903-as számú specifikációjában fellelhető XaDES-A típusú XML állomány határozza meg. Megfelelő megállapodások mellett az ilyen állományt létrehozó alkalmazások képesek interoperábilisan működni.

Javasolt felépítés:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <EmbeddedSignedData>
  <Data Id="Data_1" FileName="test.txt" FileSize="4" MimeType="text/plain"
Encoding="http://www.w3.org/2000/09/xmldsig#base64">dGVzdA==</Data>
  <Data Id="Data_2" FileName="test.txt" FileSize="4" MimeType="text/plain"
Encoding="http://www.w3.org/2000/09/xmldsig#base64">dGVzdA==</Data>
- <Signature Id="Signature_1"
xmlns="http://www.w3.org/2000/09/xmldsig#">
- <SignedInfo Id="Signature_1_SignedInfo_1"
xmlns="http://www.w3.org/2000/09/xmldsig#">
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315" />
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
- <Reference Id="Signature_1_Reference_1" URI="#Data_1">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>...</DigestValue>
</Reference>
- <Reference Id="Signature_1_Reference_2" URI="#Data_2">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>...</DigestValue>
```

```

</Reference>
- <Reference Id="Signature_1_Reference_3"
Type="http://uri.etsi.org/01903/v1.2.2#SignedProperties"
URI="#Signature_1_SignedProperties_1">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue Id="Signature_1_SignatureValue_1">...</SignatureValue>
- <KeyInfo Id="Signature_1_KeyInfo_1">
- <X509Data>
- <X509IssuerSerial>
  <X509IssuerName>...</X509IssuerName>
  <X509SerialNumber>...</X509SerialNumber>
</X509IssuerSerial>
  <X509Certificate>...</X509Certificate>
</X509Data>
</KeyInfo>
- <Object>
- <QualifyingProperties Target="#Signature_1">
- <SignedProperties Id="Signature_1_SignedProperties_1"
xmlns="http://www.w3.org/2000/09/xmldsig#">
- <SignedSignatureProperties>
  <SigningTime>2004-05-01T12:00:00Z</SigningTime>
- <SigningCertificate>
- <Cert URI="#Signature_1_KeyInfo_1">
- <CertDigest>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>...</DigestValue>
</CertDigest>
- <IssuerSerial>
  <X509IssuerName>...</X509IssuerName>
  <X509SerialNumber>...</X509SerialNumber>
</IssuerSerial>
</Cert>
</SigningCertificate>
  <SignaturePolicyIdentifier>...</SignaturePolicyIdentifier>
</SignedSignatureProperties>
- <SignedDataObjectProperties>
  <CommitmentTypeIndication>...</CommitmentTypeIndication>
</SignedDataObjectProperties>
</SignedProperties>
- <UnsignedProperties Id="Signature_1_UnsignedProperties_1"
xmlns="http://www.w3.org/2000/09/xmldsig#">
- <UnsignedSignatureProperties>
  <CounterSignature
Id="Signature_1_CounterSignature_1">...</CounterSignature>
  <SignatureTimeStamp
Id="Signature_1_SignatureTimeStamp_1">...</SignatureTimeStamp>
- <CompleteCertificateRefs Id="Signature_1_CompleteCertificateRefs_1">
- <CertRefs>
- <Cert URI="#Signature_1_EncapsulatedX509Certificate_1">
- <CertDigest>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />

```

```
<DigestValue>...</DigestValue>
</CertDigest>
- <IssuerSerial>
  <X509IssuerName>...</X509IssuerName>
  <X509SerialNumber>...</X509SerialNumber>
</IssuerSerial>
</Cert>
- <Cert URI="#Signature_1_EncapsulatedX509Certificate_2">
- <CertDigest>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlldsig#sha1" />
  <DigestValue>...</DigestValue>
</CertDigest>
- <IssuerSerial>
  <X509IssuerName>...</X509IssuerName>
  <X509SerialNumber>...</X509SerialNumber>
</IssuerSerial>
</Cert>
</CertRefs>
</CompleteCertificateRefs>
- <CompleteRevocationRefs Id="Signature_1_CompleteRevocationRefs_1">
- <CRLRefs>
- <CRLRef>
- <DigestAlgAndValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlldsig#sha1" />
  <DigestValue>...</DigestValue>
</DigestAlgAndValue>
- <CRLIdentifier URI="#Signature_1_EncapsulatedCRLValue_1">
  <Issuer>...</Issuer>
  <IssueTime>...</IssueTime>
  <Number>...</Number>
</CRLIdentifier>
</CRLRef>
- <CRLRef>
- <DigestAlgAndValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlldsig#sha1" />
  <DigestValue>...</DigestValue>
</DigestAlgAndValue>
- <CRLIdentifier URI="#Signature_1_EncapsulatedCRLValue_2">
  <Issuer>...</Issuer>
  <IssueTime>...</IssueTime>
  <Number>...</Number>
</CRLIdentifier>
</CRLRef>
</CRLRefs>
- <OCSPRefs>
- <OCSPRef>
- <OCSPIdentifier URI="#Signature_1_EncapsulatedOCSPValue_1">
  <ResponderID>...</ResponderID>
  <ProducedAt>...</ProducedAt>
</OCSPIdentifier>
- <DigestAlgAndValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlldsig#sha1" />
  <DigestValue>...</DigestValue>
```

```

</DigestAlgAndValue>
</OCSPRef>
- <OCSPRef>
- <OCSPIdentifier URI="#Signature_1_EncapsulatedOCSPValue_2">
  <ResponderID>...</ResponderID>
  <ProducedAt>...</ProducedAt>
</OCSPIdentifier>
- <DigestAlgAndValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
  <DigestValue>...</DigestValue>
</DigestAlgAndValue>
</OCSPRef>
</OCSPRefs>
</CompleteRevocationRefs>
- <CertificateValues Id="Signature_1_CertificateValues_1">
  <EncapsulatedX509Certificate
Id="Signature_1_EncapsulatedX509Certificate_1">...</EncapsulatedX509Certificat
e>
  <EncapsulatedX509Certificate
Id="Signature_1_EncapsulatedX509Certificate_2">...</EncapsulatedX509Certificat
e>
  </CertificateValues>
- <RevocationValues Id="Signature_1_RevocationValues_1">
- <CRLValues>
  <EncapsulatedCRLValue
Id="Signature_1_EncapsulatedCRLValue_1">...</EncapsulatedCRLValue>
  <EncapsulatedCRLValue
Id="Signature_1_EncapsulatedCRLValue_2">...</EncapsulatedCRLValue>
  </CRLValues>
- <OCSPValues>
  <EncapsulatedOCSPValue
Id="Signature_1_EncapsulatedOCSPValue_1">...</EncapsulatedOCSPValue>
  <EncapsulatedOCSPValue
Id="Signature_1_EncapsulatedOCSPValue_2">...</EncapsulatedOCSPValue>
  </OCSPValues>
</RevocationValues>
- <ArchiveTimeStamp Id="Signature_1_ArchiveTimeStamp_1">
  <Include URI="#Signature_1_Reference_1" referencedData="true" />
  <Include URI="#Signature_1_Reference_2" referencedData="true" />
  <Include URI="#Signature_1_Reference_3" referencedData="true" />
  <Include URI="#Signature_1_SignedInfo_1" />
  <Include URI="#Signature_1_SignatureValue_1" />
  <Include URI="#Signature_1_KeyInfo_1" />
  <Include URI="#Signature_1_CounterSignature_1" />
  <Include URI="#Signature_1_SignatureTimeStamp_1" />
  <Include URI="#Signature_1_CompleteCertificateRefs_1" />
  <Include URI="#Signature_1_CompleteRevocationRefs_1" />
  <Include URI="#Signature_1_CertificateValues_1" />
  <Include URI="#Signature_1_RevocationValues_1" />
  <Include URI="#Signature_1_ArchiveTimeStamp_1" />
  <Include URI="#Signature_1_UnsignedProperties_1" />
  <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xmll-
c14n-20010315" />
  <EncapsulatedTimeStamp>...</EncapsulatedTimeStamp>

```

```
</ArchiveTimeStamp>  
</UnsignedSignatureProperties>  
<UnsignedDataObjectProperties />  
</UnsignedProperties>  
</QualifyingProperties>  
</Object>  
</Signature>  
</EmbeddedSignedData>
```

A formátum részletei érdektelenek, hiszen részletesen leírva megtalálhatók a szabványban. A lényeg az archiválás folyamata. Ez a következőképp történik meg:

1. Elkészül az elektronikus aláírás az eredeti dokumentumhoz. Ez azt jelenti, hogy egy XML keretbe beágyazzák az aláírandó fájlt (vagy annak URI-ját), annak lenyomatát, az aláírói tanúsítványt, stb. Ez a legegyszerűbb struktúra a XaDES-BES vagy XaDES-EPES, attól függően, hogy tartozik-e hozzá aláírási szabályzat.
2. Időpecsét kerül az elektronikus aláírásra. Ez a XaDES-T, az első igazán használható, rövidtávon letagadhatatlan formátum.
3. Az eddig elkészült struktúrához hozzáadjuk a teljes hitelesítési és visszavonási lánc referenciáját. Ez a XaDES-C, mely a tanúsítvány lejártáig biztosan garantálja az aláírás letagadhatatlanságát, hiszen rámutat minden szükséges információra.
4. Ha az ES-C formátumra kerül még egy időbélyegző és eltároljuk a teljes visszavonási és hitelesítési láncot, megkapjuk az ES-X Long formátumot. Ez hitelesen, hosszú ideig tárol minden szükséges információt.
5. Amennyiben még egy időbélyegzőt teszünk az állományra, eljutunk a XaDES-A formátumhoz. Ez az, mely elméletileg végtelen ideig képes hitelesen archiválni a dokumentumot, mert a teljes érvényesség fenntartásához csak felül kell időbélyegezni az állományt minden esetben, amikor az időbélyegzőhöz tartozó tanúsítvány lejár.

A hiteles archiválás tehát XaDES-A formátummal elvileg megvalósítható. Fennáll viszont a megjelenítés problémája. Egyrészt a formátum mellett tárolni kell azokat a megjelenítő alkalmazásokat, melyekkel olvashatóvá válik az archivált adat, másrészt olyan környezetet kell teremteni, ahol az állomány nem sérül.

A probléma megoldására az elektronikus aláírásról szóló törvény 2004-es módosítása szolgál, ami megteremtette a lehetőséget az elektronikus archiválási szolgáltatók működésére. Ezek a szolgáltatók elvileg képesek lesznek az általuk meghatározott dokumentumokat a fentiek alapján archiválni. Ezzel lehetőség nyílik pl. az elektronikus számlázás használatára is, hiszen azokat az adatokat (PDF, nyílt szöveg vagy XML formátumban) legalább 5 évig tárolni kell. A jogi környezet tehát készen áll az elektronikus aláírás használatára, a nagy kérdés az, hogy a felhasználók mikor igénylik majd a technológiát.

Irodalomjegyzék

European Telecommunications Standards Institute, „XML Advanced Electronic Signatures (XAdES)”, TS 101 903 v1.2.2, 2004. április
European Telecommunications Standards Institute, „Electronic Signature Formats”, TS 101 733 v1.5.1, 2003. december