



TRUST & SIGN

elektronikus aláírás, hitelesítés, titkosítás



MÁV INFORMATIKA Kft.

TRUST & SIGN

elektronikus aláírás, hitelesítés, titkosítás

Korunkban egyre jobban nő annak az igénye, hogy az Interneten, Intraneten vagy Extraneten kommunikáló személyek és eszközök által végzett műveleteket minél pontosabban és hitelesebben lehessen beazonosítani, kontrollálni. Erre azért van szükség, hogy csak az illetékes felhasználó vagy eszköz férjen hozzá a kívánt tartalomhoz vagy alkalmazáshoz úgy, hogy közben az általa végzett tevékenység és annak időpontja utólag bármikor ellenőrizhető legyen és a hitelesített dokumentumok, állományok minél inkább azonosíthatóak, személyhez köthetőek legyenek.

Mit jelent az elektronikus tanúsítvány kifejezés?

Az elektronikus formában keletkező tanúsítvány egy olyan igazolás, amelyet egy külön erre a célra létrehozott Hitelesítés Szolgáltató bocsát ki személyek, szervezetek, valamint eszközök részére annak érdekében, hogy a **digitális világban biztonságosan és hitelt érdemlően kommunikálhassanak**, azonosíthassák egymást. A MÁV INFORMATIKA Kft. által nyújtott TRUST & SIGN szolgáltatás ennek a kívánalomnak - a kapcsolódó szolgáltatásokkal együtt - az elektronikus megoldását jelenti.

Kinek ajánljuk a használatát?

Azoknak a cégeknek, szakembereknek és magánszemélyeknek javasoljuk az elektronikus tanúsítvány bevezetését és használatát, akik a rendszert használók megbízhatósága és folyamataik egyszerűsítése, felgyorsítása végett dokumentumokat (megrendelés, szerződés, visszaigazolás, stb.), e-mail-eket és egyéb iratokat - a törvény által szabályozott módon kívánják korszerűen, elektronikus hitelesítve elkészíteni, továbbítani, valamint tárolni.

Milyen előnyökkel jár az elektronikus aláírás, hitelesítés használata?

A szolgáltatás igénybeviteléhez és használatához nem szükséges különleges informatikai előképzettség, mivel néhány, a technológiával kapcsolatos fogalmi ismeretanyag át tanulmányozásával hasznosíthatja a módszer nyújtotta előnyöket, azaz:

- garantálhatja a megbízhatóságot,
- csökkentheti költségeit,
- felgyorsíthatja a kooperációs folyamatokat,
- növelheti a hatékonyságot,
- megszüntetheti a távolságból adódó akadályokat.

A hitelesítési szolgáltatás további pozitívuma, hogy a kiadott tanúsítvány a meglévő eszközön egyszer meghosszabbítható.

Az e-aláírás főbb törvényi háttere

Az elektronikus aláírás legfőbb törvényi hátterét az 1999/93-as EU direktíva alapján kidolgozott 2001. évi XXXV. tv. és annak 2004. LV. tv. módosítása, valamint az Informatikai és Hírközlési Minisztérium által elkészített rendeletek adják.

Ezekben a jogszabályokban - a nemzetközi szabványok és a hazai sajátosságok figyelembe vételével - különböző aláírási típusok, alkalmazható hardverek és szoftverek fajtái, valamint Hitelesítés Szolgáltatókra vonatkozó előírások olvashatók.

Felhasználási területek

A törvényi szabályozás ma már nagyon sok területen biztosítja az elektronikus aláírás, a nyilvános kulcsú titkosítási technológia széleskörű alkalmazását. Néhány példa az elterjedt alkalmazási lehetőségek közül:

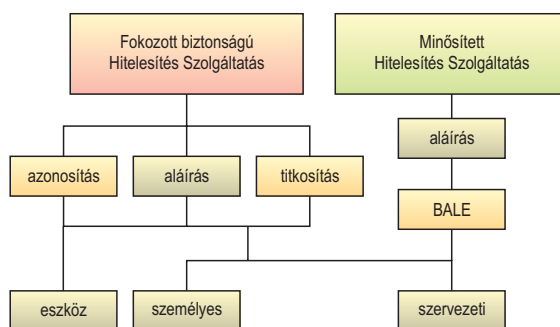
- A magánnyugdíj-pénztári bevallások, ahol a vállalatok ingyenes szoftver segítségével elektronikusan küldhetik el bevallásaikat a legtöbb nyugdíjpénztárba,
- az elektronikusan kötelező vizsgajelentések,
- e-cégljárásban az ügyvédek küldhetik be elektronikusan a cégszolgálatok változásait,
- az OEP részére a kórházak által küldendő jelentések,
- közjegyzői tevékenység,
- vállalati elektronikus számlázás,
- hiteles archiválás, akár a másolati példányokat nem kell kinyomtatni, akár meglévő papír dokumentumait archiválhatja úgy, hogy utána a papírt megsemmisítheti,
- e-bussines folyamatok: megrendelés, visszaigazolás, szerződés-kötés Interneten keresztül.

Milyen típusai vannak?

A hitelesítési tevékenységet elsősorban a törvényi előírások miatt két részre szükséges bontani, amely alapján **fokozott és minősített biztonságú**, ezen belül aláírói, azonosítási és titkosítói tanúsítvány típusokat különböztetünk meg. Ezek további részekre fejthetők, így megkülönböztetünk természetes és jogi személyeket, valamint eszközöket (pl.: szerverek, stb.).

Ennek megfelelően az alábbi ábrán szemléltetett tanúsítványok készülhetnek:

- magánszemélyeknek,
- szervezeti személyeknek,
- eszközöknek.



A fent ábrázolt tanúsítványtípusokon kívül az alkalmankénti kötelezettségvállalás mértéke az, amely még meghatározza a hitelesítési tevékenységet. E kötelezettségvállalás alatt azt kell érteni, hogy egy adott tranzakcióhoz - aláíráshoz - mekkora összegig vállal felelősséget az aláíró szervezet vagy személy. A felelősség mértéke a mindenkori szolgáltatási szabályzatban, valamint a kibocsátott tanúsítványokban a Hitelesítés Szolgáltató közli.

A tanúsítványok a jogszabályok szerint kétféle módon készülhetnek: szoftveresen vagy hardveresen - attól függően, hogy fokozott vagy minősített esetről van szó. Mivel a szoftveres tanúsítványok joghatása szűkebb körű (fokozott), mint az intelligens kártyás (BALE- biztonságos aláíró eszköz) minősített változatáé, ezért felhasználási területei is ennek megfelelően változnak.

Fokozott biztonságú e-aláírás

A fokozott biztonságú elektronikus aláírás olyan aláírás, amelyhez a Hitelesítés Szolgáltató olyan tanúsítványt bocsátott ki, hogy az **alkalmas** legyen az **aláíró azonosítására**, továbbá **e-mailek, dokumentumok vagy más adatok aláírására**.

Minősített e-aláírás

Aminősített elektronikus aláírás olyan aláírás, amelyhez szükséges egy speciális, ún. intelligens kártya (BALE - biztonságos aláíró eszköz), valamint a Hitelesítés Szolgáltató által kibocsátott tanúsítvány, ami alkalmassá teszi az aláírót az általa **hitelesített állományok letagadhatatlanságára**. Így olyan elektronikus hitelesített dokumentumok hozhatók létre, amelyek **személyhez köthetők** és **teljes bizonyító erejű magánokiratoknak felelnek meg**.

A technológiáról bővebben

Szimmetrikus kulcsokat már évszázadok óta használnak a kriptográfiában, de tulajdonságából adódóan - miszerint a kódoláshoz és a visszafejtéshez egyazon kulcs kell - komoly problémákat vetett fel azok biztonságos elosztásában, a hivatott személyekhez történő eljuttatásában. Ezért szükség volt egy olyan technológiai újításra, amellyel ez a gond kiküszöbölhetővé válik.

Így a szimmetrikus kulcsok mellett megjelentek az aszimmetrikus kulcspárok, amelyeket mára a kriptográfiában elterjedten alkalmaznak. Előbbi (szimmetrikus kulcs) legjobb tulajdonsága a gyorsaságában rejlik, utóbbi azonban nagyfokú biztonsága és könnyű, de biztonságos terjeszthetősége miatt vált a technológia egyeduralmójává. E tulajdonságok ötvözésével a szimmetrikus kulcsokat aszimmetrikus kulcspárral kombinálva a titkosításban, míg külön az aszimmetrikus kulcspárokat az elektronikus aláírásban és a hitelesítésben kezdték el használni.

A PKI technológia - azaz a Publikus (Nyilvános) Kulcsú Infrastruktúra - használatával lehetőség nyílik a megbízhatatlan hálózatokon belüli biztonságos és hiteles kommunikációra, ezen belül is az elektronikus aláírás, titkosítás és azonosítás alkalmazására. Vagyis a technológia az előbb felsorolt összes funkciót magában hordozza, azonban az alkalmazott módszerek mégis különböznek egymástól.

A PKI technológia lényege felhasználói szempontból az egyedi kulcspárok és tanúsítványok alkalmazása, amellyel **egyértelműen beazonosítható, hogy mely dokumentumot ki írta alá, kinek a részére titkosították vagy engedtek hozzáférést egy adott tartalom megtekintéséhez**.

Az aszimmetrikus kulcspár egy olyan egyedi azonosító számsor, amely egyik oldalról egy magánkulcsot, másik oldalról pedig egy nyilvános kulcsot tartalmaz. A kulcsok az alábbi tulajdonsággal bírnak:

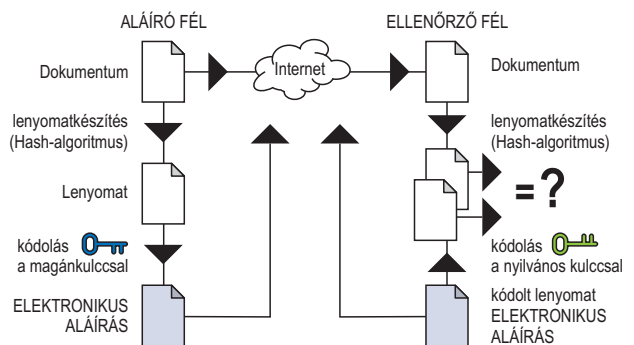
- Két kulcs együtt egy párt alkot,
- Nincs két egyforma kulcspár,
- A kulcsok különbözőek, egyik ismeretében a másik nem fejtető vissza,
- Amit az egyikkel kódoltunk, csak a másikkal fejthető vissza.

Ahhoz, hogy megállapítható legyen, kihez tartozik egy adott kulcspár, egy tanúsítványt szükséges hozzárendelni a nyilvános kulcshoz. A tanúsítvány azonosítási információkat tartalmaz a felhasználóról, de csak akkor tekinthető megbízhatónak, ha a kulcspárt és a tanúsítványt egy regisztrált Hitelesítés Szolgáltató rendelte össze, azaz hitelesítette. Miután a szolgáltató elvégezte a szükséges azonosítási műveleteket és kiállította az egyedi azonosítót és a hozzá kapcsolódó tanúsítványt, a kulcspárral végzett műveletek már személyhez köthetők, azok letagadhatatlanná válnak. Így egy tetszőleges állomány hitelesítése

egyértelműen személyhez köthetővé válik, s ha azon a dokumentumon, e-mailen utólag bármilyen változtatást hajtanak végre, az érzékelhetővé válik, tehát megbízhatóságát elveszti.

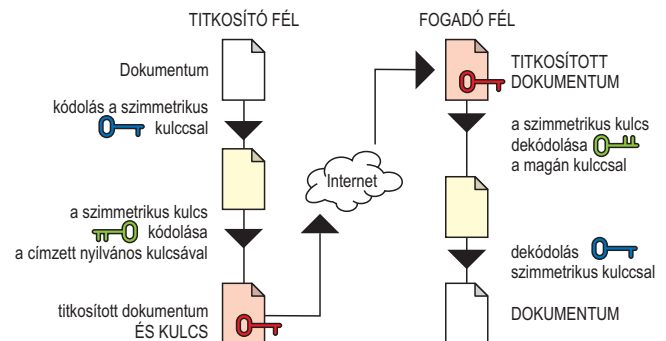
Elektronikus aláírás

Az elektronikus aláírás technikailag úgy megy végbe, hogy egy aláíró alkalmazás a hitelesítendő adatról egy ún. lenyomatot, kvázi ujjlenyomatot, rövid kódot - képez, amely az állományra jellemző adatokat tartalmazza. A magánkulccsal ezt az állományt írjuk alá, csomagoljuk be. Az ellenőrzéshez először az aláírt adatról, a már említett algoritmus segítségével lenyomatot képzünk, másodszor az aláírt becsomagolt lenyomatot a nyilvános kulccsal kibontjuk. Amennyiben megegyezik a két lenyomat, **garantált az állomány sértetlensége, hitelessége és megbízhatósága**.



Titkosítás

A titkosítási műveletnél a kulcspárok speciális tulajdonságát kell alkalmazni - természetesen egy megfelelő célszoftver alkalmazásával - oly módon, hogy eközben a felhasználónak ne kelljen semmit érzékelnie a háttérben zajló folyamatokról. A titkosítást végző alkalmazás a rejtjelezni kívánt teljes adatot egy szimmetrikus kulccsal titkosítja, majd a szimmetrikus kulcsot a címzett tanúsítványában szereplő nyilvános kulcsával titkosítja. Ezt követően a titkosított adat tartalmához csak az a személy fér hozzá, az tudja visszafejteni, aki rendelkezik a nyilvános kulcshoz tartozó magánkulccsal.





MÁV INFORMATIKA Kft.

Ahhoz, hogy egy szervezet biztonságos elektronikus kommunikációt folytasson partnereivel és ügyfeleivel, eszköz (szerver) tanúsítványra van szüksége, amellyel megvalósítható a biztonságos és titkosított adatforgalom belső és külső hálózatokban egyaránt. A tanúsítvány használatával az adatforgalom biztonságossá tehető, így az olyan adatok, mint a jelszó, a bankszámlaszám, a személyes információk vagy egyéb adatok kódolva érkeznek rendeltetési helyükre, lehetetlenné téve ezzel az adatokhoz való illetéktelen hozzáférést. A szerver tanúsítvány Web szerverre történő telepítésével (pl.: Apache, Microsoft IIS, stb.) az ügyfelek meggyőződhetnek arról, hogy a kiszolgáló, amivel kommunikálnak, nem egy hamis, ál szerver, így elkerülhető a hamis azonosságú szerverrel történő adatátvitel.

Egy tanúsított szerveren az ügyfél úgy tud hozzáférni a kívánt tartalomhoz, hogy a nyilvános kulcsát tartalmazó tanúsítványhoz tartozó magánkulcsot a szerveren elhelyezik és azonosításkor az ehhez tartozó egyedi magánkulcsával a felhasználó az elektronikus aláíráshoz hasonlóan hitelesíti magát. Így létrejön a biztonságos kapcsolat kliens és szerver között.

Mit kell tennie a TRUST & SIGN szolgáltatás igénybevételéhez?

A hitelesítéshez látogasson el Internetes oldalunkra és válassza ki az Önnek megfelelő szolgáltatást, majd töltsse ki a megrendelő űrlapot, amelyet követően elkészítjük tanúsítványát. Ezután fáradjon be Ügyfélkapcsolati Irodánkba, ahol a szükséges személyi, cég esetében szervezeti okmányok bemutatását követően átveheti tanúsítványát.

A MÁV INFORMATIKA Kft. a következő kapcsolódó szolgáltatásokkal áll ügyfelei rendelkezésre:

- Szükséges eszközök biztosítása (chipkártya, chipkártya olvasó, szoftverek, token,...)
- Rendszer biztonsági felmérés, auditálás,
- Szabályzatok kidolgozása, tanácsadás,
- Általános és egyedi megoldások, szolgáltatások (e-számlázás, hiteles archiválás, ...)
- Üzemeltetés, informatikai rendszer felügyelet 7/24 időtartamban.

MÁV INFORMATIKA Kft.

PKI Szolgáltató Egység

1012 Budapest, Krisztina krt. 37/a

Tel.: (1) 457-9337 • Fax: (1) 457-9520

E-mail: hiteles@mavinformatika.hu • Web: www.mavinformatika.hu/ca

Valamint a következő Területi Szolgáltató Központokban:

4025 Debrecen, Petőfi tér 12.

Tel.: (06-52) 415-952

E-mail: dbik@mavinformatika.hu

3530 Miskolc, Rákóczi u. 7.

Tel.: (06-46) 509-916

E-mail: msik@mavinformatika.hu

7623 Pécs, Szabadság út 39.

Tel.: (06-72) 512-430

E-mail: psik@mavinformatika.hu

6724 Szeged, Boros József utca 4/b

Zöld szám: (06-80) 82-00-26

E-mail: sgik@mavinformatika.hu

9700 Szombathely, Széll Kálmán u. 2.

Tel.: (06-94) 340-402

E-mail: smik@mavinformatika.hu

4625 Záhony, Európa tér 12.

Tel.: (06-45) 426-277

E-mail: zhik@mavinformatika.hu

TRUST & SIGN

elektronikus aláírás, hitelesítés, titkosítás