SZAKCIKK

Az elektronikus aláírásról

Az elektronikus vagy más néven digitális aláírás ugyanúgy működik, mint a hagyományos kézi aláírás, a fő különbség az, hogy elektronikus dokumentumokat írunk alá. A digitális aláírással szemben elvárás, hogy az

- letagadhatatlan legyen és ne lehessen hamisítani; azaz egyetlen személy tudja létrehozni a rá jellemző aláírást
- az létrehozott aláírás kapcsolódjon az aláírt dokumentumhoz, azt az aláírást követően ne lehessen módosítani, illetve az utólagos módosítást detektálni lehessen

Az elektronikus aláírás módszere az úgynevezett nyilvános kulcsú titkosításon alapul. Ezen titkosítás alkalmazásakor egy üzenet titkosításához és visszafejtéséhez két különböző kulcsra – úgynevezett kulcspárra – van szükség. Egy adott üzenet titkosításához az egyik kulcsot, míg a titkosított üzenet visszafejtéséhez a kulcspár másik elemét kell felhasználni. A kulcspár két eleme egymástól független, egyik kulcs ismeretében nem lehet „kikövetkeztetni" a másik kulcsot. A nyilvános kulcsú titkosítás a nevét onnan kapta, hogy az algoritmusban használt kulcspár egyik elemét annak tulajdonosa nyilvánosságra hozza – ez az ő nyilvános kulcsa – míg a kulcspár másik elemét biztonságos helyen őrzi – ez az ő titkos kulcsa. Amennyiben egy adott kulcspár tulajdonosa számára titkosított üzenetet kívánunk küldeni, akkor az ő nyilvános kulcsával kell kódolni az üzenetet, az üzenet visszafejtése csak kulcspár másik elemének –a titkos kulcsnak – a felhasználásával lehetséges.

A digitális aláírás létrehozása során azonban a folyamat fordítva történik. Az üzenet küldése során a küldő fél saját titkos kulcsát felhasználva kódolja az általa küldött üzenetet, melyet a fogadó fél a csak küldő nyilvános kulcsát felhasználva tud visszafejteni. Ez esetben a cél nem az üzenet tartalmának védelme –hiszen a publikus kulcsot felhasználva azt bárki visszafejtheti –, hanem az, hogy a fogadó fél biztos lehessen, hogy az üzenet valójában kitől származik. Tehát amennyiben a fogadó fél a küldő nyilvános kulcsát felhasználva vissza tudja fejteni a kódolt üzenetet biztos lehet benne, hogy az valóban attól a küldőtől származik akinek a nyilvános kulcsát a visszafejtés során felhasználta, mivel a kódolt üzenetet csak a titkos kulcs birtokában lehetett létrehozni.

A gyakorlatban a titkosítás és a digitális aláírás folyamata több lépésből áll, több matematikai algoritmust is felhasználnak a hatékonyság és a biztonságosság növelése érdekében, de a folyamat biztonságossága a nyilvános kulcsú titkosításon alapul. Ahhoz, hogy két kommunikálni kívánó fél digitálisan aláírt üzenetekkel kommunikáljon egymás között szükséges, hogy ismerjék egymás nyilvános kulcsait. Minden digitálisan aláírt üzenet ellenőrizhető a küldő fél nyilvános kulcsának birtokában. Az ellenőrzés során kiderül, hogy valójában a küldőé-e a digitális aláírás, illetve az, hogy az aláírt dokumentum sértetlen-e. Az ellenőrzéshez elengedhetetlen, hogy a kommunikáló felek biztonságos módon hozzájussanak egymás nyilvános kulcsaihoz, mely abban az esetben, ha a kommunikáció nem szűk körben, hanem több fél között – például egy nagyobb szervezeten belül – történik igen bonyolult lehet. A digitális aláírások kezelése során a legfontosabb kérdés az, hogy a nyilvános kulcsokat megbízható módon annak tulajdonosához kössük, azaz a lehető legnagyobb mértékig lehessünk biztosak abban, hogy egy adott személyhez melyik publikus kulcs tartozik

Azt a feladatot, hogy egy nyilvános kulcsot megbízható módon egy adott kommunikáló félhez lehessen rendelni az úgynevezett tanúsítványszolgáltató szervezetek végzik el. A tanúsítványszolgáltatók alapszolgáltatása a nyilvános kulcs személyekhez, vagy szervezetekhez rendelése, mely hozzárendelés úgynevezett tanúsítványok kiadásával történik meg. A tanúsítvány tulajdonképpen egy elektronikus igazolvány, mely tartalmazza a tulajdonosa adatait, valamint annak nyilvános kulcsát. A tanúsítványigénylés folyamata során az igénylő a tanúsítványszolgáltató felé igazolja magát, majd az azonosítást követően a szolgáltatótól egy olyan digitális igazolványt – tanúsítványt - kap, mely igazolja, hogy ő mely nyilvános kulccsal rendelkezik, a kiadott tanúsítványokat a szolgáltató egy nyilvános adatbázisban eltárolja. A tanúsítványszolgáltató tevékenységeinek keretében azonosítja az igénylő személyét, tanúsítvány bocsát ki, nyilvántartást vezet, karbantartja a tanúsítványváltozásokkal kapcsolatos adatokat.

A digitális aláírásnál használt titkos kulccsal csak a felhasználó rendelkezik, - annak érdekében, hogy azzal ne lehessen visszaélni annak biztonságos tárolását meg kell oldani. A kulcs tulajdonképpen egy hosszú nullákból és egyesekből álló bitsorozat, melyet valamilyen médián célszerű tárolni. A titkos kulcsok tárolásának legelterjedtebb és az egyik legbiztonságosabb módja a chipkártyán való tárolás. Ez a védelmi mód biztosítja azt, hogy illetéktelen személy nem férhet hozzá a titkos kulcshoz, valamint annak lemásolását is megakadályozza.

A digitális kommunikáció egyre elterjedtebbé válik – elég az elektronikus levelezésre gondolnunk -, egyre nagyobb mértékben használunk elektronikus dokumentumokat. A digitális aláírás elfogadásának módjáról illetve annak feltételeiről csakúgy mint az Európai Unióban úgy Magyarországon is törvény rendelkezik. A digitális aláírás jogi szabályozásának megjelenése előtt is lehetőség volt arra, hogy a felek egymás között megegyezzenek abban, hogy az egymás közti megállapodásokat, szerződéseket elektronikus formában is elfogadják, de ezen megállapodást hagyományos módon kellett hitelesíteniük. A digitális aláírással kapcsolatos törvény lehetővé teszi, hogy ne legyen szükség az előzetes papír alapú szerződésre, valamint lehetővé teszi a digitálisan aláírt dokumentumok elfogadását különböző területeken: az államigazgatásban, a kereskedelemben illetve a polgárjogi szerződésekben.

Magyarországon az elektronikus aláírásról szóló törvény 2001 szeptember 1.-én lépett hatályba. A törvény három különböző szintű elektronikus aláírást különböztet meg – normál, fokozott biztonságú illetve minősített -, ugyanakkor kétfajta tanúsítványt – fokozott biztonságú és minősített –különböztet meg. A lényeges különbség az egyes tanúsítványtípusok között a regisztrációs folyamatban van, azaz ott, hogy milyen módon, mennyire megbízhatóan azonosítja a tanúsítványszolgáltató az igénylő személyét, hogy győződik meg identitásáról (személyi igazolvány, útlevél, közjegyzői igazolás stb.).

A digitális tanúsítványok kezelését manapság számos alkalmazás és operációs rendszer támogatja. Amennyiben a felhasználó rendelkezik digitális tanúsítvánnyal képes digitálisan aláírt levelek küldésére, a számítástechnikai rendszerekhez való hozzáférése is alapulhat digitális igazolványán.

Ezek után feltehető a kérdés, hogy kik használhatják ezen szolgáltatást, kik azok akinek digitális tanúsítványra szükségük lehet? Azok számára, akik valaki felé megbízható módon szeretnének különböző elektronikus dokumentumokat eljuttatni, vagy eltárolni azokat az egyik leghatékonyabb megoldás a digitálisan aláírt dokumentumok használata. A digitális aláírások mai leggyakoribb alkalmazási területei:

- Elektronikus levelezés során a levelek digitális aláírása
- Elektronikus formában eljuttatott anyagok aláírása
- Belső iratkezelő rendszerekben az iktatott anyagok digitálisan aláírt verzióinak tárolása
- Elektronikus kereskedelemben, Interneten keresztül bonyolított elektronikus tranzakciók hitelesítése

A legfontosabb előnyök melyet a digitális aláírás biztosíthat

- A digitális aláírás ellenőrzése után biztosak lehetünk benne, hogy ki az aki aláírta a dokumentumot, az aláíró nem tudja ezt letagadni
- Az aláírás után a dokumentumot nem lehet módosítani, amennyiben ez mégis megtörténik a digitális aláírás érvénytelen lesz, azaz ki lehet mutatni, hogy valaki azt az aláírást követően módosította

A digitális tanúsítványok igénylése a tanúsítványszolgáltatónál történik, ahol az igényelt tanúsítvány típustól függően az igénylőnek azonosítania kell magát. Az igénylő azonosítása után a szolgáltató kiadja a digitális igazolványt, azaz magát a tanúsítványt. A titkos kulcs megfelelő védelme érdekében azt célszerű biztonságos adathordozón tárolni, ez a mai gyakorlat szerint chipkártyán valósulhat meg. A szolgáltató a titkos kulcs tárolásához szükséges kártyát, valamint a kártyaolvasót is az igénylő rendelkezésére bocsátja amennyiben az nem rendelkezik ezen eszközökkel.

Az elektronikus aláírások használatának bevezetésében jelentős eredményt ért el a Microsec Kft. A Microsec E-szignó szolgáltatást a Microsec Kft. 2002. évben vezette be, miután jogosultságot szerzett az elektronikus aláírás hitelesítésére a Hírközlési Felügyelettől.
Az E-szignó program segítségével szerkesztett szabályos formátum elektronikus aláírással ellátott dokumentumok az államigazgatási és magánszervezeteknél általános elfogadást nyertek.

MICROSEC KFT • 1022 Budapest, Marcibányi tér 9. • Levelezési cím: 1374 Budapest, Pf. 515
Telefon: (36-1) 438-6321 • www.e-szigno.hu