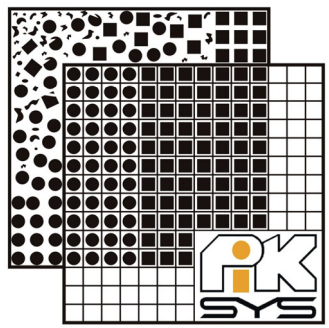
Szoftvertechnológiák a hitelesség megítélésének támogatásához

Tíz érv a vállalati PKI használata mellett

Helfer Pál

PiK-SYS Kft.



Elektronikus aláírás törvény

- Magyarország az Európai Közösséggel és azok tagállamaival kötött társulási megállapodás („Európa Megállapodás”) alapján fennálló jogharmonizációs kötelezettségeinek teljesítése céljából valamit gazdaságpolitikai megfontolások alapján fogadta el a 2001. évi XXXV. törvényt az elektronikus aláírásról.

- A magyarországi „digitális aláírás kultúra” igényelte a törvényi szabályozást; a jogszabály megteremti a hitelesített elektronikus aláírás elfogadásának lehetőségét és feltételeit.
- A törvényjavaslat hatályba lépése: 2001. szeptember 1.

Az elektronikus aláírás

Elektronikus aláírásnak minősül minden „elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.”

1. Egyszerű aláírás

Általános bizonyítóérvénnyel bír.

2. Fokozott biztonságú elektronikus aláírás

Alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető. Olyan eszközzel hozták létre, amely kizárólag az aláíró befolyása alatt áll. Az aláírás úgy kapcsolódik a dokumentum tartalmához, hogy azon minden az aláírás elhelyezését követően tett módosítás érzékelhetővé válik.

3. Minősített elektronikus aláírás

Bizonyíthatóan igazoló erejű, a Nemzeti Hírközlési Hatóság által nyilvántartásba vett hitelesítési szolgáltató minősíti. A törvény végrehajtási utasításában előírt magasabb biztonságtechnológiai követelményeknek is meg kell felelnie.

Elektronikus aláírás felhasználási területei:
E-közigazgatás

- A közigazgatási szerveknél meg kell teremteni a digitális dokumentumok kezelésének, az elektronikus levelezésnek a feltételeit. Ezután beszélhetünk arról, hogy az elektronikus aláírás bevált gyakorlattá vált.
- Amíg a közigazgatásban, a banki szférában és a gazdaság egyéb szereplői sincsenek megfelelően felkészülve, addig nem lehet a vállalatok, magánszemélyek felé nyitni a PKI technológiával, elektronikus aláírással.

Elektronikus aláírás felhasználási területei:
E-banking

- Az Interneten keresztül történő banki ügyintézést egyelőre csak kevesen veszik igénybe, pedig biztonságos, időtakarékos és nem kell sorban állni.

- Az emberek illetéktelen adatfelhasználástól tartanak, nem bíznak a rendszer biztonságában.

Elektronikus aláírás felhasználási területei:
E-kereskedelem

- Az Internet-használat tendenciája azt mutatja, hogy az e-kereskedelmet iránt a legfogékonyabbak az emberek.
- Ma még az Internetes vásárlások harmadának ellenértékét utánvéttel egyenlítik ki.
- Jövő : a biztonságos elektronikus fizetési lehetőségek alkalmazása.

A hitelesítés fogalma

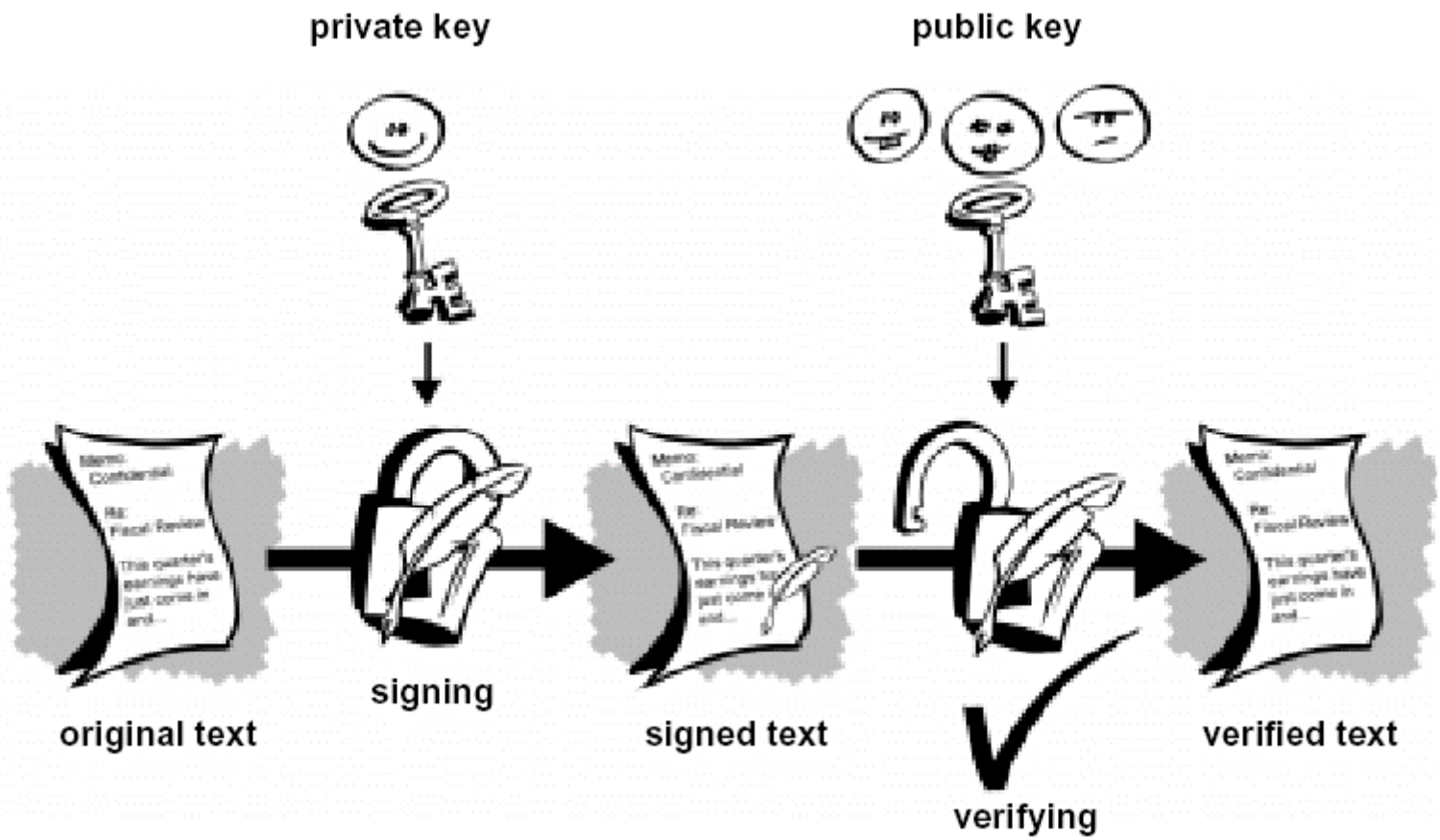
- 1. [biztonság] Tanúsítvány érvényességének ellenőrzése.

- 2. Szoftver vagy hardver megadott kritériumok szerinti megfelelőségének vizsgálata, illetve az erről szóló bizonyítvány kiállítása.

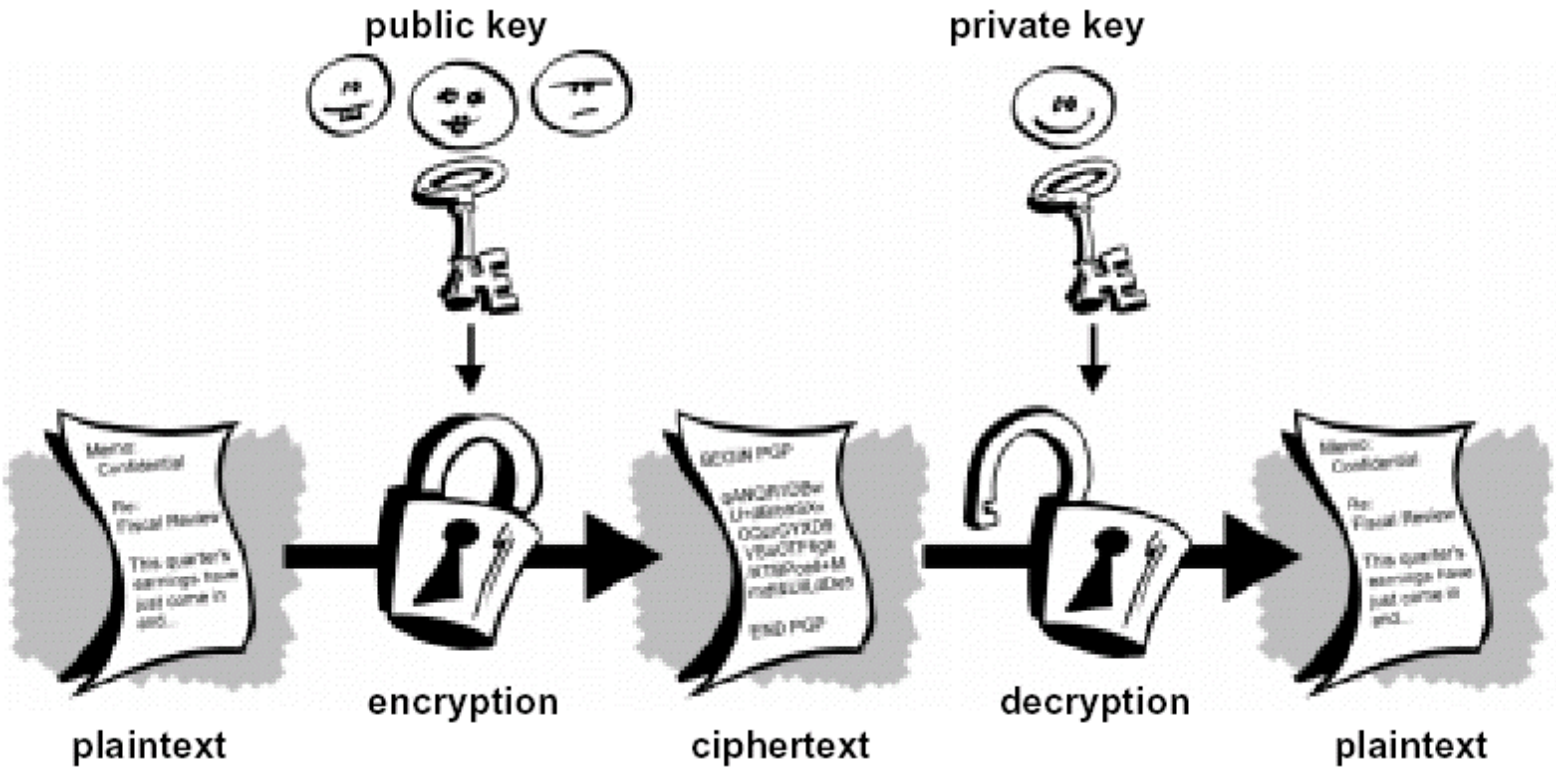
Hitelesség és azonosítás

- Az ilyen rendszerek a jelszóhasználatot egy véletlenszerűen hozzáadott elemmel egészítik ki, amelyet nehéz másolni és sokszorosítani.
- Ez a megbízható hozzáférés-ellenőrzés, valamint adatkezelés alapja.
- Az adatok (és így a személyiségi jogok) sértetlenségének és megváltoztathatatlanságának érdekében hitelesítés-szolgáltató által szavatolt digitális aláírás elhelyezésének lehetősége.

Digitális aláírás



Aszimmetrikus titkosítás



Public Key Infrastructure - PKI

- a külföldi cégek már előírták a digitális aláírás, illetve a titkosítás használatát – így a velük kapcsolatban álló magyarországi cégek is kötelesek használni.

- kis cégeknél is (egy-két személy részére) szükség van rá...

...és, hogy miért?

PKI napjainkban

Mert...

- manapság már minden cégnek fontosak az alábbi követelmények:
  - sértetlenség
  - bizalmasság
  - letagadhatatlanság
  - titkosság

Pl.: Biztonságos levelezés, állomány-titkosítás, digitális aláírás, biztonságos web-elérés, VPN

A titkosítás jelentősége I.

- A bizalmas jellegű vállalati információkat digitálisan tárolják;
- A szabályzatok és a vállalati biztonsági vezetők megkövetelik a kritikus adatok titkosítását;
- A belső és külső levelezés mennyisége megnöveli az adatlopással és visszaélésekkel összefüggő bűncselekmények számát.

A titkosítás jelentősége II.

A megfelelő titkosítási megoldáshoz ismerni kell a vállalat különleges igényeit, céljait,levelezési rendszerét és infrastrukturális adottságait.

- **A siker képlete: bizonyított technológia + tapasztalt szakember kiválasztása és alkalmazása**

Tíz érv a vállalati PKI használata mellett vagyis mit vegyünk számításba...

1. Bizonyított és elismert technológia

- Több éven keresztül, valós vállalati környezetben alkalmazott és szakemberek által tesztelt hatékony eszköz.
- Nyílt forráskód kiadása az előzetes betekintéshez.
- Szoftverfejlesztő nemzetközi múltja és hírneve.

2. Ipari szabványokra történő alapozás

- együttműködési képesség más termékekkel
- megnöveli a létező infrastruktúra értékét
- OpenPGP, S/MIME, X.509 … szabványok támogatása

Tíz érv a vállalati PKI használata mellett

3. Kapcsolódik a saját vagy az üzleti partnerek által üzemeltett levelezőrendszer(ek)hez

- széles körű összeegyeztethetőség a telepítéskor

4. Integrált és átfogó termékcsomag

- az integrált adattitkosító termékek hosszabb életciklussal rendelkeznek, melyet az egyszerű felépítésnek és a felhasználóbarát kezelőfelületnek köszönhetnek;
- további előnyt jelent az alacsony fenntartási költség, illetve a megfelelő technikai támogathatóság

Tíz érv a vállalati PKI használata mellett

5. Többszintű és irányú védelem elérésének képessége

- vállalati biztonsági politika kétirányú (ki- és bejövő információtovábbítás) és réteges (alkalmazotti-vezetőségi vagy külső partnerekkel történő kommunikáció) szintjének megvalósítása.

6. Egyszerű és automatizált kulcsmenedzsment

- skálázható megoldás, amely nemcsak a szakértők, hanem az alkalmazottak és a külső partnerek számára is érthető.

Tíz érv a vállalati PKI használata mellett

7. Digitális aláírás és titkosítás a hitelesítéshez

Hitelesítés: az eljárás, amely...

- ...igazolja a levél küldőjét vagyis összeveti azzal, akinek az mondja magát;
- ...megállapítja, hogy az e-mail tartalma a továbbküldés alatt megváltozott-e.

8. Együttműködés a vírusvédelmi, spam- és tartalomszűrő megoldásokkal

- a titkosítási és biztonsági megoldások hatékony együttműködése a zökkenőmentes vállalati működéshez.

Tíz érv a vállalati PKI használata mellett

9. Elveszett kulcsok visszaállítása

- Törvényi előírások a vállalati titkosított adatok hozzáféréséhez pl: nemzetbiztonsági / bűnügyi indokból;
- emelt szintű titkosítási jellemzők pl: ADK, kulcs visszaállítási és megosztási funkciók előnyben részesítése a fokozott biztonságú információkhoz.

10. Pénzügyi stabilitás, folytonosság

- A hosszú távú és megbízható együttműködés érdeke;
- Vállalati fejlődés töretlensége, új befektetések ösztönzése;
- Nemzetközi, interkontinentális kapcsolatrendszer és támogatás.

Melyik az a szoftvermegoldás, amely ezeknek a követelményeknek megfelel ?

PGP Universal

www.pgp.com

PGP Corporation termékcsalád

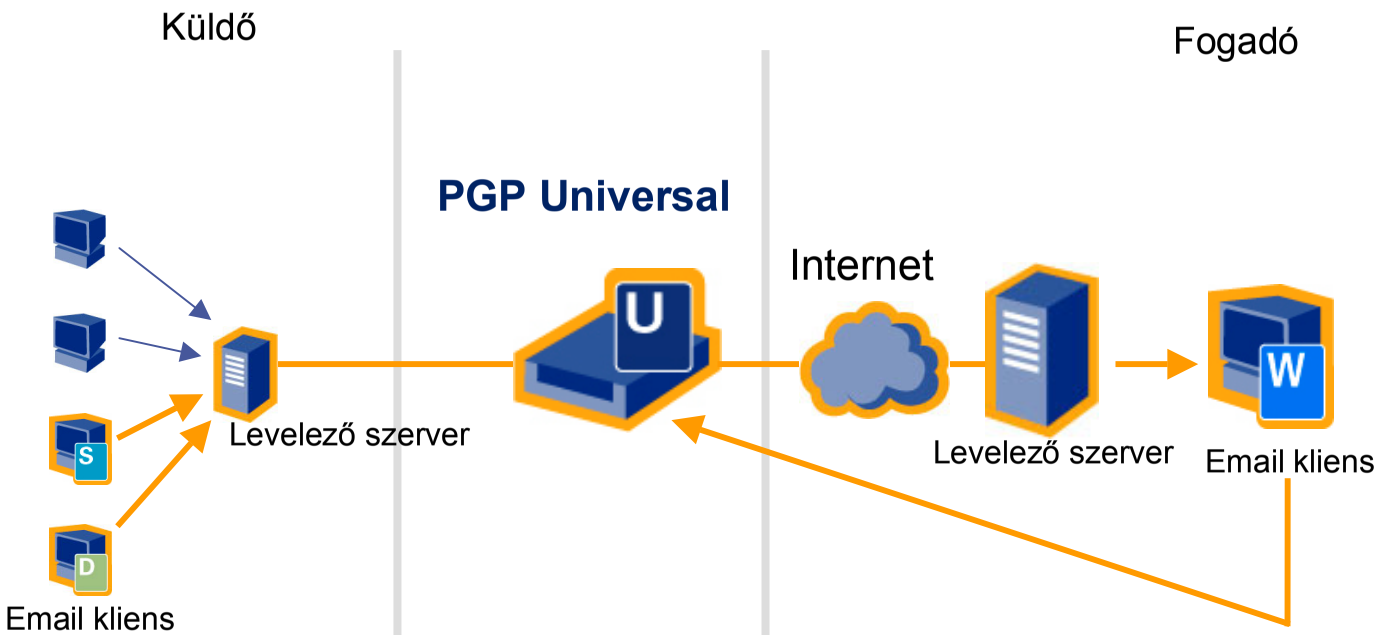
PGP Desktop termékek

- Munkaállomásoldali alkalmazások
- A felhasználó dönti el mikor, mit szeretne titkosítani
- Végpontok közötti titkosítás (munkaállomások között)

PGP Universal termékek

- Szerver (hálózat) oldali alkalmazás
- Központi házirend, felhasználói beavatkozást nem igényel a titkosítás/hitelesítés
- Végpontok közötti megoldás (PGP Satellite funkció használata során)

PGP Universal



Kiegészítő funkciók: PGP Web Messenger, PGP Satellite

Nemzetközi esettanulmányok

- Egészségügy - USA egészségbiztosítási törvény (Health Insurance Portability & Accountability Act, HIPAA)

  Titkosítási és biztonsági követelményei:

1, személyes adatokhoz történő hozzáférés ellenőrzése;

2, felülvizsgálat ellenőrzése;

3, adattovábbítás biztonságosságának szükségessége;

4, adatsértetlenség megőrzése.

PiK-SYS Informatikai és Tanácsadó Kft.

- másfél évtizedes tapasztalat az elektronikus információvédelem területén
- Technológiai partnerek:

- McAfee
- PGP Corporation
- WatchGuard Technologies
- Packeteer

- Szolgáltatásaink: tanácsadás, oktatás, felülvizsgálat…

Köszönöm a figyelmet!

pal.helfer@piksys.hu

www.piksys.hu