PKI alapok

Korunk informatikájának kulcs kérdésévé vált az adatbiztonság és a hitelesség. A számítógépes hálózatok fejlődése (Internet), az elektronikus kereskedelem és pénzforgalom kialakulása, olyan adatbiztos környezetet igényelnek, ami könnyen kezelhető és törvényileg elfogadott. Az egyszerű kezelhetőséget az elmúlt néhány év technológiai fejlődése valósította meg, míg a törvényességi keretet az a világszerte beindult törvénykezési folyamat, ami a digitális aláírás révén hivatalossá teszi az elektronikus dokumentumokat. Az EU Bizottság 93/1999 direktívája európai szinten fogalmazza meg a hivatalos elektronikus dokumentum kezelés elvárásait, útmutatást adva a tag és jelölt országok ez irányú törvénykezéséhez. Nálunk a törvény várhatóan 2001 szeptemberében lép hatályba. Az EU ugyanakkor gondoskodik a technológiai szabványok harmonizációjáról is, amit az EU Bizottság által támogatott és koordinált szervezetekben történik (ETSI, CEN ISSS, EESSI, IST).

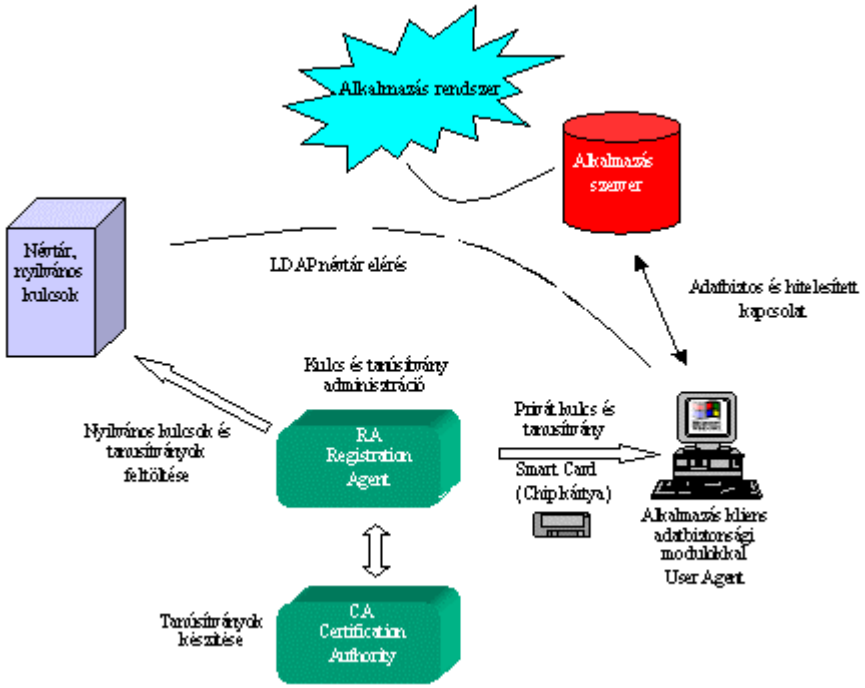
A PKI rendszer, mint azt neve is mutatja (Public Key Infrastructure), olyan alkalmazás környezetet (infrastruktúrát) kínál, ami lehetővé teszi a törvények által elfogadott kétkulcsú harmadik személyes hitelesítési és adatbiztosítási eljárások használatát a számítógépes alkalmazások számára.

A PKI rendszerek alkalmazásának előnyei nem csak abból a kötelezettségből származnak, hogy használatát a jövőben akár törvényileg is elő lehet írni, noha önmagában nagy előny jelent az, ha valaki olyan rendszert alkalmaz, ahol az elektronikus dokumentumok (pl.: banki dokumentumok, megrendelések, számlák, államigazgatási dokumentumok, stb.) hivatalosan elismertethetők. A PKI rendszerek kialakításával, a chip kártyák használatával a számítástechnikai környezet és az egyre terjedő adatátviteli rendszerek (pl.: Internet) úgy tehetők biztonságossá és hitelessé, hogy kezelésük továbbra is egyszerű marad. Sok esetben ezen egyszerűség a mai biztonságos alkalmazáskezelést egyszerűsíti például akkor, ha több alkalmazás vagy elektronikai rendszer password-jei vagy kártyái helyett, egy chip kártyát lehet használni. Mindez jelentős költség csökkenést jelent, ha a párhuzamos biztonsági rendszerek password vagy kártya adminisztrációja helyett egy PKI alapú chip kártya adminisztrációt kell üzemben tartani. Az adminisztráció csökkenése természetesen a biztonságot is növeli.

Az elektronikus adatok hitelesítése és kódolása egységes alapelven működik, amit a technológiában PKI rendszernek nevezünk. A rendszerben a felek két kulccsal (kóddal) rendelkeznek. Az egyik kulcs a saját, privát kulcs, amit csak az adott fél ismer és birtokol (pl.: smart kártyán). A másik kulcs a nyilvános, public, amit mindenki elérhet és általában elektronikusan jól elérhető helyen tárolnak (pl.: névtárakban). A két kulcs kombinációjával digitális aláírást lehet képezni, illetve adattartalmat lehet kódolni, titkosítani úgy, hogy a másik félnek a hitelesség ellenőrzésére, illetve az adattartalom dekódolására csak a küldő fél nyilvános kulcsára van szüksége. A privát kulcs minden esetben továbbra is titkos marad, ugyanakkor a hitelesített és adatbiztos tranzakció elvégezhető. Lényeges követelmény, hogy a saját és nyilvános kulcsok hitelesek legyenek, vagyis hogy annak valódiságát és az adott félhez való tartozását hiteles harmadik fél garantálja, közjegyezze. E feladatot az elektronikus közjegyző végzi a rendszerben (CA= Certification Authority) A CA mint harmadik fél nem tesz mást mint aláírja, hitelesíti az adott fél kulcsait, amit tanúsítványként (certification) szolgáltat a kulcsokhoz.

Általános felépítés, működés

A PKI rendszer általános felépítését az alábbi ábra mutatja be:



PKI PKI alapú adatbiztonsági rendszer elemei

A privát és a nyilvános kulcsok létrehozása több helyen is történhet. A létrehozó lehet a CA, RA is, illetve a kulcsok a chip kártyán is generálhatók, aminek az az előnye, hogy a privát kulcs sohasem hagyja el a smart (chip) kártyát. A nyilvános kulcsok a névtárban kerülnek tárolásra, a privát kulcsok smart kártyán vagy egyéb hordozón kerülnek a felhasználókhoz. A kulcspárok, felhasználók szerinti kezelését az RA–val lehet szakszerűen adminisztrálni, ami biztosítja a nyilvános azonosítók és tanúsítványok tömeges továbbítását is a névtárba. A CA tanúsítványokat állít elő, amivel harmadik személyként hitelesíti a nyilvános és privát kulcsok tulajdonoshoz való tartózását. A tanúsítványkészítési kérelmeket az RA indítja a CA felé, a CA az adott kulcsokhoz elkészített tanúsítványokat az RA felé továbbítja. A tanúsítványok a nyilvános és privát kulcsokhoz mellékelődnek.

Az alkalmazás kliens oldalon, a privát és nyilvános kulcsok elérését, összevetését és a rejtjelezést biztonsági modulok végzik. Az alkalmazásfunkciók kezelése mellett lehetőség nyílik az elektronikus dokumentumok digitális aláírására és titkosítására is. Az alkalmazás kliensek, a nyilvános kulcsok kezelésekor rendszerint LDAP protokollon keresztül érik el a névtárat.

A hitelesítésben résztvevő valamennyi felhasználó tanúsítványozott nyilvános kulcsa tárolásra kerül a névtárban.

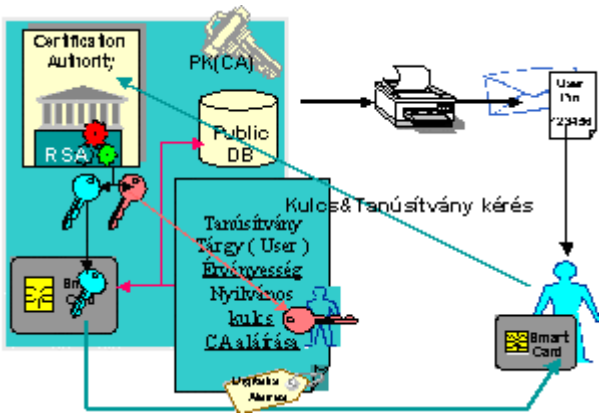
Hitelesítéskor az alkalmazás kliens chip kártyáról olvassa be a privát kulcsot, LDAP protokollon keresztül éri el a névtárban lévő nyilvános kulcsot és ezen kulcsokkal különféle kombinációk szerint digitális aláírást képez. A kulcsok kombinálásával, a tartalmat is rejtjelezni (titkosítani, kódolni) lehet.

Fogadó oldalon, az alkalmazás kliens vagy szerver a saját nyilvános és privát kulcsa, valamint a küldő nyilvános kulcsának kombinálásával a rejtjelezett tartalomhoz hozzáfér, illetve a digitális aláírás hitelességét ellenőrzi. Az alkalmazás bármilyen jellegű lehet, a hitelesítés és titkosított adatkezelés az alkalmazás használói között történik. WEB-es alkalmazáskor a hitelesítési és titkosítási eljárások hasonló elvek szerint működnek, csak a szereplők közötti adatbiztos és hitelesített kapcsolatot, az on-line technológiákra jellemző adatbiztonsági és hitelesíti modulok biztosítják.

Kulcsok generálása

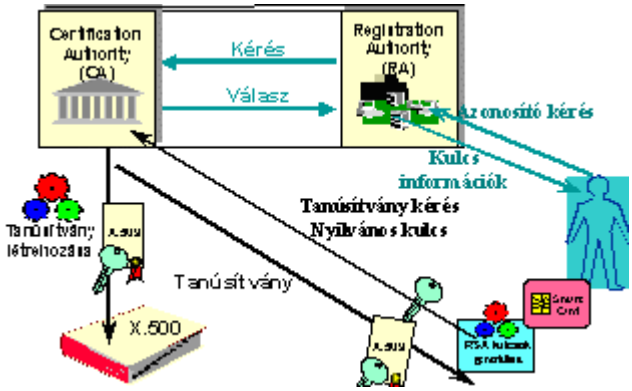
Alapvető biztonságtechnikai kérdés a kulcsok előállítási helye, ami valamelyik PKI elemen történik. A PKI rendszerek fejlődése során ez egyre több elemen vált lehetővé. Általánosságban két lehetőség kínálkozik a

kulcspárok generálására, és mindkettő rendelkezik mind a maga előnyeivel mind hátrányaival a CA illetve a felhasználó oldaláról nézve. A két lehetőséget centralizált és decentralizált kulcsgenerálásnak nevezzük.



Centralizált kulcspár generálás folyamata

Lényegét tekintve, központi (centralizált) kulcsgenerálásról beszélünk, amennyiben a kulcsokat a CA oldalon, illetve lokális kulcs előállításról (decentralizált), amennyiben a felhasználó vagy a RA oldalán állítjuk elő.



Lokális kulcspár generálás folyamata

A kulcsok generálásának jelenlegi legbiztonságosabb módja, ha olyan chip kártyán tároljuk a kulcsokat, amely egyben azok generálására is képes. Ezt a módszert nevezi az irodalom on-board kulcsgenerálásnak. A módszer biztonsága abból adódik, hogy az előállított kulcsok közül az egyén titkos kulcsa soha nem tartózkodik a kártya memóriáján kívül. A nyilvános kulcs a többi módszerhez hasonlóan kerül a CA-hoz. Minden valószínűség szerint biztonságossága miatt, ez utóbbi módszer fog a közeljövőben elterjedni.

PKI rendszer elemeinek ismertetése

Mint azt már a bevezetőben is említettük a PKI rendszer, olyan alkalmazás környezetet (infrastruktúrát) kínál, ami lehetővé teszi a törvények által elfogadott kétkulcsú harmadik személyes hitelesítési és adatbiztosítási eljárások használatát a számítógépes alkalmazások számára. A gyakorlatban, ezért a PKI elemei sokszor fontos alkalmazásintegrációs elemeket jelentenek, így a PKI bevezetése szorosan érintheti egy szervezet meglévő és a jövőben kialakulásra kerülő elektronikus dokumentumkezelő alkalmazásait. A PKI önállónak mondható elemeit, mint a CA, RA és a felhasználói modulok (kliensek) jelen fejezetben ismertetjük, de itt érdemes megjegyezni, hogy a valóságban mindezen elemek funkciói jelentősen integrálódhatnak az adott alkalmazásokban és azok tulajdonságaként is megjelenhetnek.

PKI elemként soroljuk fel a névtárakat is, noha az nem tartozik szorosan ide. A névtárakat azért érdemes mégis itt megemlíteni, mert az utóbbi idők LDAP integrációs és névtár technológiai fejlődése a névtárakat egyre inkább előtérbe helyezte a nyilvános kulcsok és tanúsítványok tárolására és elérésére (LDAP). A névtár

technológia önálló technológiának tekinthető és az utóbbi időben szintén jelentős alkalmazásintegrációs szerepre tett szert. A PKI rendszerek elterjedt alkalmazás környezetének tekinthető, ezért mindenképpen érdemes vele foglalkozni a PKI elemek ismertetésénél is. Jelen anyag végén a névtár technológia alkalmazásintegrációs és PKI szerepével külön is foglalkozunk.

CA

A PKI rendszerek generációs fejlődése alapvetően arról szól, hogy a CA és az RA milyen funkciók kezelésében válik el egymástól. Kezdetben (első generációs PKI rendszerek) nem is volt külön RA egység, minden regisztrációs adminisztrációt a CA-n végeztek. A további generációk során (második, harmadik, negyedik) az RA egyre több adminisztrációs funkciót vesz át és a policy management is többnyire itt került kialakításra. Mindezek miatt a CA és az RA funkciók szétválasztása attól függ, hogy éppen milyen generációs rendszerről beszélünk, ezért alábbi (negyedik generációs) szétosztásunk sem minden gyártó esetében igaz.

A **CA** lényegesebb funkciói az alábbiakban foglalhatók össze:

- RSA kulcspárok generálása
- X.509 tanúsítványok kibocsátása (a CA által aláírva)
- nyilvános kulcsok személyekhez kötése
- tanúsítvány visszavonási listák generálása (Certificate Revication List)
- adatbázisok és névtárak kezelése
- master kulcsok kezelése

CRL (Certificate Revocation List): azoknak a tanúsítványoknak a listája, amelyek valamilyen okból kifolyólag vissza lettek vonva. A visszavonás általában az RA által igényelt folyamat, melynek során az adott tanúsítvány már nem használható tovább. A okok között szerepelhet például az, ha a tulajdonos elvesztette kártyáját, vagy esetleg az általa igénybevett szolgáltatás megszakadt, vagy akár a CA kulcs kompromittálása. A CRL „lista” megfelelő időközökben való frissítése és publikálása az egyik legfontosabb kérdése a policy-nak. Szabályozni kell a CRL maximális érvényességének idejét, a benne található tanúsítványok lejáratának idejét, valamint gondoskodni kell a CRL megfelelően sűrű periódusokban való közzétételét egy mindenki által hozzáférhető helyen. A CRL közzététele leggyakrabban X.500 névtárakban történik, amelyeket az alkalmazások a CRL letöltése érdekében periódikusan érnek el.

RA

A negyedik generációs PKI rendszereknél az RA egyre inkább a rendszer adminisztációs és eljárás központjává válik. Az esetek többségében a CA mint szolgáltatás is rendelkezésre állhat.

Az **RA** lényegesebb funkciói az alábbiakban foglalhatók össze:

- felhasználó azonosító generálása
- felhasználó kulcs kérése a CA-tól
- felhasználó kulcs fogadása a CA-tól
- felhasználó kulcs fájlban való tárolása
- felhasználó kulcs kártyán való tárolása
- tanúsítvány visszavonás kérése a CA-tól
- felhasználó policy menedzsmentre
- felhasználó kulcs megújítás / frissítés kérelmekre
- kulcs-visszaállítás
- felhasználó törlés
- eseménynaplózás
- felhasználó kulcs tárolására (smart-kártyán vagy PKCS#12 kulcs fájlokban)
- smart-kártya kibocsátására, menedzsmentje
- policy fájl-exportálások
- felhasználó tanúsítványok kérelmére
- kérelmek visszavonására
- tömeges kulcs és tanúsítvány kezeléssel kapcsolatos műveletek batch üzemmódú kezelése

A PKI rendszer menedzselése szempontjából rendkívül fontos a policy menedzsment kialakítása, ami a kulcsmenedzsmentről és általában arról szól, hogy a rendszerben kinek, illetve melyik rendszer elemnek milyen funkcionális jogai vannak. A policy management kezelését általában az RA végzi és az RA kommunikál

evvel kapcsolatban a többi rendszer komponenssel (CA, user agent).

User Agent (PKI kliens)

A User Agent olyan alkalmazás, amely a végfelhasználó gépén kerül installálásra és a felhasználó kulcsokkal tanúsítványokkal és chip kártyákkal kapcsolatos műveleteket tesz lehetővé. Ezek a műveletek, amelyeket csak a végfelhasználó végezhet el, függnek az RA policy előírásoktól. A kliens funkciók szintén függnek attól, hogy milyen generációjú PKI rendszerről van szó. A magasabb generációjú rendszerekben a kliensek több funkcióval is felruházhatók amit általában a policy menedzsment határoz meg.

A **User Agent** tipikus funkciói:

- digitális alírás képzés
- kódolás, dekódolás
- hitelesítési eljárások
- tanúsítvány kérelmek
- kulcs megújítás kérelmek (jogosultság esetén)
- visszavonási kérelmek, (jogosultság esetén)
- a helyi RSA kulcs pár generálása, smart kártya kibocsátás (jogosultság esetén)

Az adatbiztonsági felhasználói modulok más felhasználói alkalmazáshoz is kapcsolódhatnak. A PKI engedélyezett alkalmazások fejezetben láthatjuk, hogy a PKI integráció során a kliens kerül leginkább integrálásra, sokszor olyan mértékig, hogy a kliens kezelése teljesen az adott alkalmazás keretében történik.

PKI engedélyezett rendszerek

Mit jelent az, hogy PKI engedélyezett? Funkcionálisan a kétkulcsú kódolási és azonosítási, hitelesítési eljárások alkalmazását a különféle kialakítású adatvédelmi és azonosítási szituációkban, alkalmazásokban. A gyakorlatban mindez azt is jelentheti, hogy egy chip kártyával több rendszerbe (alkalmazásba) is be lehet lépni vagy több értelemben lehet digitálisan aláírni, illetve adattartalmat kódolni vagy kódolt adattartalmat elérni. A PKI alapú elektronikus hitelesítési és adatbiztonsági eljárások más adatbiztonsági környezetre épülve is használhatók. vagyis a PKI engedélyezett adatbiztonsági rendszerek további biztonsági szolgáltatásaihoz, a PKI azonosítási technológiák szerint lehet hozzáférni. (pl.: egy VPN hálózatba, számítógépbe belépni, kódolni.) E fejezet néhány mondatban próbálja összefoglalni a PKI engedélyezés értelmét az egyes alkalmazások esetében.

Mail, MS-Office, Notes dokumentumok digitális aláírása, adattartalom kódolás

Az elterjedtebb elektronikus dokumentumkezelő környezetekbe, mail rendszerekbe integrálható PKI kliens és kártyakezelő modulok, a digitális aláírás egyszerű generálhatóságát és azonosíthatóságát teszik lehetővé (2-3 klikkelés). A modulok vezérlése általában addicionális kezelő gombokkal vagy párbeszéd panelokon keresztül történik az ismert szoftver környezetben (pl.: MS Office vagy Notes)

Alkalmazásba ágyazható PKI modulok (tool kit-ek)

Minden olyan alkalmazásban szükség lehet digitális aláírásra, kódolásra, ahol partnerek egymás között elektronikus dokumentumokat akarnak cserélni hivatalos, bizalmas formában. Az ilyen alkalmazások nagyon sok félék lehetnek és azért, hogy ezeknél is hasznosíthatók legyenek a PKI eljárások, a PKI modulokat az adott alkalmazásba ágyazható toolkit-ként integrálják a rendszerbe. Ilyenkor általában a PKI modulok vezérlését teljesen az adott alkalmazás végzi és az esetek többségében a PKI szolgáltatásokat az adott alkalmazás felhasználói felületéről lehet igénybe venni.

Számítógépekbe és alkalmazásokba való belépés hitelesítése, adatok kódolása

Minősített hitelesítésű belépés engedélyezése számítógépekbe, egyes számítógép alkalmazásokba. A chip kártyás beléptetés fokozott biztonságot jelent létfontosságú alkalmazások kezelésénél, adminisztrálásánál. Itt érdemes megjegyezeni, hogy a PKI és chip kártyás technológia alkalmazásánál lehetőség nyílik arra, hogy több alkalmazásba fokozott ellenőrzés és azonosítás mellett egy chip kártyával is be lehessen lépni, Például egy pin kódot kell egy olyan banki alkalmazottnak megjegyeznie, aki több bizalmas alkalmazáshoz kénytelen munkakörileg hozzáférni. Mindez feleslegessé teszi a sok alkalmazás esetében jelentős munkával járó password adminisztrációt (jelszavak rendszeres cseréje, biztonságos terítése, stb.). A PKI technlológia lokális adatok helyszíni kódolását is lehetővé teszi. (pl.: merevlemez kódolása.) A kódoltan tárolt anyagokhoz való hozzáférés, szintén PKI hitelesítési eljárások szerint végezhető.

Helyi hálózatok adatbiztosítása

Helyi hálózati erőforrásokhoz való hozzáférés engedélyezésére az azon futó adatok titkosítására, szintén alkalmazható a PKI technológia. A helyi szerver(ek) esetén a különféle file-csoportok (file szerver) alkalmazások (alkalmazás szerver) elérése elvileg csak valamilyen szintű hitelesítés során végezhető el. (pl.: hálózati jelszavak, erőforrás hozzáférési jelszavak). Mindez PKI chip kártyás technológiával kiegészítve sokkal megbízhatóbbá és egyszerűbbé tehető. Olyan alkalmazás és file szerver környezetben, ahol a hálózati vagy alkalmazói szoftver beépített védelmi és azonosítási rendszere nem elegendő, ott e technológia mindenkép biztosítani tudja a szükséges védelmet. A helyi gép hozzáféréseit engedélyező chip kártya a hálózati hozzáférések kezelésére is használható, ami lehetővé teszi a hálózati password adminisztráció jelentős csökkentését.

VPN hálózatokon való hitelesítés és adatbiztosítás

VPN hálózatok kialakítására az esetek többségében akkor kerül sor, amikor nyilvános (pl.: Internet) vagy mások által is elérhető hálózaton kell biztonságos zárt felhasználói körű virtuális hálózatot létrehozni. A VPN funkciójából adódóan addicionális biztonsági eljárásokat használ a virtuális hálózat adat és hozzáférés védelmére, ami PKI eljárások keretében is történhet. A VPN felhasználói azonosításban az adatok titkosításában PKI alapú, chip kártyás megoldások alkalmazhatók.

WEB hozzáférés hitelesítése

Chip kártyás WEB hozzáférést biztosít a gyakorlatban. A PKI rendszer révén minősített azonosítás végezhető a beléptetésnél. Ebben az esetben a PKI kliens termékek, olyan WEB alkalmazásba ágyazható biztonsági modulokat jelentenek, amik böngészővel kezelhetők.

Single-sign on megoldás

E fogalom értelmezését és jelentőségét, talán gyakorlati jelentőségében lehet legjobban érzékeltetni. A digitális aláírás minden esetben biztonságosan azonosítja annak használóját, ezért az minden azonosítást igénylő elektronikus folyamatba egységes kezeléssel léphet be. A gyakorlatban például ez azt jelentheti, hogy ugyanazt a chip kártyát alkalmazva lehet számítógépekbe belépni, hálózati erőforrásokhoz hozzáférni, WEB vásárlást végezni, a cég VPN hálózatát otthonról használni, a hazavitt notebook adatait kódolni arra az esetre ha azt véletlenül ellopnák, reggel a cég kártyás azonosítású főbejáratán bemenni, aláírt hivatalos e-mailt küldeni és még sorolhatnánk a jelen és jövő alkalmazásait. A lényeg az, hogy a felhasználó digitális aláírásával egységes módon tud az elektronikus alkalmazások hiteles, törvény által elfogadott alkalmazója lenni. Mindez a hiteles elektronikus ügyvitelt egyszerűen kezelhetővé teszi, ami rendkívüli jelentőséggel bír a jövő szempontjából.

Forrás: http://www.ediport.hu