Madár János
SZINVA NET Informatikai Kft.
madar@szinvanet.hu

HARDVERES AZONOSÍTÁS ÉS INFORMÁCIÓVÉDELEM

Az informatikai biztonság

Az informatikai biztonság egy olyan állapot, amikor az informatikai rendszer védelme (a rendszer által kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása szempontjából) a következő tulajdonságokkal rendelkezik:

- **zárt:** az összes releváns fenyegetést figyelembe veszi a védelem,
- **teljes körű**: a védelmi intézkedések a rendszer összes elemére kiterjednek,
- **folyamatos:** az időben változó körülmények és viszonyok ellenére is megszakítás nélküli,
- **kockázatokkal arányos:** a védelem költségei arányosak a potenciális kárértékkel.

Az informatikai biztonság két alapterületet foglal magába. Az első terület az információvédelem, amely az adatok által hordozott információk sértetlenségének, hitelességének és bizalmasságának elvesztését hivatott megakadályozni. A második az informatikai rendszer megbízható működésének területe, amely az adatok rendelkezésre állását és a hozzájuk kapcsolódó alkalmazói rendszerek funkcionalitását hivatott biztosítani.

Ma a piaci környezetben az üzleti információk védelme az üzleti siker egyik fontos összetevője, így a digitálisan tárolt adatok és az adatokhoz történő hozzáférések biztonsága nélkülözhetetlen a megfelelő működéshez, működtetéshez. Minden információt kezelő személy, szervezet birtokában vannak bizalmas, titkos adatok, melyek elérhetőségét az üzlet és applikációk számára folyamatosan, a lehető legnagyobb biztonságot megtartva kell biztosítani. Az e-business és az elektronikus kereskedelem hatékony működésének elengedhetetlen feltétele, de fontos szempont mind a kormányzat, mind a vállalatok, mind a magánszemélyek részére is.

Egy internetes vagy intranetes környezetben a védett információkhoz történő hozzáférések egyik kulcskérdése a felhasználó azonosítása és jogosultságának kezelése. Erre a problémára kínál megoldást a **web-kulcs** biztonsági keretrendszer.

Web-kulcs rendszerleírás

A Web-kulcs egy olyan biztonsági keretrendszer, amely egyedileg kódolt hardverkulcs segítségével képes az internet és intranet felől érkező felhasználók egyértelmű, kényelmes és biztonságos azonosítására, követésére és jogosultságának keze-

lésére. A rendszer működése kliens-szerver alapú, ahol minden kliens rendelkezik egy az azonosításhoz szükséges hardver eszközzel. Ez a *DiskOnKey*. A rendszer ezt az eszközt azonosítja, de minden esetben szükséges a felhasználó jogosultságának ellenőrzése a kulcshasználathoz.

A hardver

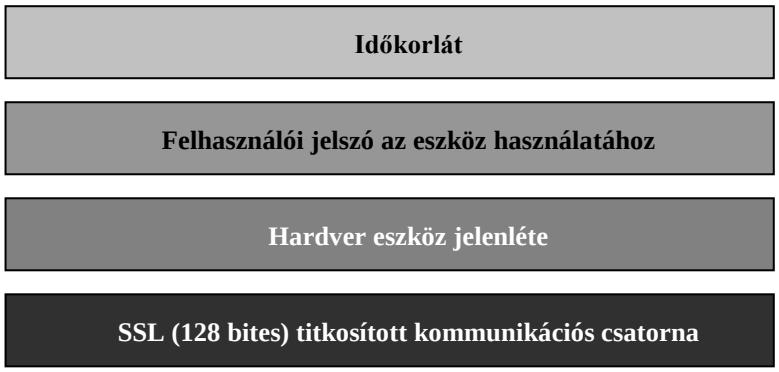
A DiskOnKey (*1. ábra*) egy *univerzális*, *biztonságos*, *megbízható* adathordozó eszköz, amely PKI alapokon biztosít kétmélységű felhasználó azonosítást. *Univerzális*, mert USB-n csatlakozik a számítógéphez, így Intel és Macintosh alapú gépekhez egyaránt csatlakoztatható. A számítógép azonnal felderíti, kiegészítő, hordozható lemezként ismeri fel és kijelöli egy újabb meghajtónak. Tárkapacitása 128MB-tól akár 4GB-ig is terjedhet. Támogatja a legújabb Windows, MacOS és Linux operációs rendszereket, (Windows 98 Second Edition, Windows 2000/Me/XP, MacOS 9.0 és fölötte, Linux 2.4.0), valamint NT alatt is használható. *Biztonságos*, mert akár a teljes kapacitás, akár csak egy része jelszóval védhető, így illetéktelenek nem tudnak hozzájutni a céges (esetleg titkos) adatokhoz, de bizonyos anyagokat így a gyerekek elől is el lehet rejteni. *Megbízható*, mert nem tartalmaz mozgó alkatrészt, kevésbé érzékeny az elektromágneses zavarokra, így a rajta lévő adatok nem sérülnek, ha pl. metrón utazik az ember, vagy mobil-telefon közelébe kerül az eszköz.

Minden DiskOnKey rendelkezik egy *ARM7 32-bit* mikroprocesszorral, ami lehetőséget biztosít olyan egyedi szoftveralkalmazások készítésére, melyek ezen processzoron keresztül kerülnek végrehajtásra. Ezek az alkalmazások minden olyan PC-n működnek, ahol Windows operációs rendszerek futnak, (Windows 98, Windows Me, Windows 2000 és Windows XP) és kiválóan alkalmasak például biztonságos adattárolásra, titkosításra vagy azonosításra.

1. ábra: DiskOnKey

Biztonsági szintek

A nagyobb biztonság érdekében a rendszer több biztonsági szintet különböztet meg, melyek egymásra épülnek a *2. ábra* hierarchiája szerint:



2. ábra: Biztonsági szintek a Web-kulcs rendszerben

A legalacsonyabb szinten áll a kommunikációs csatorna biztonsága, amely a kliens és a szerver gép között épül ki és a kapcsolat teljes időtartama alatt fennáll. Minden IP csomag titkosított formában közlekedik, így nemcsak a bejelentkezési információk, hanem a védett tartalom sem juthat illetéktelen kezekbe.

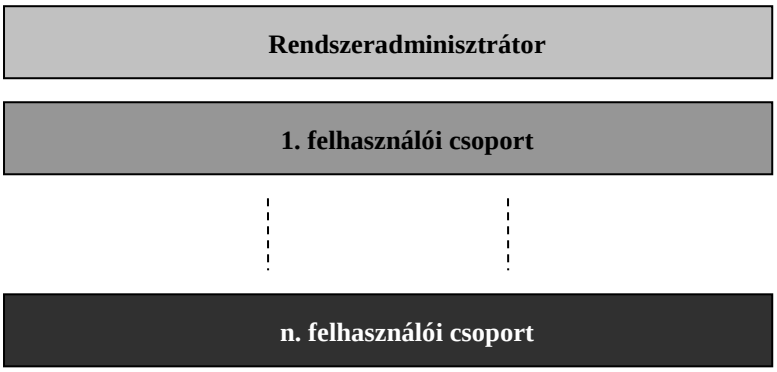
A következő szinten található a hardver eszköz jelenléte. Minden csatlakozó felhasználónak rendelkeznie kell ezzel az eszközzel, hiszen nélküle nem lehet kapcsolatot teremteni a rendszerrel. Ezen a szinten azonosítja a rendszer az eszközt.

A harmadik szinten jelenik meg a felhasználói azonosító, amely a kulcs használatának jogosultságát igazolja. Ez a „jelszó" csak a szerver felhasználói adatbázisában tárolt, a kulcson nem. Ezen a szinten azonosítja a rendszer a felhasználót.

A legfelső szinten található egy a bejelentkezés folyamatát és a kapcsolat idejét korlátozó tényező az időkorlát. Minden bejelentkezési kéréstől a felhasználó azonosításáig tartó időintervallum korlátozva van a rendszerben. Ezen időkorlát jelenleg 20 másodperc, ami elegendő idő a sikeres azonosításhoz, ugyanakkor ez túlságosan rövid idő ahhoz, hogy a jogosulatlanul betörni szándékozók bejussanak a rendszerbe. A kiépült kapcsolat ideje is korlátozott, jelenleg 8 óra. Az időkorlát túllépése esetén a rendszer automatikusan bontja a kapcsolatot a klienssel. Természetesen az időintervallumok módosíthatóak.

Hozzáférési szintek

A rendszer felhasználói között egy hierarchia értelmezhető, amely a hozzáférési szinteket szabályozza. Minden azonosított felhasználó csak a számára biztosított adatokhoz férhet hozzá. Az egyes szinteken nemcsak felhasználók, hanem felhasználói csoportok is állhatnak, és így a magasabb szinten lévők számára hozzáférhetővé tehetők az alatta lévő szintek számára biztosított adatok is. A hierarchia csúcsán a rendszeradminisztrátor áll, aki a teljes adathozzáférésen túl a rendszer paramétereit is módosíthatja, működését szabályozhatja. Az összes többi szint ez alatt helyezkedik el, ahogyan azt a *3. ábra* szemlélteti:



3. ábra: Hozzáférési szintek a Web-kulcs rendszerben

A rendszer szolgáltatásai

A Web-kulcs biztonsági rendszer alapvető szolgáltatása az internet felől érkező felhasználók egyértelmű és biztonságos azonosítása, valamint a felhasználók követése. Ezen túl olyan szolgáltatások is megtalálhatók benne, melyeket a már beazonosított felhasználók vehetnek igénybe: *adatmódosítás*, *Safe Login*, *FTP Browser*. Bizonyos szolgáltatások csak az adminisztrátor számára elérhetők: *felhasználó kezelés*, *rendszerinformációk*, míg a többi a hozzáférési szintekkel szabályozható. A rendszer tartalmazhat továbbá olyan – mindenki számára elérhető – adatokat is, amelyek nem követelik meg a felhasználó azonosítást. A kialakításnál törekedtünk mind a felhasználók, mind a rendszeradminisztrátor számára kényelmes, egyszerűen kezelhető, áttekinthető felületet biztosítani a használathoz. Ennek elemei:

- *Adatmódosítás*: Minden beazonosított felhasználó számára elérhető szolgáltatás, melynek segítségével a szerver felhasználói adatbázisában található felhasználói azonosító („password") változtatható meg.
- *Safe Login*: Minden azonosított felhasználó számára elérhető szolgáltatás, melynek segítségével a DiskOnKey védett (safe) adatterületéhez lehet hozzáférni a szükséges jelszó ismeretében. A védett területen elhelyezett adatállományok ezután feldolgozhatók a rendszerben.
- *FTP Browser*: Azok a felhasználók, akiknek ez biztosított, egy FTP szerveren elhelyezett adatállományok között tallózhatnak és tölthetnek le adatokat. Az FTP szerver hozzáférése korlátozott, csak a webszerverrel képes kapcsolatot teremteni. Minden, a felhasználó által letöltésre kijelölt, állomány ideiglenesen áttöltődik a webszerver, egy erre a célra kijelölt helyére, amely csak a letöltést kezdeményező felhasználó számára hozzáférhető mindaddig, amíg aktív kapcsolata van a rendszerrel.
- *Terminal Server kapcsolat*: A hozzáférési szinteknek megfelelően azon felhasználók, akiknek ez biztosított, terminal szerver kapcsolatot alakíthatnak ki a számítógépük és az erre a feladatra felkészített terminál kiszolgáló között. A kap-

csolat kiépítése után a távoli számítógépen futtathatnak programokat, vagy egy átjáróként használva azt, további kapcsolatot kezdeményezhetnek a belső hálózat felé. A kapcsolatok száma a rendszer keretein belül korlátozható, ellenőrizhető, kezelhető.

– *Felhasználó kezelés*: Csak a rendszeradminisztrátor számára elérhető szolgáltatás, melynek segítségével változtathat a rendszer felhasználói adatbázisában tárolt adatokon. Ennek segítségével csatlakoztathat újabb felhasználókat a rendszerhez; módosíthatja az egyes felhasználók hozzáférési szintjeit, adatait; tilthat vagy engedélyezhet felhasználói hozzáféréseket; törölhet felhasználókat. Az adminisztrátor minden műveletet „távolról" is elvégezhet, amihez csak azonosítania kell magát.
– *Rendszerinformációk*: Csak a rendszeradminisztrátor számára elérhető szolgáltatás, melynek segítségével tájékozódhat a rendszer aktuális állapotáról, valamint információkat kaphat a rendszer használatáról. Itt tekintheti meg a rendszerrel aktív kapcsolatban lévő felhasználók számát, kapcsolódásuk adatait, valamint itt találhatók meg a rendszer mögött működő naplózó tevékenység eredményei is. A naplózó tevékenység használható a felhasználók követésére. Minden bejelentkezési kérelemről, sikeres és sikertelen bejelentkezésről, kijelentkezésről naplózás történik. A naplóba bekerül a kliens publikus kulcsának titkosított alakja, IP címe, a végrehajtott művelet és annak pontos ideje. Sikertelen bejelentkezés esetén rögzítésre kerül annak oka is. Ha támadási kísérletről van szó, a rendszer automatikusan figyelmeztető levelet küld a rendszergazdának a kliens adataival. Természetesen a napló egyéb információkat is tartalmazhat.

Kapcsolat a rendszerrel

Egy internetes rendszer, ami csak meghatározott felhasználók számára férhető hozzá, általában tartalmaz valamilyen bejelentkezési folyamatot. Ennek során kell megadni egy felhasználói nevet és egy hozzá kapcsolódó jelszót ahhoz, hogy használni lehessen a rendszer szolgáltatásait. A felhasználói nevek és jelszó párok adatbázisban tárolódnak és a sikeres bejelentkezéshez mind a két adat pontos ismeretére szükség van. Használatuk *veszélyes*, hiszen ha illetéktelenek birtokába jutnak ezen adatok (akár a tudtunk nélkül), nem tudjuk megakadályozni a használatukat. Egy olyan rendszer, amely a Web-kulcsot használja a felhasználó azonosításához *biztonságos*, hiszen a bejelentkezési folyamatot az eszköz végzi. Ez egy eszközfüggő rendszer, ahol minden be- és kijelentkezés a kulcs használatával történi, az eszköz nélkül a felhasználó nem jogosult a rendszer használatára. Az eszköz viszont csak egy helyen lehet, így tudtunk nélkül nem, csak „beleegyezésünkkel" használható. (A kulcs elvesztése általában hamar kiderül, és – a bankkártyához hasonlóan – azonnal kitiltható a rendszerből.)

Minden DiskOnKey rendelkezik 2 darab 64 bájtos azonosítóval, amelyet kulcsoknak nevezünk. Az első kulcs az eszközön tárolt *privát kulcs*, amely nem ismert (eszközfüggőség). A második egy mindenki által hozzáférhető *publikus kulcs*, amely adatbázisban tárolt. (Minden eszköz ismeri a saját publikus kulcsát.) A bejelentkezés feltétele, hogy a felhasználó rendelkezzen egy olyan DiskOnKey eszközzel, amely-

nek publikus kulcsa a szerveren elhelyezett felhasználói adatbázisban rögzített és érvényes. Az azonosítás két lépésben történik. Első lépésben a rendszerhez csatlakozó DiskOnKey jelzi a bejelentkezési szándékát úgy, hogy elküldi a szervernek a publikus kulcsát. A szerver a felhasználói adatbázisban elhelyezett információk alapján dönti el, hogy a kérést küldő eszköz jogosult-e a bejelentkezésre (Tárol-e a publikus kulcsa? Nincs-e letiltva?). A belépésre nem jogosult kliensek kéréseit a rendszer elutasítja. A bejelentkezésre jogosult kérések kiszolgálásra kerülnek. A szerver válasza egy 63 bájtos véletlenszerűen generált érték, amelyet a kliensnek küld azzal a kéréssel, hogy a privát kulcsa segítségével kódolja le és küldje vissza. A DiskOnKey kódolja, majd visszaküldi a kódolt értéket. *Ez egy 64 bájtos, a privát kulcs használatával egy véletlenszerű 63 bájtos érték titkosított alakja.* A szerver a visszaküldött érték, a kiküldött érték és a kliens publikus kulcsa alapján dönti el, hogy engedélyezi-e a bejelentkezést (Visszakódolja a kliens által küldött kódolt értéket a publikus kulcs segítségével, majd összehasonlítja az általa kiküldött véletlenszerűen generált értékkel. Ha a két érték egyezik, akkor engedi a bejelentkezést, ha nem támadási kísérletnek veszi.). Sikeres bejelentkezés esetén a kliens használhatja a rendszer számára engedélyezett szolgáltatásait, amíg kapcsolata van a rendszerrel. A DiskOnKey eltávolítása az USB kapuból a kapcsolat bontását eredményezi. *Az azonosítási folyamat során, az interneten keresztül csak olyan titkosított adatok közlekednek, amelyekből sem a felhasználó személye, sem az általa használt titkos kulcspár nem határozható meg.*

Egy felhasználói kapcsolat kezelése „session” használatával történik, ami adatbázisban tárolt. A „session” egy felhasználó belépése és távozása közötti folyamat. Minden bejelentkezési kérelem esetén létrejön egy egyedi azonosító, amivel a szerveren tárolt adathalmazt azonosít be a rendszer. Ez az adathalmaz tartalmazza a felhasználó adott belépéshez tartozó adatait. A „session” használata az *időkorláthoz* kötött. Fontos megjegyezni, hogy ennek az azonosítónak semmi köze nincs a felhasználó publikus kulcsához vagy a jelszavához, hiszen csak a szerveren tárolt adathalmazt azonosítja. Amikor a felhasználó bontja a kapcsolatát, akkor az adathalmazban tárolt összes adat törlődik. Az adatok soha nem kerülnek ki a szerverről, csak egy véletlen-generált hosszú azonosító közlekedik az URL-ben oldalról oldalra, amit hiába próbál meg bárki is változtatni, mert az egyetlen lehetőség az lehet, hogy eltalálja egy másik látogató generált azonosítóját, ami viszont a nagy véletlen számok miatt hiúsul meg. (Az azonosító egy 32 karakteres, betűkből és számokból álló karaktersorozat.)

Web-kulcs rendszerkövetelmények

A Web-kulcs biztonsági rendszer működése kliens-szerver alapú. Mind a szerver, mind a kliens oldalon szükségesek bizonyos feltételek a rendszer megfelelő működéséhez.

Szerver oldal

A szerver kialakításánál figyelembe kell venni, hogy a rendszer szerveroldalon is megköveteli a DiskOnKey használatát. Szükséges tehát egy DiskOnKey eszköz (a felhasználó azonosításánál a bejelentkezési információk kódolását végzi el) és egy USB porttal is ellátott szerver számítógép Windows operációs rendszerrel (Windows 2000 Server). A szerver oldalon futnia kell egy webszervernek (Apache), ami biztosítja a generált weboldalak megjelenítését. A webszervernek képesnek kell lennie biztonságos SSL kapcsolat létesítésére a klienssel. Szükség van egy adatbázis szerverre (mySQL), ami megvalósítja a „session" kezelést, valamint a felhasználói adatok tárolását (felhasználó publikus kulcsa, password, jogosultsága, állapota). Az adatbázisban továbbá tetszőleges adatok tárolhatók, amiket a rendszer a kliensek számára is láthatóvá tehet a felhasználó azonosítása után. Szükséges továbbá egy PHP értelmező, a dinamikus oldalak generálásához, és egy FTP szerver, ami képes a hozzáférhetőségét IP cím alapján korlátozni.

Kliens oldal

Minden kliens számítógépnek rendelkeznie kell USB porttal, valamint az alábbi Windows operációs rendszerek egyikével: Windows 98 SE, Windows Me, Windows 2000, Windows XP. Kliens oldalon szükség van egy webböngészőre, egy DiskOnKey eszközre valamint egy activeX vezérlőre, ami kapcsolatot teremt a böngésző és az eszköz között.