S, mint secure

Nagy Attila Gábor
Wildom Kft.
nagya@wildom.com

Egy fejlesztő, sok hozzáférés

- Web alkalmazások esetében a fejlesztést és a telepítést általában ugyanaz a személy végzi
- Több rendszerhez és géphez rendelkezik hozzáféréssel
  - SSH+SCP
  - Web adminisztrációs felület (HTTP, HTTPS)
  - WebDAV
- Mindegyik jelszót kér

Ugye már elfelejtettük?

- Nem titkosított protokollok:
  - Telnet
  - FTP
  - POP3
- *Nagyon* könnyen lehallgathatóak, és valaki folyton hallgatózik

Ideális esetben

- Minden hozzáférést más jelszóval használunk
- A jelszavakat nem írjuk le
- Néhány havonta mindet lecseréljük

Képtelenség!

- Egyszerű megoldások:
  - Jelszótárak
  - Mindenütt ugyanaz a (pár) jelszó
- Gyenge pont

További problémák

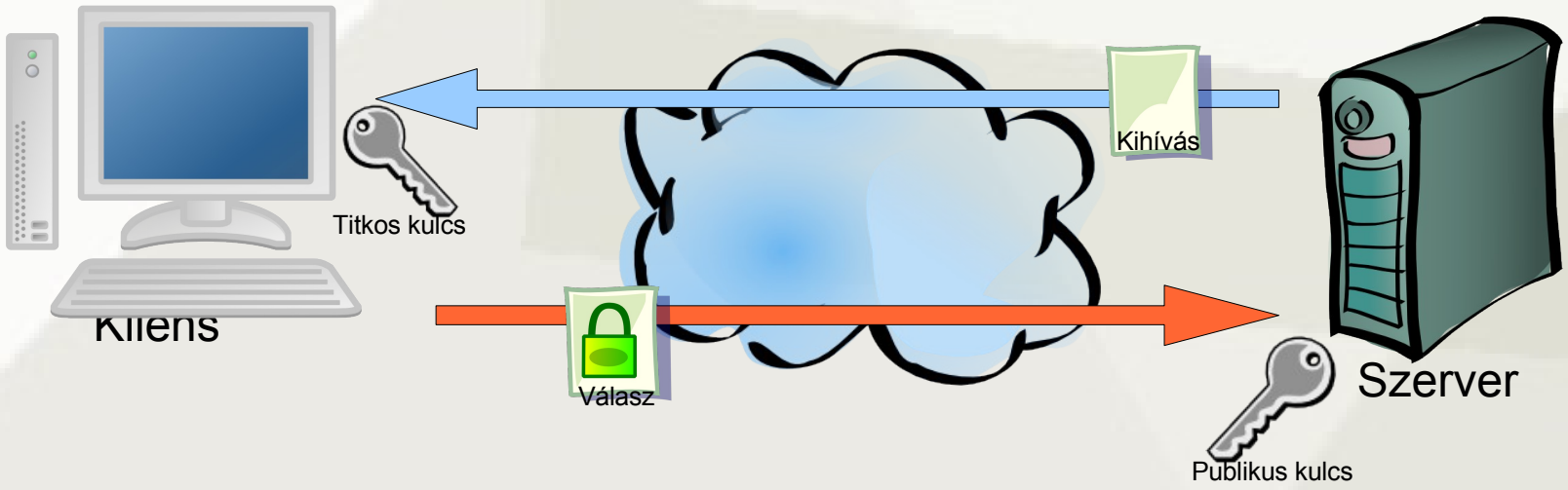
- Közös használatú hozzáférések (például telepítésre)
- Kényelmetlen mindig jelszót gépelni
- Jelszó csere nem biztonságos (emailben, telefonon, szóban)
- Kompromittálódott gép esetében még a biztonságos alkalmazások sem használhatóak
  - Például módosított, naplózó SSH szerver

Publikus kulcsú azonosítás

- Nincsen közös titok
- Asszimetrikus kulcsok
  - Titkos kulcs: a kliensnél, egy példányban
  - Publikus kulcs: a szervernél, szabadon közzétehető
- A titkos kulcsból bármikor előállítható a publikus, fordítva viszont nem lehetséges
- A titkos kulcsot soha nem kell a hálózaton átküldeni

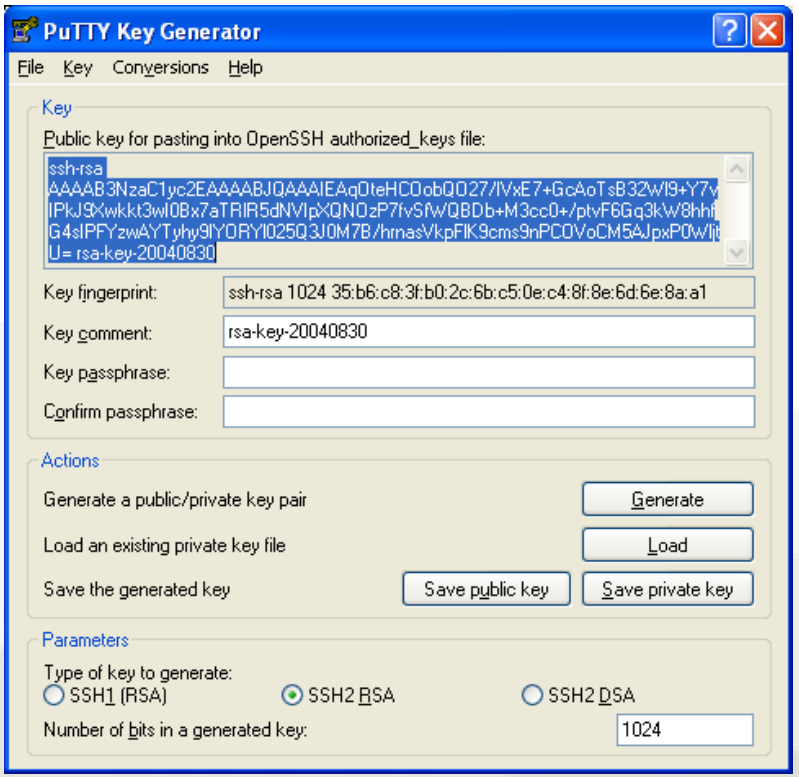
Azonosítás menete

- Szerver elküld egy kihívást
- A kliens a titkos kulccsal titkosítja (aláírja)
- Kliens visszaküldi az eredményt
- A szerver a publikus kulcs segítségével dekódolja, ellenőrzi



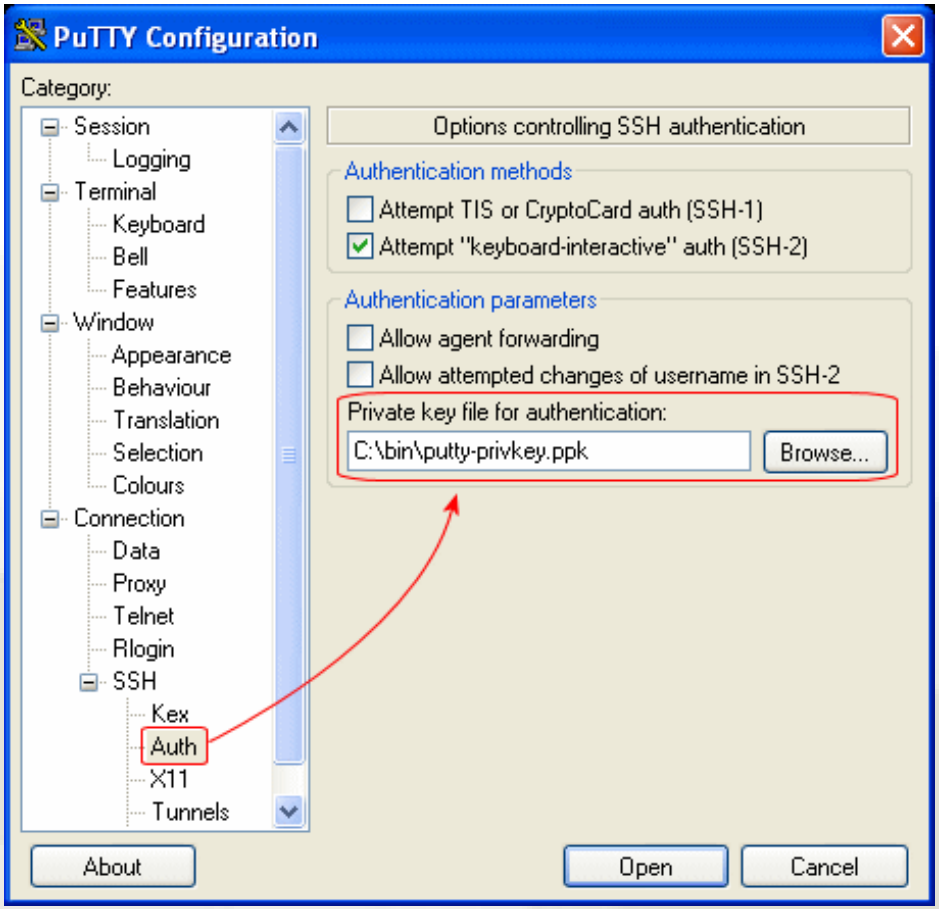
Beállítás

- Kell egy kulcspár
  - PuTTYgen
  - ssh-keygen -t dsa -C <comment>
  - Adjunk meg jelszót!
- Publikus kulcs elhelyezése:
  - Szerveren a ~/.ssh/authorized_keys fájlba



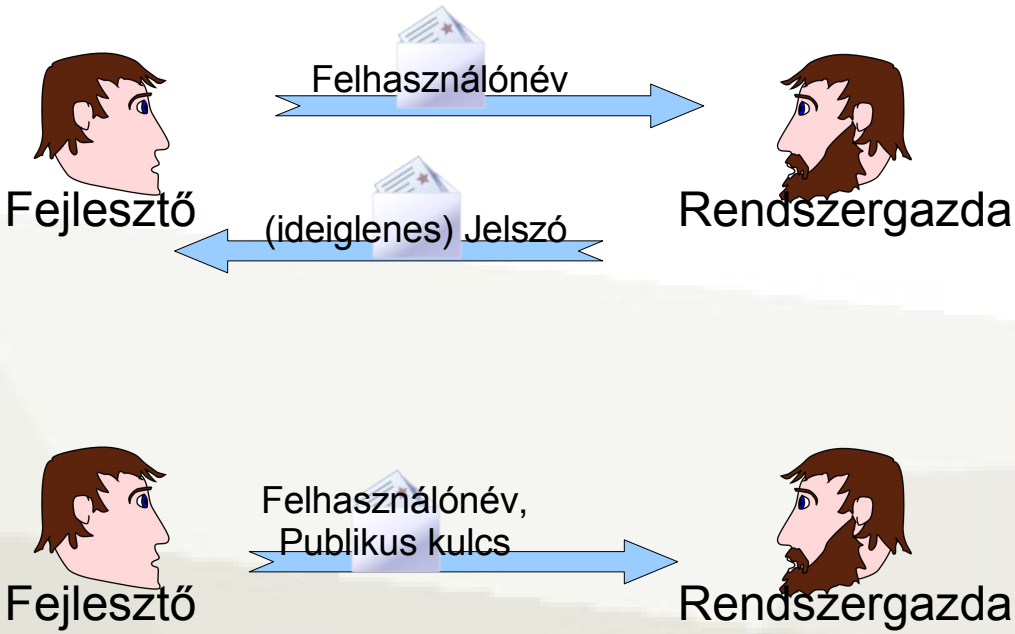
Belépés

- A belépéshez ki kell választanunk a titkos kulcsot, és meg kell adni a hozzá tartozó jelszót
- PuTTY:
  - Session adatai között
- OpenSSH:
  - ssh -i <kulcsfájl>



Már előnyben vagyunk

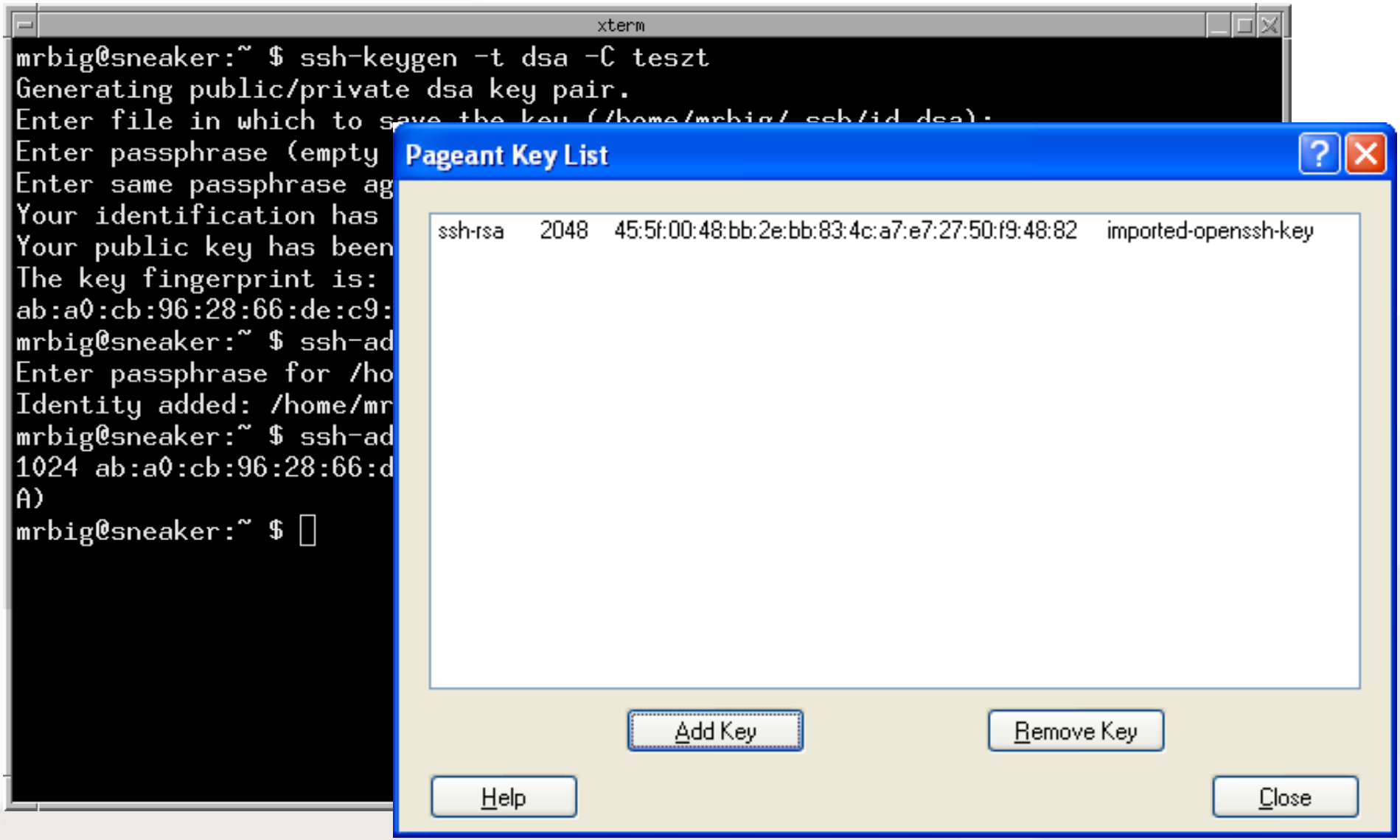
- Most már csak a publikus kulcsot továbbítjuk, jelszót nem
- Authentikáció során sem küldünk át érzékeny adatot
- Jelszó és kulcscsere elkülönül



Jó, de még mindig kell a jelszó!

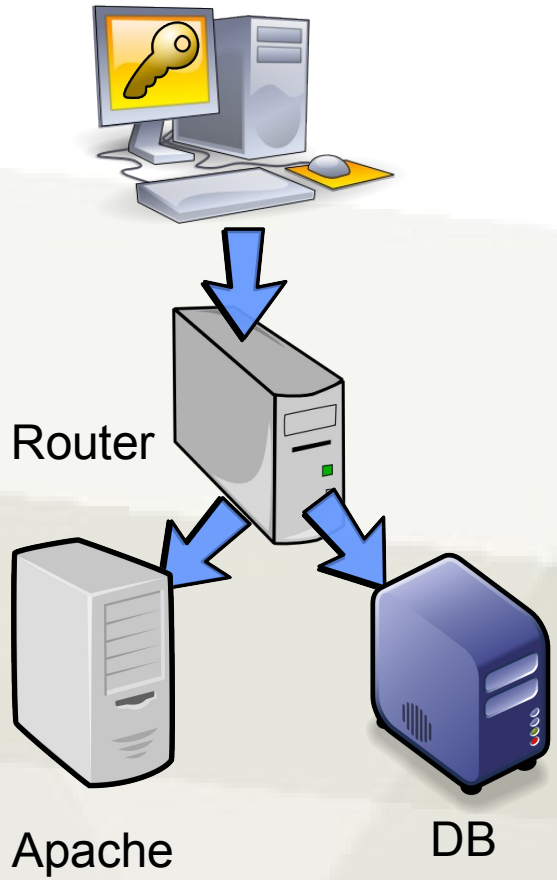
- SSH agent: a dekódolt titkos kulcsot tárolja a memóriában
- Elegendő egyszer megadni a kulcshoz tartozó jelszót
- Minden belépésnél elvégzi az aláírást
- PuTTY: Pageant
- OpenSSH: ssh-agent

Agent használata



Agent forwarding

- Több gépes szerver infrastruktúránál nagyon hasznos
- Elegendő csak az asztali gépre titkos kulcsot létrehozni
  - Kevesebb elveszteni való
  - Kevesebb adminisztráció



Szeretném ugyanezt HTTP-n!

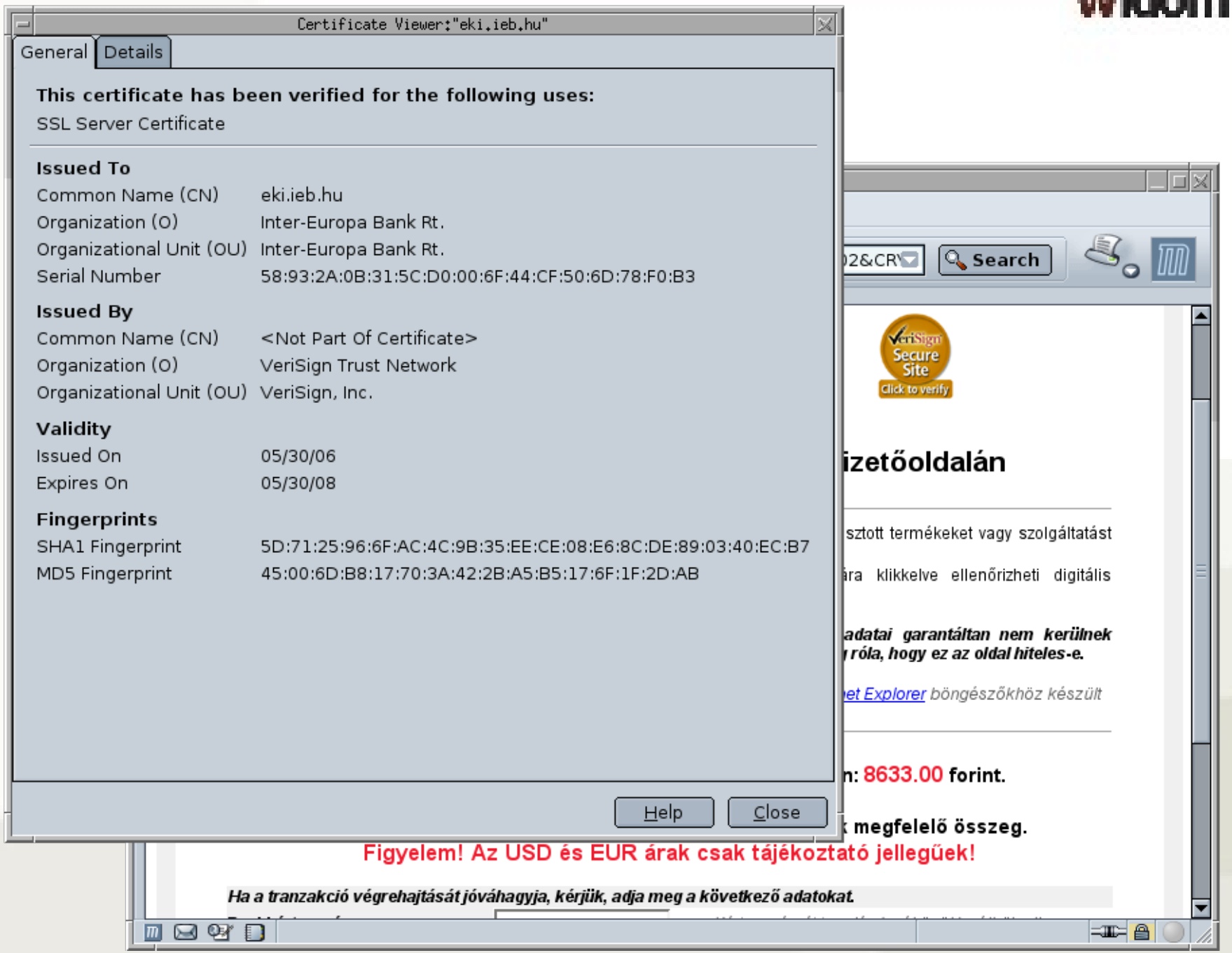
- SSL: működésben nagyon hasonló
- Fő szereplő a tanúsítvány:

  kulcspár

  + tulajdonos leírása

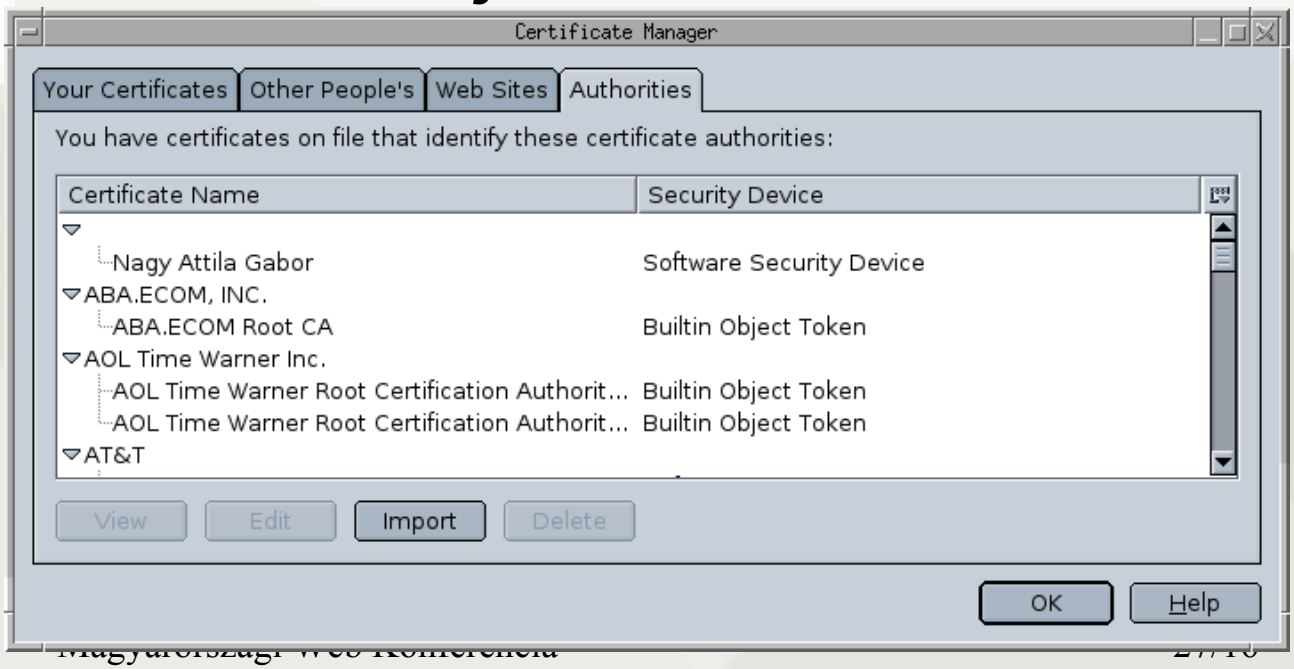
  + harmadik fél által hitelesítve

- Szervernek mindig kell tanúsítvány


Certificate Viewer:"eki.ieb.hu"
General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) eki.ieb.hu
Organization (O) Inter-Europa Bank Rt.
Organizational Unit (OU) Inter-Europa Bank Rt.
Serial Number 58:93:2A:0B:31:5C:D0:00:6F:44:CF:50:6D:78:F0:B3
Issued By
Common Name (CN) <Not Part Of Certificate>
Organization (O) VeriSign Trust Network
Organizational Unit (OU) VeriSign, Inc.
Validity
Issued On 05/30/06
Expires On 05/30/08
Fingerprints
SHA1 Fingerprint 5D:71:25:96:6F:AC:4C:9B:35:EE:CE:08:E6:8C:DE:89:03:40:EC:B7
MD5 Fingerprint 45:00:6D:B8:17:70:3A:42:2B:A5:B5:17:6F:1F:2D:AB
Help
Close
Search
VeriSign Secure Site Click to verify
izetőoldalán
sztott termékeket vagy szolgáltatást
ára klikkelve ellenőrizheti digitális
adatai garantáltan nem kerülnek
róla, hogy ez az oldal hiteles-e.
et Explorer böngészőkhöz készült
n: 8633.00 forint.
megfelelő összeg.
Figyelem! Az USD és EUR árak csak tájékoztató jellegűek!
Ha a tranzakció végrehajtását jóváhagyja, kérjük, adja meg a következő adatokat.

Hitelesítés menete

- A böngésző összehasonlítja hitelesítő szerv
  - tanúsítványon lévő aláírását
  - a böngészőben korábban tárolttal
- Megbízható hitelesítők listája bővíthető



Kliensnek is lehet

- Személyre szóló tanúsítványok
- SSL szintjén már azonosítjuk a klienst
- Tanúsítványellenőrzési lehetőségek
  - nem kell
  - opcionális bemutatni
  - kötelező bemutatni
  - Apache: SSLVerifyClient

Tanúsítvány előállítása

- Certificate Authority telepítése
  - Például: OpenSSL (alap), Microsoft CA
  - Self-signed certificate előállítása
    - A CA-ra szól
- Tanúsítvány igény előállítása: kulcs + váz
  - Személyre szól
- CA aláírja a tanúsítványt (*nem a kulcsot!*)
- Ügyfél használja a kulccsal együtt

http://www.oreillynet.com/pub/a/security/2004/10/21/vpns_and_pki.html

Lekérdezés Apache oldalán

HTTPS_KEYSIZE	256
HTTPS_SECRETKEYSIZE	256
SSL_CLIENT_DN	/C=HU/O=Wildom Kft./CN=Teszt User/emailAddress=teszt@wildom.com
SSL_CLIENT_C	HU
SSL_CLIENT_O	Wildom Kft.
SSL_CLIENT_CN	Teszt User
SSL_CLIENT_EMAILADDRESS	teszt@wildom.com
SSL_CLIENT_S_DN	/C=HU/O=Wildom Kft./CN=Teszt User/emailAddress=teszt@wildom.com
SSL_CLIENT_S_DN_C	HU
SSL_CLIENT_S_DN_O	Wildom Kft.
SSL_CLIENT_S_DN_CN	Teszt User
SSL_CLIENT_S_DN_EMAILADDRESS	teszt@wildom.com
SSL_CLIENT_I_DN	/C=HU/L=Budapest/O=Wildom Kft./CN=Wildom Kft/emailAddress=nagya@wildom.com
SSL_CLIENT_I_C	HU
SSL_CLIENT_I_L	Budapest
SSL_CLIENT_I_O	Wildom Kft.
SSL_CLIENT_I_CN	Wildom Kft
SSL_CLIENT_I_EMAILADDRESS	nagya@wildom.com
SSL_CLIENT_I_DN_C	HU
SSL_CLIENT_I_DN_L	Budapest
SSL_CLIENT_I_DN_O	Wildom Kft.
SSL_CLIENT_I_DN_CN	Wildom Kft
SSL_CLIENT_I_DN_EMAILADDRESS	nagya@wildom.com
SSL_CLIENT_M_SERIAL	01
SSL_CLIENT_V_START	Mar 30 07:45:44 2007 GMT
SSL_CLIENT_V_END	Mar 29 07:45:44 2008 GMT
SSL_CLIENT_M_VERSION	3

- PHP-ban: $_SERVER
- Környezeti változókból elérhető
  - SSL_CLIENT_xxx
- PERL, CGI-ből is használható

Alkalmazási lehetőségek

- Webfelület elérésének korlátozása
  - Csak tanúsítvánnyal rendelkező felhasználók
  - Bármikor visszavonható
    - (CRL – Certificate Revocation List)
  - Automatikusan lejár
- Kliens naplózása
- Automatikus beléptetés
- Automatikus felhasználó létrehozás

Hogyan tároljuk a kulcsokat?

- A titkos kulcsból csak egy példány megengedett
  - Ezért gépenként külön kulcs
- Merevlemezről észrevétlenül ellophatják
  - Időszakonként cserélni
  - Mobil adathordozón:
    - Pen drive
    - CD
    - (Floppy)

Tokenek

- Erre a célra kifejlesztve:
  - SmartCard (kártya + olvasó)
  - USB Token
- Minden funkciót egy chip lát el:
  - Kulcs generálás
  - Kulcs tárolás
  - Aláírás
- Egyirányú tároló: a kulcsot soha nem adja ki

USB Token: kisebb infrastruktúrákhoz

- Nem kell kártyaolvasó
  - Aladdin e-Token
  - Rainbow iKey 3000
  - *SafeNet iKey 4000*
- Sajnos nem mindegyik tud PKI-t
- PKCS#15, PKCS#11 kompatibilitás szükséges

Meghajtó programok

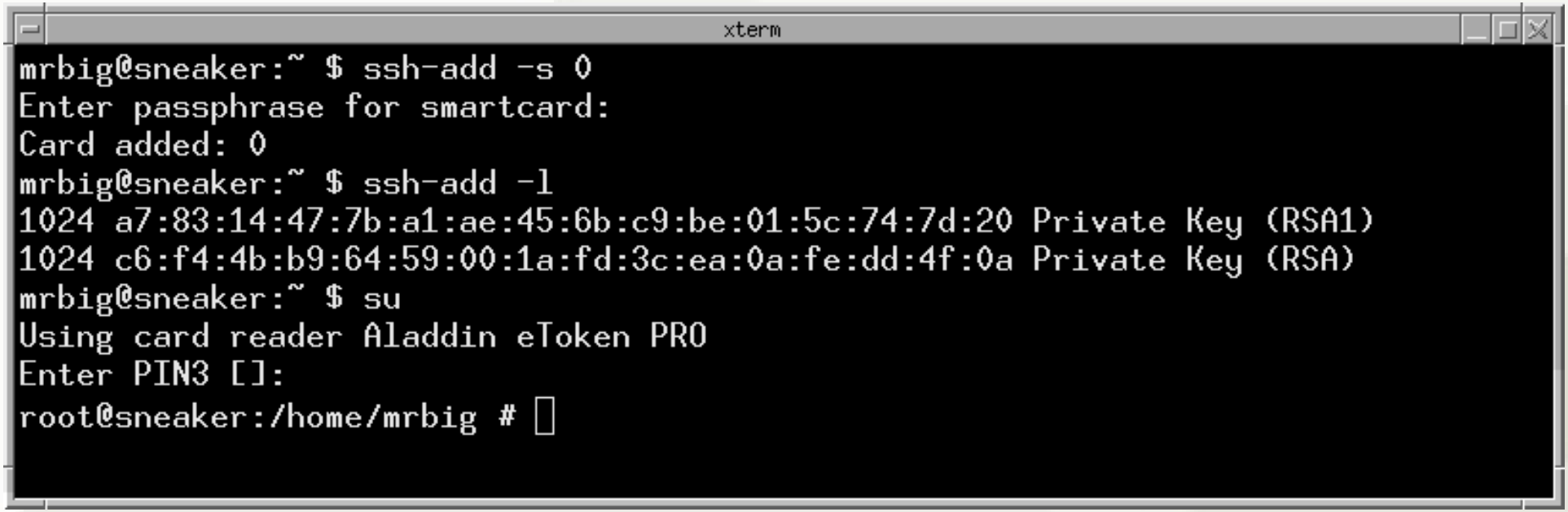
- Ahány gyártó, annyiféle driver
  - PKCS#15 szabvány a kártya API-ra, de nem mindenki tartja be
- Gyártó független interface: OpenCT, OpenSC
- Open-source, cross-platform:
  - Linux
  - Windows
  - Mac OS X

Alkalmazási lehetőségek

- OpenSSH (ssh-agent segítségével)
- PuTTY (PageAnt)
- Mozilla, Firefox, Thunderbird
- PGP
- OpenSSL (webszerver, VPN)
- PAM – általános körű authentikáció
- LDAP, Kerberos, ActiveDirectory

Alkamazása

- Napi rutin részévé válik
- Egyetlen jelszó, az is ritkábban
- Ellophatatlan



Linkek

- OpenSC:
  - http://www.opensc.org
- Aladdin eToken:
  - http://www.aladdin.com/etoken/usb_device.asp
- SafeNet iKey 4000:
  - http://www.safenet-inc.com/products/tokens/ikey4000.asp