BEZPEČNOSTNÍ SYSTÉM

Obsah

- AreaGuard® a jeho místo v bezpečnostní infrastruktuře organizace
- Jednotlivé moduly systému AreaGuard®
- Praktická ukázka
- Práce se šifrovacími klíči

Komponenty PKI

- Provedení analýzy rizik a vytvoření bezpečnostní politiky.
- Serverová strana – CA, LDAP (AD).
- Klientská strana – bezpečnostní mechanismy klientské pracovní stanice - AreaGuard®.

Bezpečnostní mechanismy

- Bezpečná autentizace
- Transparentní šifrování souborů
- Šifrování e-mailů
- Elektronický podpis
- Bezpečná komunikace (VPN klient)

Požadavky na uživatele

- Uživatel musí pracovat ve standardním (známém) prostředí
- Bezpečnostní mechanismy nesmí být závislé na chování uživatele
- Chování uživatele podléhá celkové bezpečnostní politice organizace

AreaGuard® moduly

- **AreaGuard® Gina** – autentizace
- **AreaGuard® Notes** – on-line šifrování dat
- **AreaGuard® FirmWall** – ochrana proti manipulaci s daty
- **AreaGuard® AdminKit** – administrace s centrální a vzdálenou správou

AreaGuard® Gina

- Autentizace do operačního systému pomocí HW tokenu
- Autentizace pomocí hesla nebo certifikátu a privátního klíče uložených v HW tokenu
- Synchronizace obsahu HW tokenu s OS

AreaGuard® Notes

- On-line šifrování složek a souborů pomocí symetrické kryptografie
- Šifrované složky na lokálních, síťových a výměnných discích
- Citlivé soubory jsou na disku vždy uloženy v zašifrovaném tvaru

AreaGuard® FirmWall

- Privilegované aplikace a chráněné oblasti (složky)
- Privilegovaná aplikace může ukládat soubory pouze do příslušné chráněné oblasti
- Soubory z chráněných oblastí nelze zkopírovat do jiné oblasti (složky)

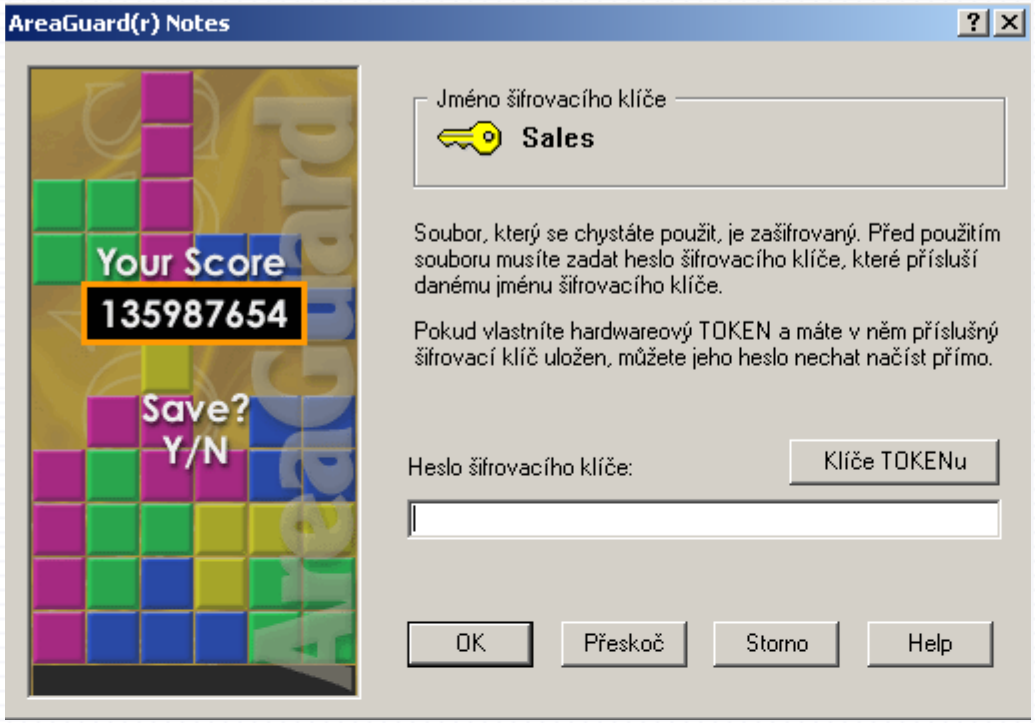
AreaGuard® AdminKit

- Automatická instalace a konfigurace koncové stanice
- Evidence uživatelů, šifrovacích klíčů a konfigurací pracovních stanic
- Záloha šifrovacích klíčů sloužící k obnově dat
- Vzdálená správa šifrovacích klíčů a konfigurací pracovních stanic

Praktická ukázka

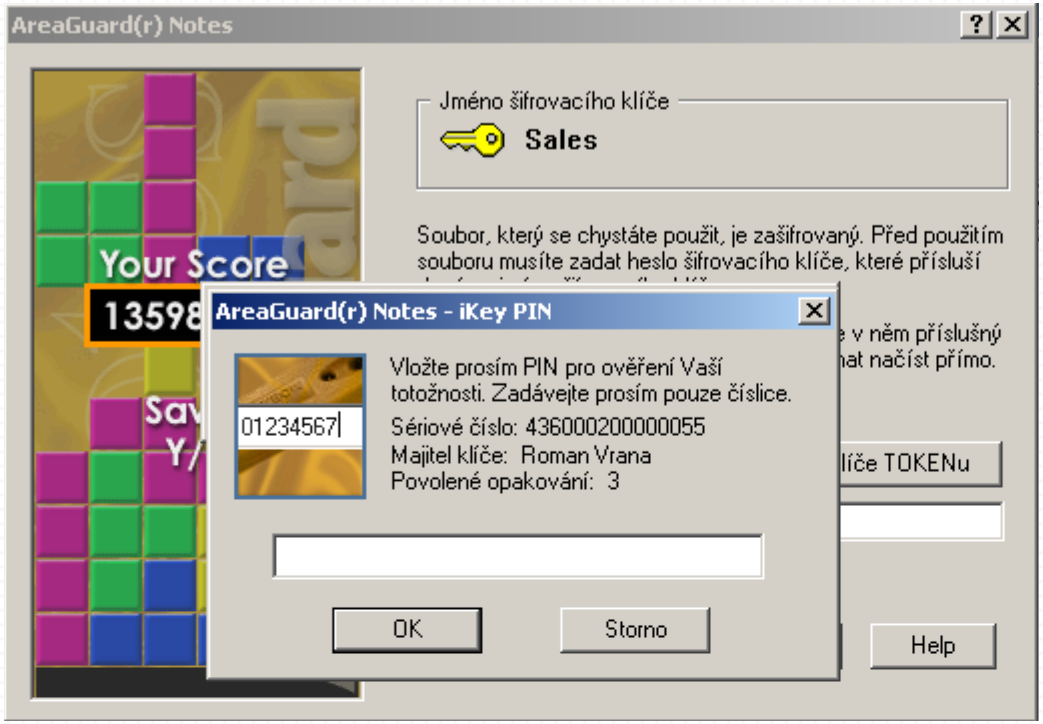
- Práce běžného uživatele se systémem AreaGuard®
- Lokální administrace systému AreaGuard®
- Centrální a vzdálená správa

Přístup k šifrovanému adresáři



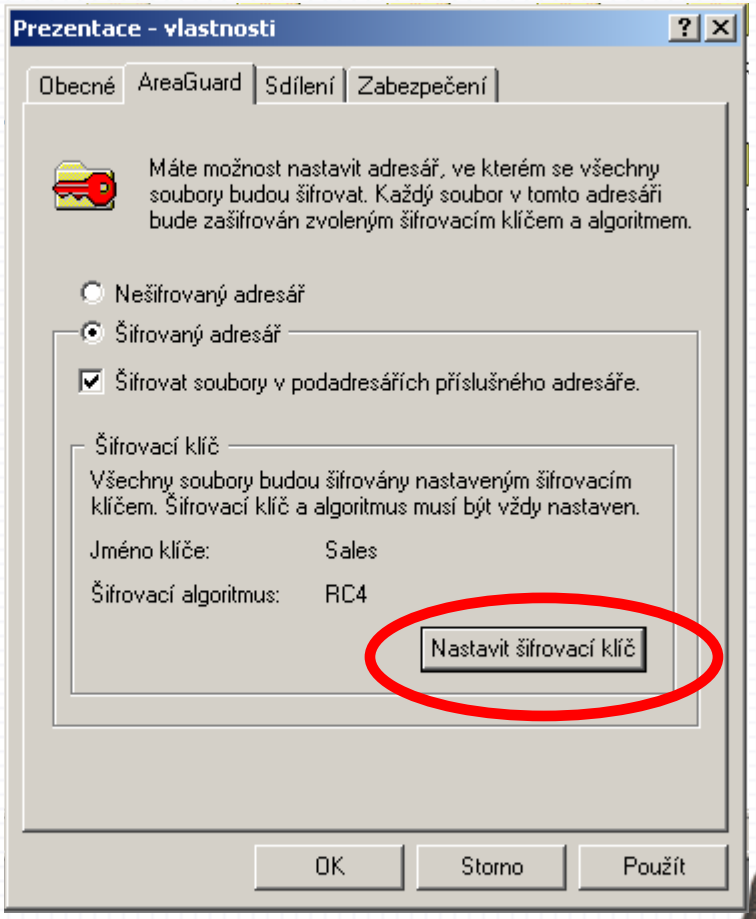
sodat

Načtení šifrovacích klíčů z HW prostředku iKey-1000



Nastavení automaticky šifrovaného adresáře

Kopírované soubory do šifrovaného adresáře a nové v něm vytvářené jsou automaticky šifrovány nastaveným šifrovacím klíčem.



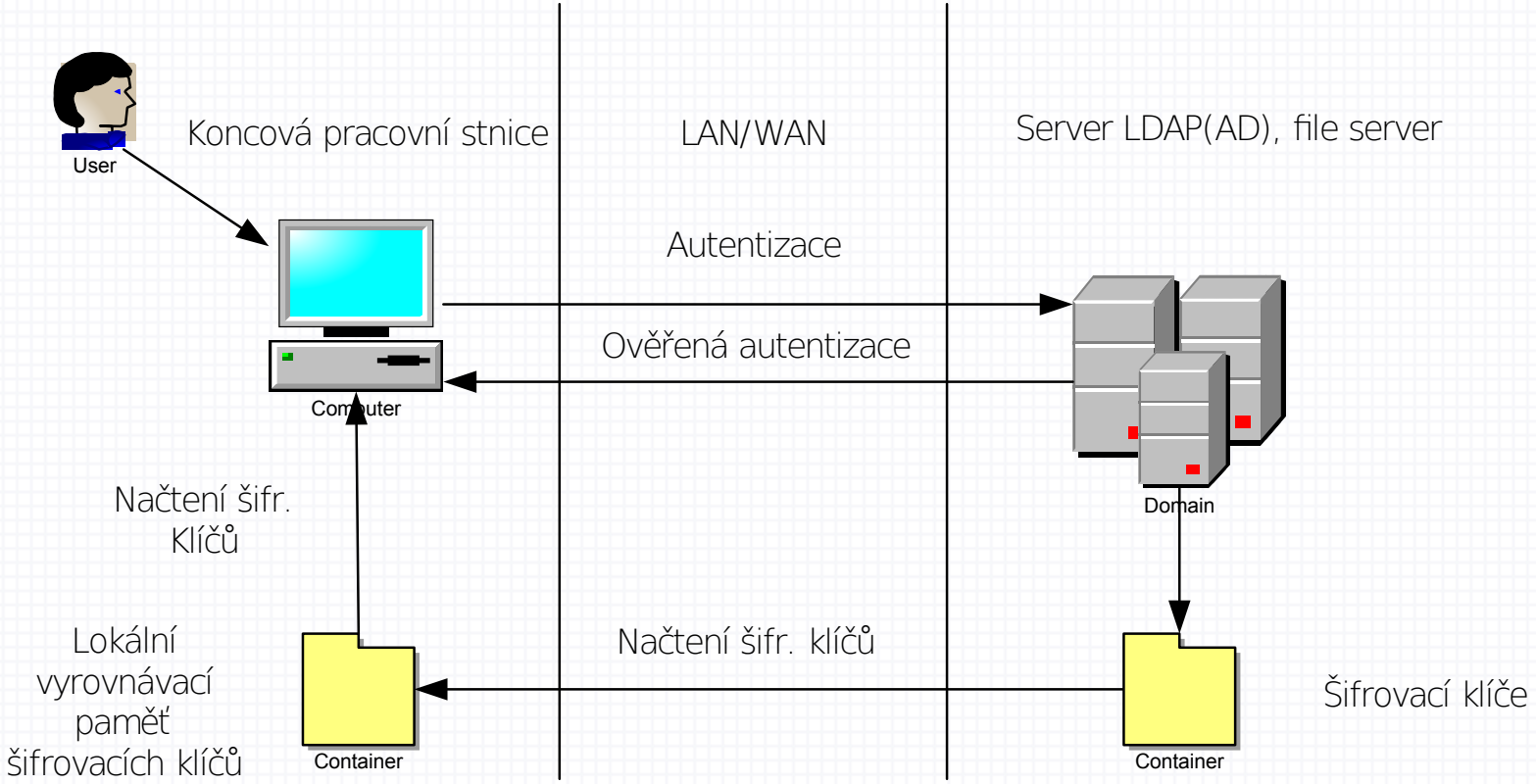
Šifrovací klíče uživatele

- Certifikát s privátním klíčem k autentizaci a e-podpisu
- Certifikát s privátním klíčem k šifrování e-mailů
- Symetrické šifrovací klíče k on-line šifrování souborů a složek

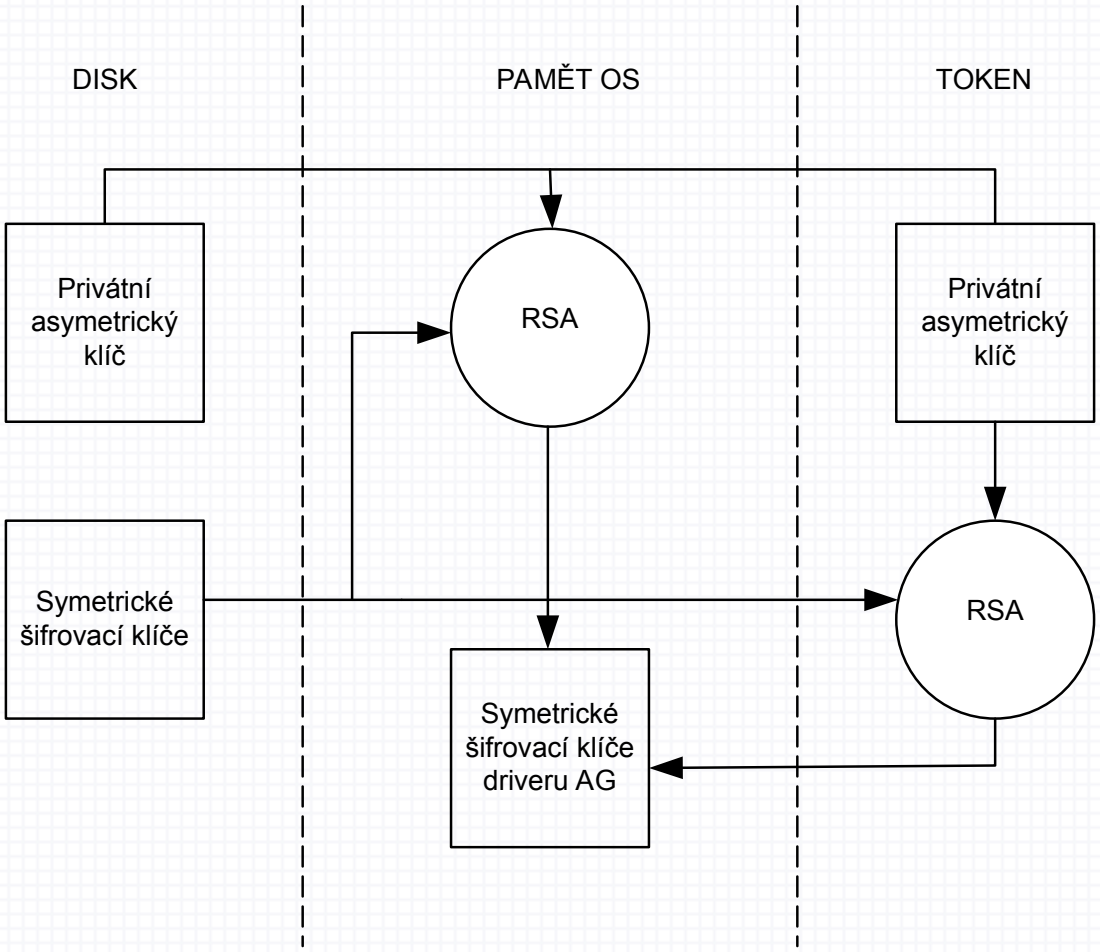
Uložení šifrovacích klíčů

- V souboru nebo registrační databázi
- V HW tokenu bez RSA šifrovacího algoritmu
- V HW tokenu s RSA šifrovacím algoritmem

Centrální sklad informací systému AreaGuard®



Příprava symetrických šifrovacích klíčů pro AreaGuard® Notes



Závěr

- Nikdo nemůže vyloučit možnost ztráty dat
- Ochrana dat šifrováním silnou kryptografií
- Uložení šifrovacích klíčů do HW prostředku
- Zachování zašifrovaného souboru při přenosu do jiných než chráněných oblastí
- Možnost sdílení dat více uživateli
- Ochrana soukromých dat i před správci systému
- Možnost vytvoření SFX souboru např. pro zasílání důvěrných dat e-mailem

Děkujeme za pozornost

www.areaguard.cz
www.areaguard.com

... and users have a better sleep

SODAT software, Sedlákova 33, BRNO, Czech Republic