

Bezpečná mobilní kancelář


sodat
SOFTWARE



AreaGuard

for Windows

www.areaguard.cz

bezpečná autentizace uživatele do Windows
on-line šifrování dat
bezpečné uložení šifrovačích klíčů v tokenu
elektronický podpis



Úvod

- Citlivá data
- Bezpečná autentizace do OS
- Cestovní notebook = pracovní stanice
- Ztráta přístroje - ztráta citlivých dat
- Současné ochranné funkce OS
- Ochranný mechanismus AreaGuard Notes



Citlivá data

- **Data organizace**
vnitrofiremní data - smlouvy, data s finančním tokem,
adresář s kontakty, e-mailové zprávy s důvěrným obsahem,
- **Soukromá data**

Cena notebooku < cena dat



Bezpečná autentizace

- Bezpečná autentizace do OS
- Autentizace prostřednictvím certifikátu
- Čipová karta, token iKey



Ochranné mechanismy

- Použití ochranných funkcí OS
- On-line šifrování AreaGuard Notes



Ochranné funkce Operačního Systému

- Šifrovací klíče definované pouze OS
- Možnost uložení šifrovaných dat jen na disku NTFS
- Nemožnost sdílení šifrovaných dat



On-line šifrování AreaGuard Notes

- On-line systém = oprávněný uživatel není omezen při práci s daty
- Šifrování 128b algoritmy
- Neomezená velikost souboru a typ souboru
- Libovolné umístění (disk FAT32, NTFS, výměnná média)



Princip metody šifrování

AreaGuard Notes

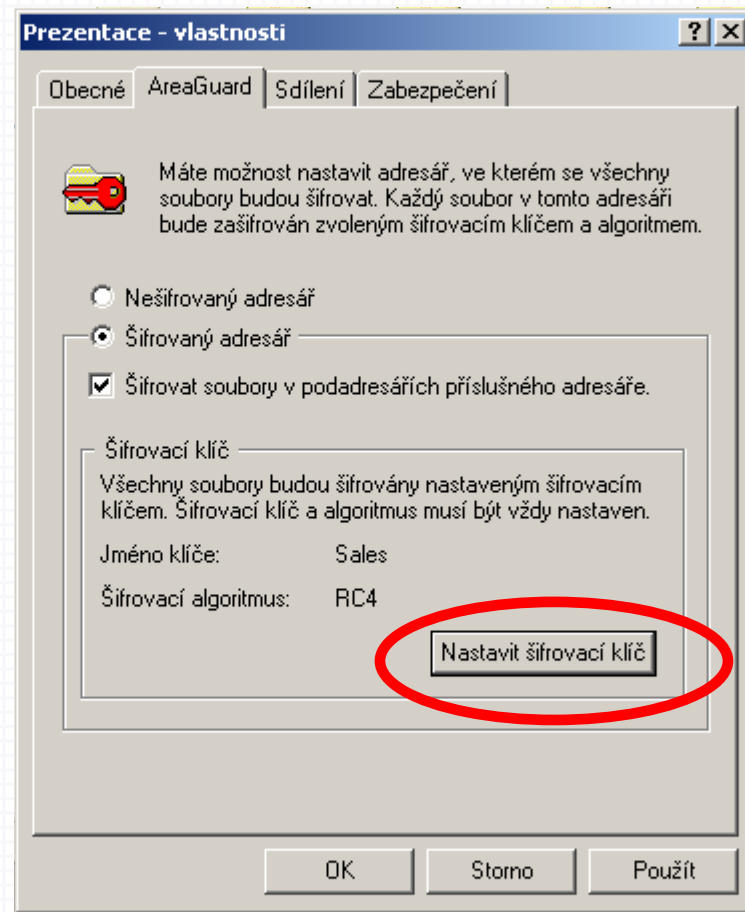
- Nastavení adresáře jako šifrovaného
(po provedení změn je vše on-line šifrováno)
- Uložení šifrovacích klíčů do externího
HW předmětu (čipová karta, token
iKey-1000)
- Automatické načtení
a odstranění klíčů z paměti



Nastavení automaticky šifrovaného adresáře

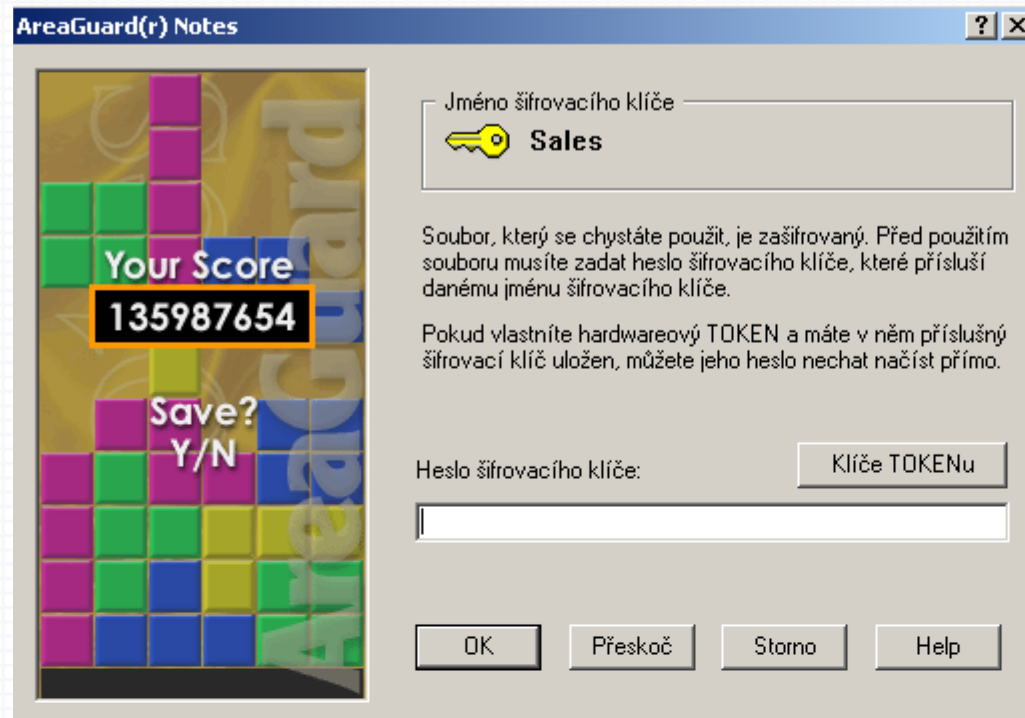
Nastavení automatického šifrování adresáře v nabídce vlastností – záložka AreaGuard

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




Přístup k šifrovanému adresáři

AreaGuard(r) Notes



Jméno šifrovacího klíče

 Sales

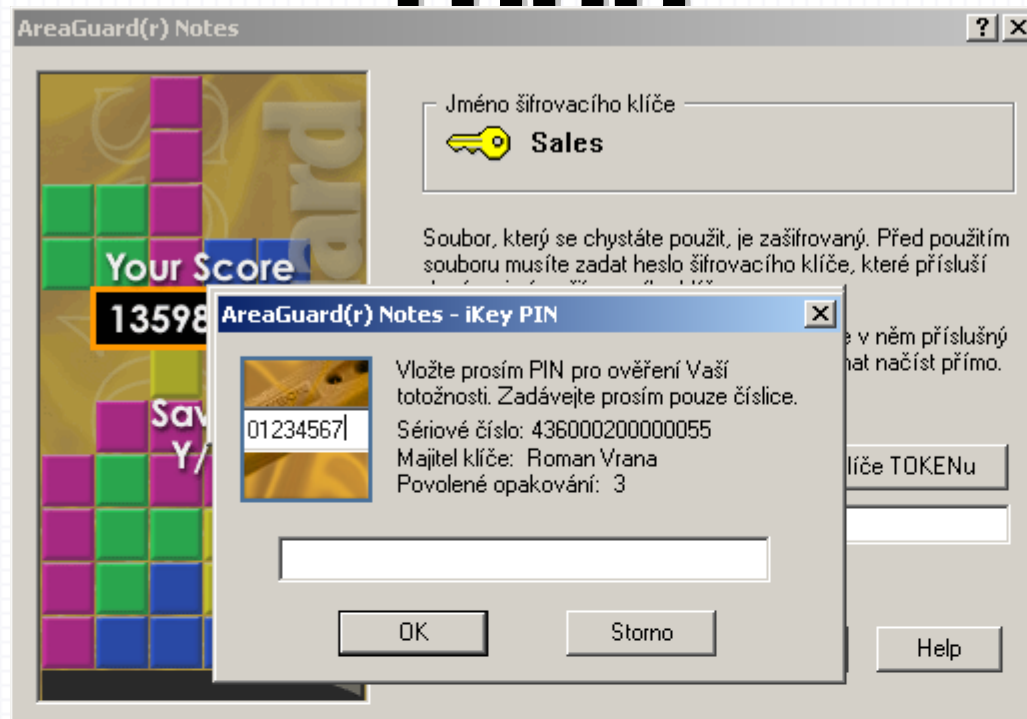
Soubor, který se chystáte použít, je zašifrovaný. Před použitím souboru musíte zadat heslo šifrovacího klíče, které přísluší danému jménu šifrovacího klíče.

Pokud vlastníte hardwareový TOKEN a máte v něm příslušný šifrovací klíč uložen, můžete jeho heslo nechat načíst přímo.

Heslo šifrovacího klíče:



Načtení šifrovacích klíčů z HW prostředku iKey- 1000



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



Díky za pozornost



Tomáš STRANYÁNEK
tomas@sodatsw.cz

www.areaguard.
www.areaguard.com

... and users have a better sleep

SODAT software, Sedláková 33, BRNO, Czech Republic

