



Bezpečná autentizace – nezaměnitelný základ ochrany

Mgr. Pavel Hejl, CSc.

- Realita dnešního dne
- Řešení
- ✓ Bezpečná autentizace
- ✓ Klíčník
- ✓ Single Sign-On
- Bezpečná autentizace všude
- Shrnutí
- Reference
- Závěr



Gartner/IBM:

- Až 90% útoků jsou cílené útoky
- Cílem útoků jsou státní organizace, ...
- Cílem jsou i osobní počítače
- Každou minutu jsou zcizeny data ze 3 počítačů

Hodnocení: **probíhá kybernetická válka !**





Analýzy bohužel dokazují, že:

1. OS nemají nainstalované bezpečnostní hotfixy
2. Aplikace nemají nainstalované bezpečnostní hotfixy
3. Využívají se pouze základní bezpečnostní politiky a konfigurace
4. Jako hlavní autentizační prostředek se používá Heslo
5. Heslo je navíc jednoduché a jedno pro všechno

Útočníci jsou ZATÍM stále o krok dopředu a používají další útoky:



! Především útočí na naše Heslo:
keylogger, phishing, pharming, silový útok, ...

! Získání Hesla (4-8 znaků) podle typu útoku trvá od minut do několika dní....

! Získání Hesla znamená nejenom získání dat, ale i třeba ovládnutí počítače/sítě !



Použít řešení, které je o krok PŘED útočníky:

Především mít naše autentizační data bezpečně uložené:

- ✓ HW token (smart karta/USB smart token)

Jaká autentizační data?:

- ✓ Certifikáty
- ✓ Hesla do každé aplikace/OS



Autentizační data uložené v počítači nejsou dostatečně zabezpečené !



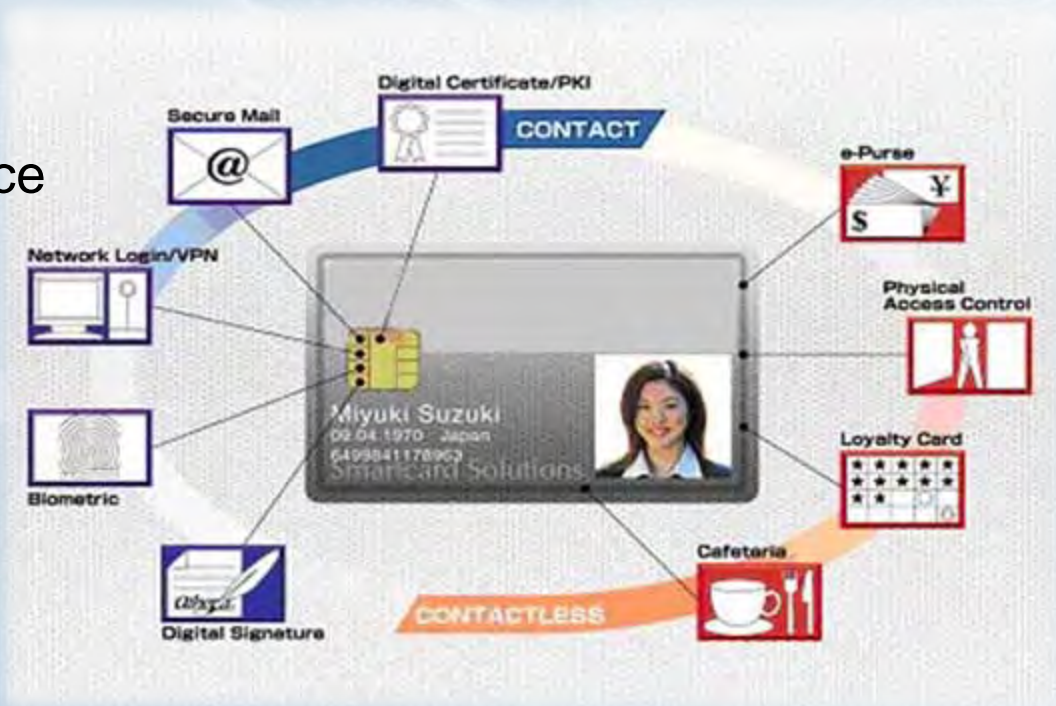
Pouze HW token nám bezpečně ochrání naše autentizační data:

- ✓ Privátní klíč nikdy neopustí paměť
- ✓ Hesla jsou zde zašifrovaná
- ✓ HW token generuje bezpečně klíče i Hesla
- ✓ Certifikace FIPS a CC garantují bezpečnost

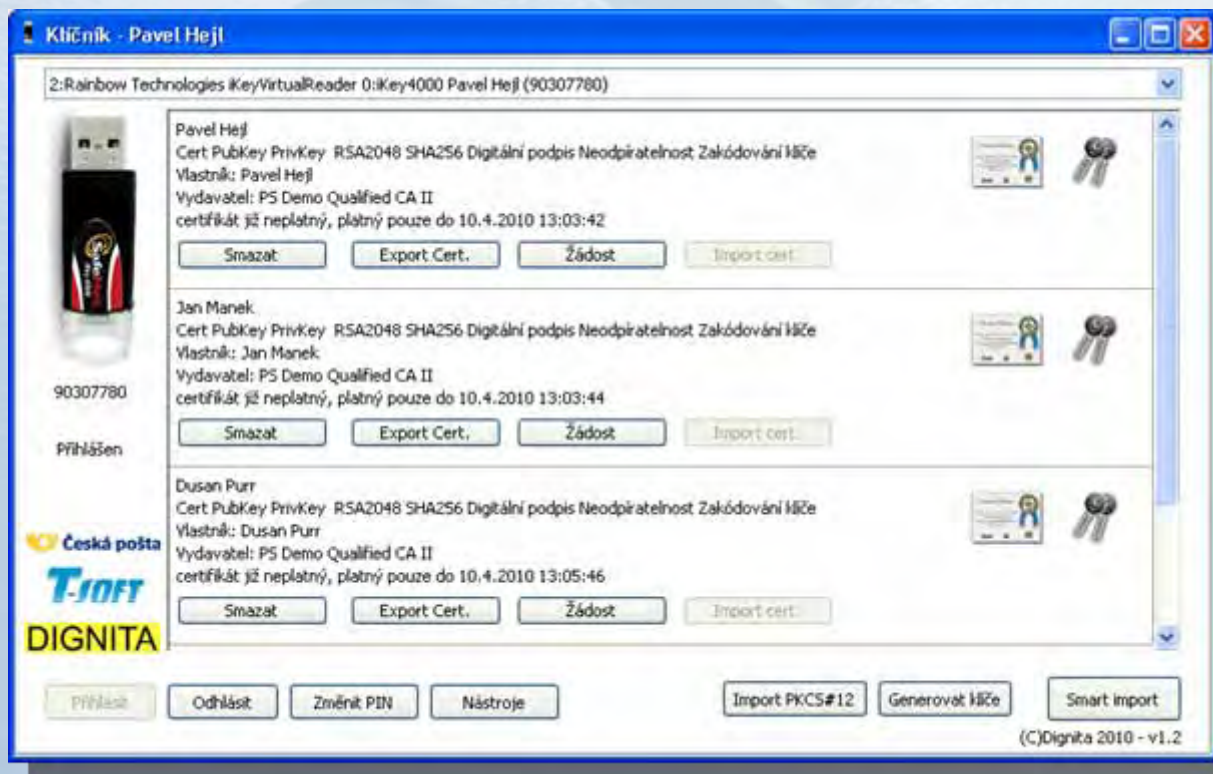


Certifikáty v kartě/tokenu

- ✓ Bezpečná autentizace
- ✓ Bezpečný el. podpis
- ✓ Zabezpečený mail
- ✓ Bezpečná komunikace



Uživatelský nástroj pro smart karty a USB tokeny SafeNet



Personifikace hw tokenu



Personalizace tokenu

Token: 90399201 90399201

Generuj automaticky vše

PIN:

PUK 1:

PUK 2:

PUK 3:

PUK 4:

PUK 5:

PUK 6:



- ✓ Personifikace tokenu/karty
- ✓ Bezpečné zálohování PINu a PUKů
- ✓ Přihlášení/odhlášení ke kartě/tokenu
- ✓ Zobrazení informací o kartě/tokenu
- ✓ Generování klíčů
- ✓ Generování žádosti o certifikát
- ✓ Import certifikátů cer, der, crt a PKCS#12
- ✓ Změna/odblokování PINu
- ✓ Mazání klíčů a certifikátů
- ✓ Podpora CA České pošty



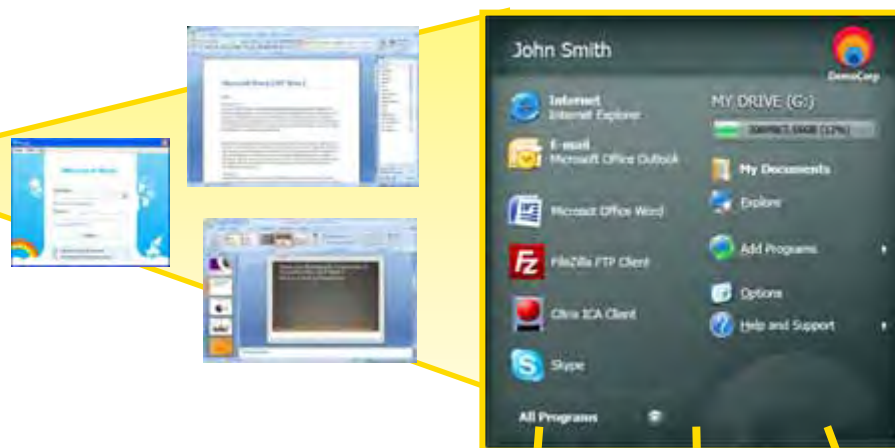
- ✓ Umožňuje autentizaci do aplikací pomocí silného Hesla
- ✓ Umožňuje automatické generování hesel
- ✓ Musíme si pamatovat pouze PIN





- ✓ *Jednoduchá instalace*
- ✓ *Velice příjemné uživatelské prostředí*
- ✓ *Všechny potřebné funkce v jedné aplikaci*
- ✓ *Nezávislost na webovém prohlížeči*
- ✓ *Podpora CA České pošty*

Bezpečná autentizace v nebezpečném prostředí



Zabezpečení dat znamená:

- ✓ Aktualizovaný OS a aplikace
- ✓ Implementace bezpečnostní politiky
- ✓ Bezpečnou více faktorovou autentizaci
- ✓ Zabezpečenou komunikaci
- ✓ Zašifrování citlivých dat



Česká národní banka

Státní pokladna

Česká pošta

Czech POINT (eGovernment)

Datové schránky (eGovernment)

Silové složky



Děkuji za pozornost !

T-SOFT a.s.
Novodvorská 1010/14, 142 01 Praha 4,
Česká republika

tel.: +420 261 710 561 – 562

fax: +420 261 710 563

info@tsoft.cz

