Bezpečný přístup do Datových schránek

Mgr. Pavel Hejl, CSc.

Obsah

- Jednofaktorová autentizace
- Dvoufaktorová autentizace
- Smart tokeny
- PKI autentizace
- Single Sign-On
- Hardware Security Module
- Závěr

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

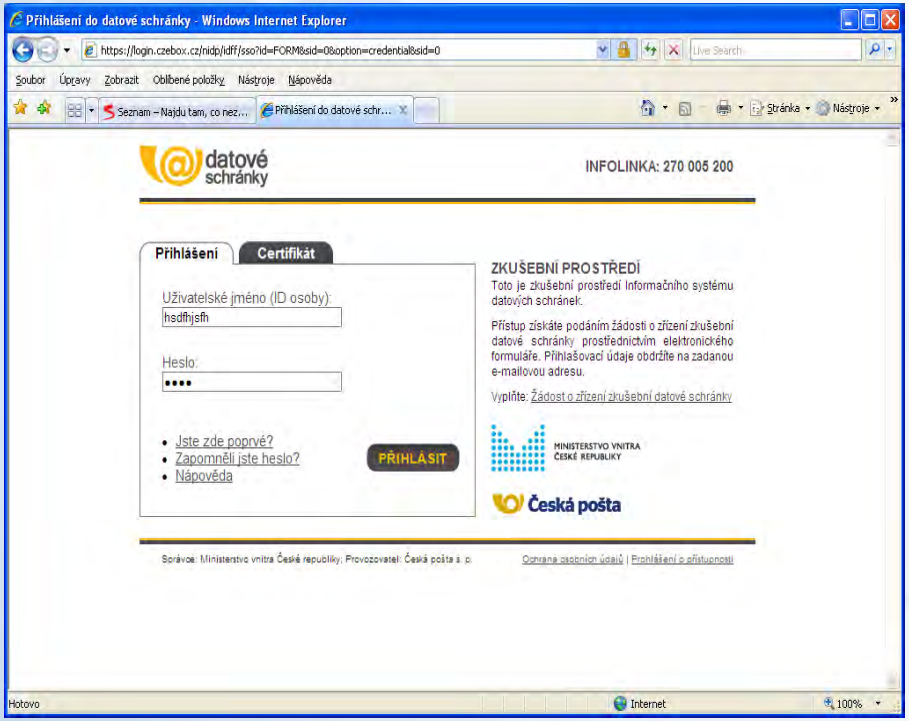
Jednofaktorová autentizace

AUTENTIZACE POMOCÍ JMÉNA A HESLA

- Krátké heslo – jednoduché pro uživatele
- Silné heslo – složité pro uživatele

TYPICKÉ ÚTOKY:

- Phishing, pharming
- Keylogger ...



Dvoufaktorová autentizace

AUTENTIZACE POMOCÍ:

- Něčeho, co mám – hw token
- Něčeho, co znám – PIN

VÝHODY:

- Musím si pamatovat pouze PIN
- Kompromitace PINu ještě neznamená úspěšný útok
- Ztráta tokenu ještě neznamená ztrátu dat

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

USB Smart token

USB smart token:

- Uživatelská paměť 64 KB
- RSA klíče 1 024/2 048 bitů

- SHA-1/SHA-2
- Privátní klíč nikdy neopustí token
- FIPS 140-2 úroveň 3, EAL 4+

PKI smart karta

- PKI smart čipové karty
- Privátní klíč nelze vyexportovat
- Multifunkční/multiplikační

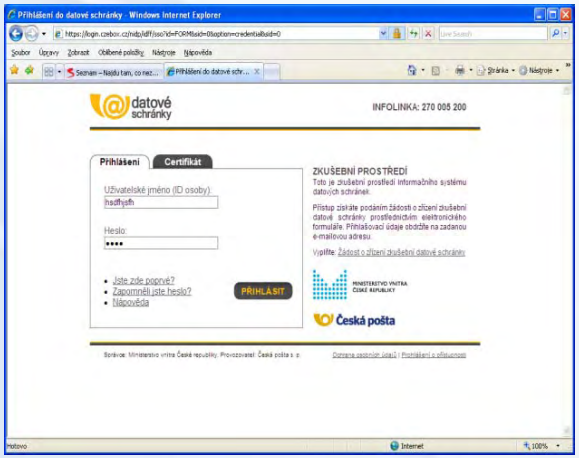
PKI autentizace

- Umožňuje autentizaci do OS i aplikací pomocí certifikátu
- Umožňuje generování klíčů v tokenu
- Umožňuje import certifikátu do tokenu
- Umožňuje bezpečný elektronický podpis
- Autentizace do aplikací i el. podpis je možný i z domácího počítače
- Šifrování komunikace i bezpečná výměna klíčů

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Single Sign-On

- Umožňuje autentizaci do OS pomocí hesla
- Umožňuje autentizaci do aplikací pomocí hesla
- Umožňuje automatické generování hesel
- Umožňuje nasazení silných hesel
- Musíme si pamatovat pouze PIN



Smart tokeny

VÝHODY:

- *Bezpečné úložiště pro citlivá data*
- *Zjednodušení autentizace*
- *Výrazné zvýšení bezpečnosti autentizace*
- *Možnost integrace s dalšími systémy*
- Splňuje požadavky vyhlášky MV ČR

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Hardware Security Module

- Potřebný výkon při hromadném zpracování dat – až 7 000 operací/s
- Bezpečné generování klíčů v modulu
- Bezpečná komunikace a autentizace
- Bezpečný elektronický podpis
- FIPS 140-2 úroveň 2/3, EAL 4/4+

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Hardware Security Module

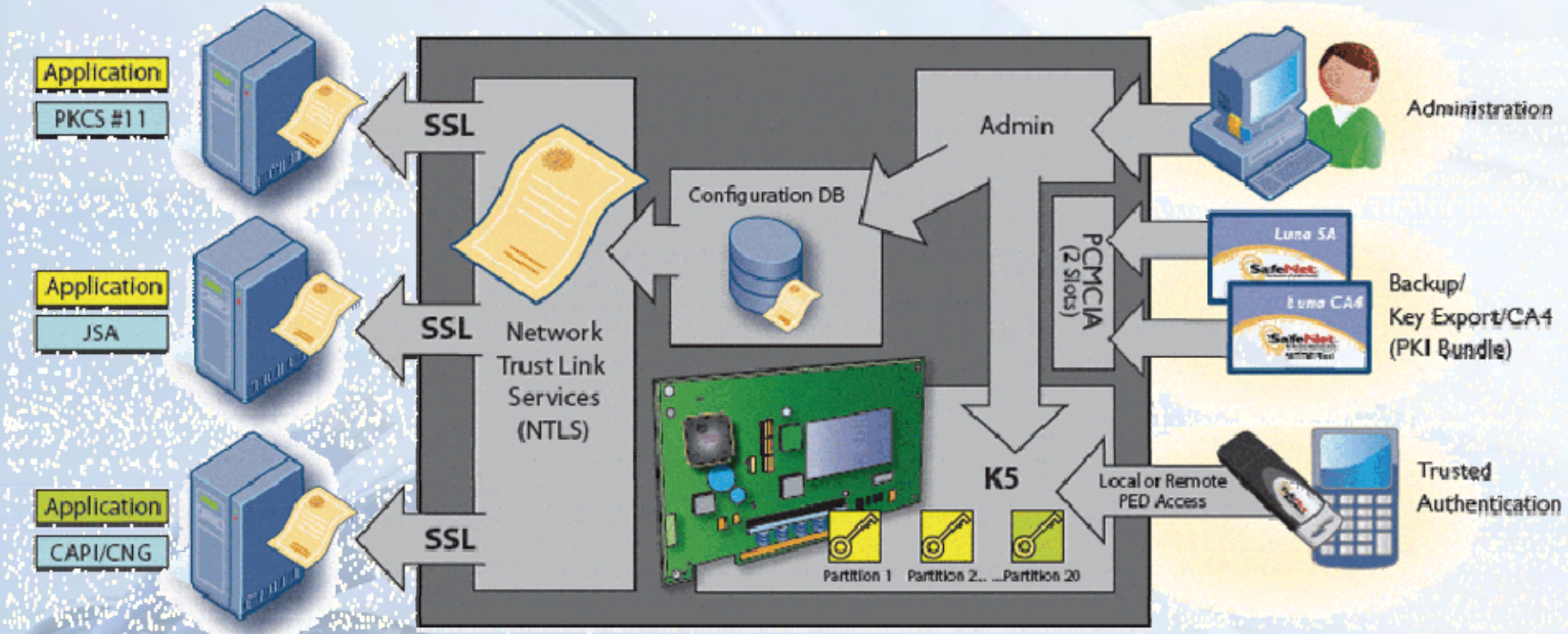


Figure 1

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Hardware Security Module

- Import certifikátů
- Možnost integrace s aplikacemi – ePodatelna, eSpisovka …
- Rozdělení bezpečnostních rolí
- Mohou komunikovat s mnoha aplikacemi najednou
- Bezpečný backup klíčů

www.tsoft.cz T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Příklady implementace

- Česká národní banka
- Datové schránky
- Czech POINT
- Česká pošta
- SAP

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Hardware Security Module

- *Bezpečné uložení autentizačních dat*
- *Bezpečná komunikace a autentizace*
- *Integrace s různými systémy*
- *Velká výkonnost*
- Splňuje požadavky vyhlášky MV ČR

Otázky

T-SOFT a.s., Novodvorská 1010/14, 142 01 Praha 4, tel.: +420 261 710 561–562; fax: +420 261 710 563

Děkuji za pozornost!

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

tel.: +420 261 710 561 – 562
fax: +420 261 710 563
info@tsoft.cz