



Bezpečnost ICT

ISSS 2009

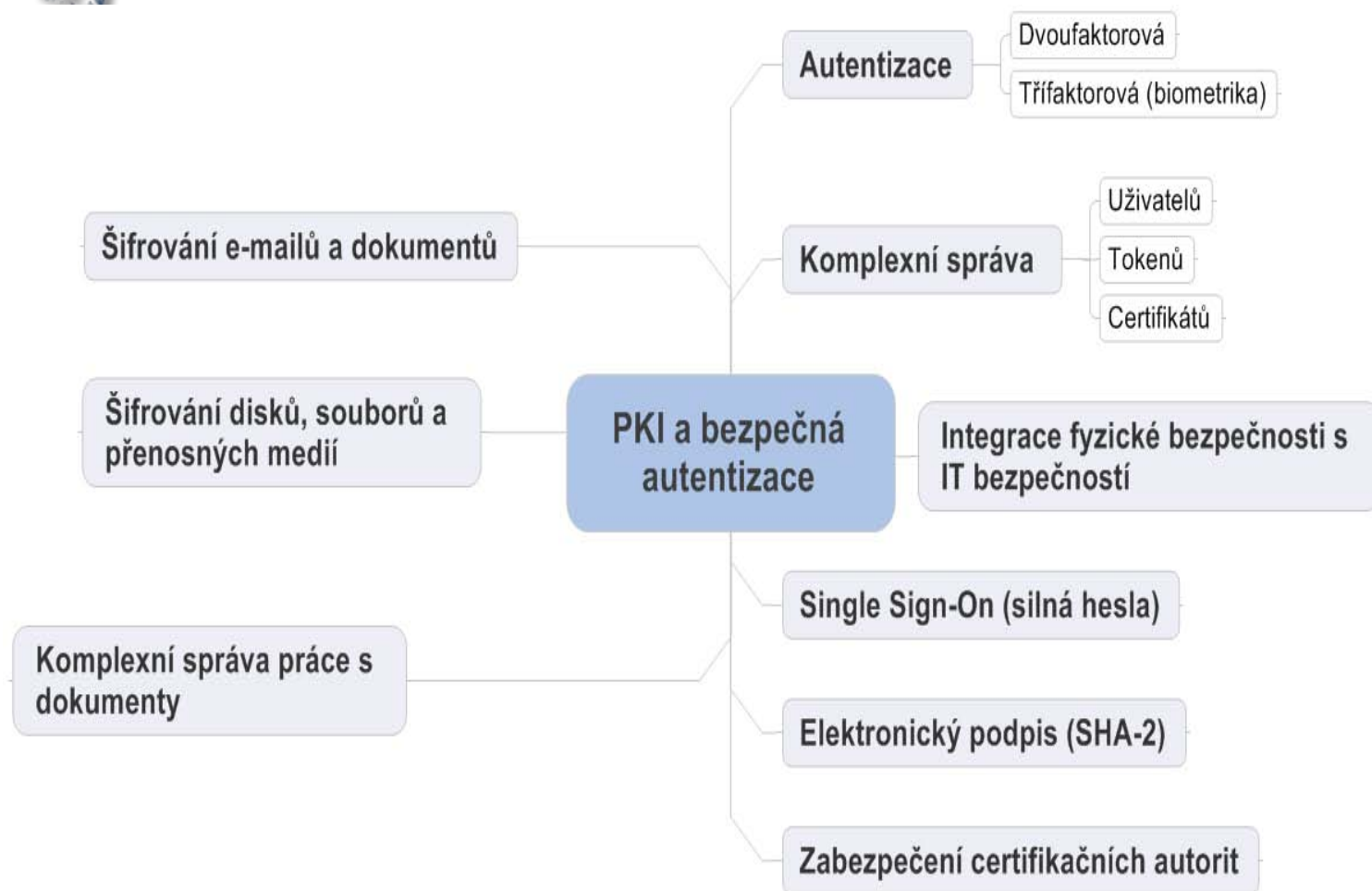
Mgr. Pavel Hejl, CSc.

T- SOFT spol. s r.o.

Obsah

- 🌐 PKI a bezpečná autentizace
- 🌐 Bezpečná komunikace
- 🌐 Czech POINT
- 🌐 Závěr

PKI a bezpečná autentizace



Bezpečná komunikace

Ochrana elektronického podpisu při bankovních transakcích

Ochrana elektronického podpisu v SAP

Antimalwarová ochrana elektronické pošty

Antimalwarová ochrana internetové komunikace

Bezpečná komunikace

Zabezpečení síťové / linkové komunikace

Zabezpečení VPN komunikace

Komplexní správa I/O zařízení

Zabezpečení webových aplikací

Smart tokeny

- 🌐 PKI smart tokeny
- 🌐 Dvou/třífaktorová autentizace
- 🌐 Multifunkční/multiplikační



Smart tokeny

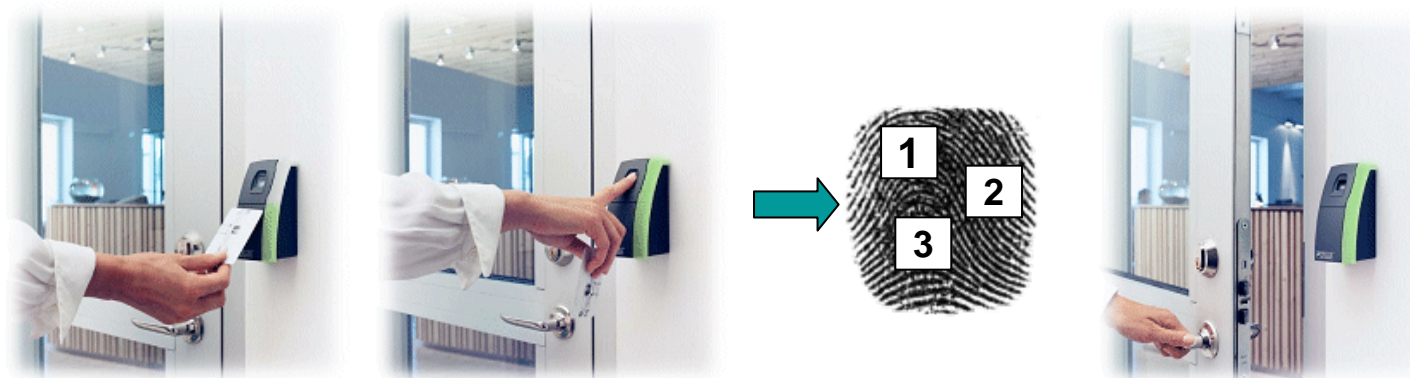


Výhody:

- Bezpečné úložiště pro citlivá data
- Možnost integrace s dalšími systémy

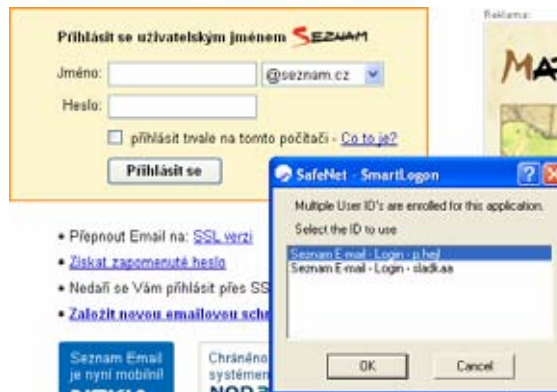
Bezkontaktní čipy

- Mifare DESFire, iClass
- Biometrická autentizace
- Šifrování komunikace i dat



Single Sign-On

- Umožňuje autentizaci do OS i aplikací pomocí hesla
- Umožňuje automatické generování hesel
- Umožňuje nasazení silných hesel



Single Sign-On

Výhody:

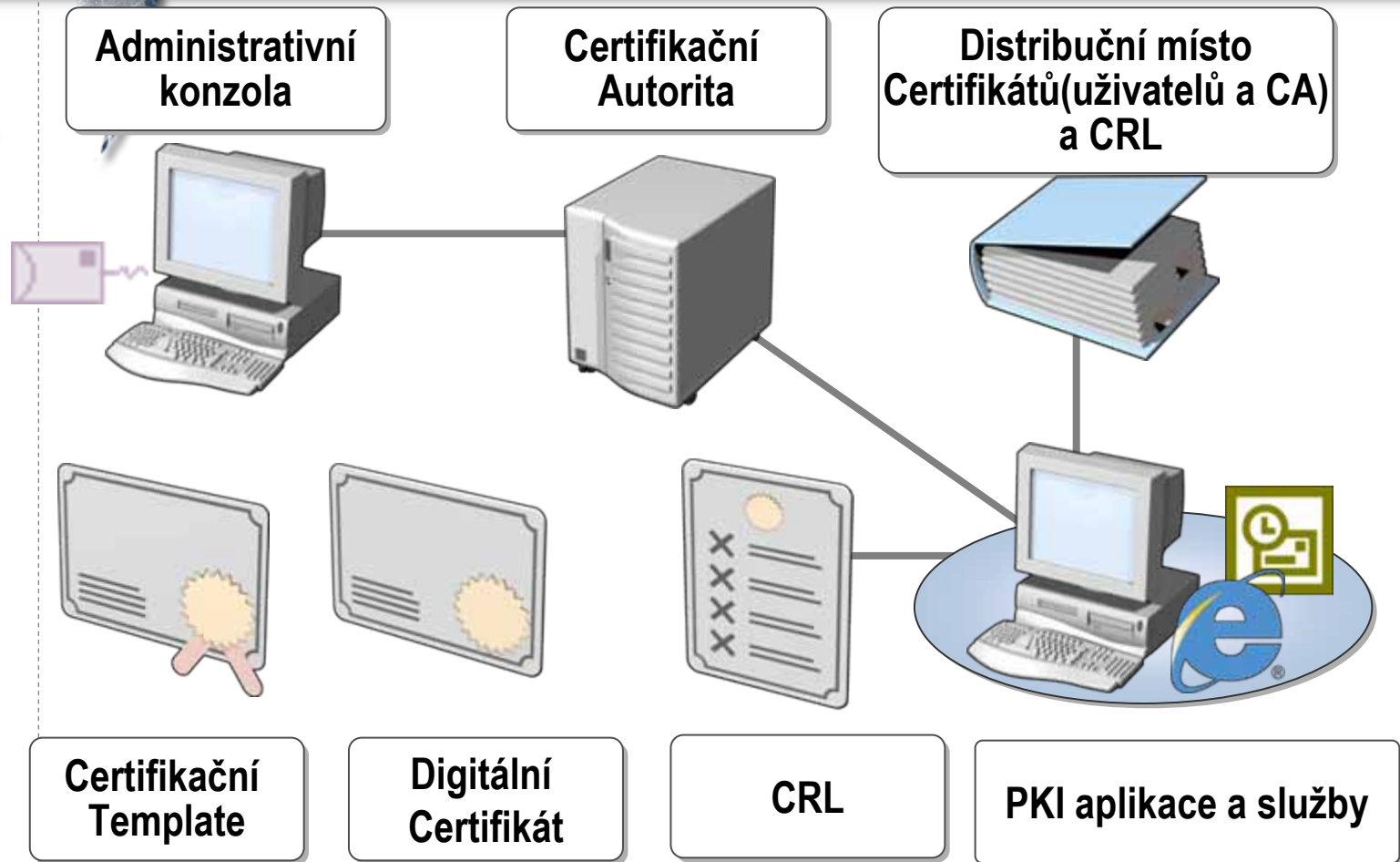
- Výrazné zvýšení bezpečnosti autentizace do OS i aplikací
- Výrazné zjednodušení procesu autentizace
- Rychlá návratnost investic

Co je PKI?

Kombinace software, šifrovacích technologií, procesů a služeb, které umožňují organizacím zabezpečit její komunikaci a obchodní transakce

Požadavky	PKI řešení
Důvěrnost	Zašifrování dat
Integrita	Digitální podpis
Důvěryhodnost	Hash algoritmus, message digests, digitální podpis
Neodpíratelnost	Digitální podpis, audit logů
Dostupnost	Redundance

Komponenty PKI



Šifrování dat

- 🌐 Šifrovací on-line programy
- 🌐 Šifrování souborů ve chráněných sdílených síťových složkách
- 🌐 Šifrování lokálních disků a vyměnitelných médií
- 🌐 Klíče jsou uloženy bezpečně na smart tokenu

Šifrování dat

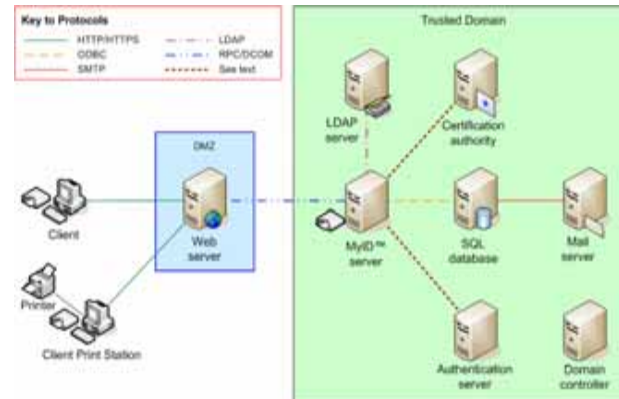
Výhody:

- Jednoduchá instalace a správa
- Jednoduché užívání
- Vysoké zabezpečení proti neoprávněnému přístupu ke chráněným datům

Komplexní správa ID

- Systém pro správu tokenů, uživatelů, certifikátů, klíčů s přímým napojením na CA
- Fyzická i logická personalizace tokenů
- Umožňuje lokální i centrální vydávání tokenů
- Propojuje tokeny, osobní data v digitální podobě a umožňuje kontrolu účtů.
- Usnadňuje práci v oblasti aktivit identifikace v krizovém managementu

Komplexní správa ID



Výhody:

- Výrazné zjednodušení správy
- Výrazné zvýšení bezpečnosti
- Připojením termotiskárny získáváme možnost komplexní personifikace smart karty včetně potisku

Plug & Play management



Bezpečná komunikace

- Ochrana Certifikačních autorit
- Ochrana VPN
- Linkové, síťové, ATM a ethernetové šifrátory
- Ochrana transakčních operací
- FIPS 140-2 úroveň 2/3, EAL 4/4+



Bezpečná komunikace

- Ochrana elektronické pošty
- Ochrana web komunikace
- Ochrana webových aplikací



ŘEŠENÍ T-SOFT:

- *Bezpečné uložení autentizačních dat*
- *Zabezpečení citlivých dat na médiích*
- *Integrace fyzické bezpečnosti s IT bezpečností*
- *Bezpečná komunikace*
- *Zjednodušení práce uživatelů i administrátorů*



Okruh zákazníků v ČR a SR:

- 🌐 Státní správa a samospráva
- 🌐 Bezpečnostní složky
- 🌐 Finanční sektor
- 🌐 Zdravotnictví
- 🌐 Radiotelekomunikace
- 🌐 IT integrátoři
- 🌐 Průmyslové podniky

Reference:

- 🌐 Česká národní banka
- 🌐 Czech POINT
- 🌐 Česká pošta
- 🌐 Ministerstvo obrany ČR
- 🌐 Ministerstvo dopravy ČR

Czech POINT:

- Spolupráce s Českou poštou
- Od hesla k dvoufaktorové autentizaci
- PKI autentizace
- Kvalifikovaný certifikát
- Podpora OS Windows i Linux
- Podpora MS IE i Mozilla

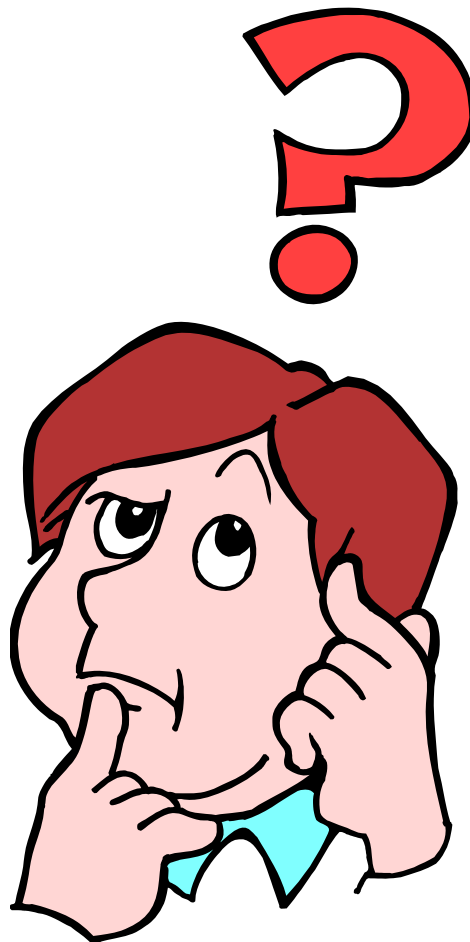
Czech POINT:

USB smart token iKey 4000:

- 🌐 Uživatelská paměť 64 KB
- 🌐 RSA klíče 1 024/2 048 bitů
- 🌐 SHA-1/SHA-2
- 🌐 3DES, RSA a AES
- 🌐 FIPS 140-2 úroveň 3, EAL 4+



Otázky





T-SOFT spol. s r.o.
Novodvorská 1010/14
142 01 Praha 4

www.tsoft.cz