

Demonstrace práce s PKI kartou

Ondřej Těthal

tethal@coprosys.cz

Demonstrace práce s PKI kartou

- Podepisování e-mailu
- Dešifrování e-mailu
- Ověřování identity uživatele pro přístup k webové stránce pomocí SSL

- Bezkontaktní rozhraní
- Microsoft prostředí
- Duální karta StarCOS 2.5DI (Giesecke & Devrient)

Vydávání karty - postup

- 1. Personalizace karty
 - 2. Generování žádostí o certifikáty
 - 3. Instalace certifikátů na kartu a do systému
-
- Kontaktní rozhraní

Personalizace - požadavky

- StarCOS Toolkit 2.5, Giesecke & Devrient
- Podporovaná kontaktní čtečka čipových karet (GemPC Twin, Gemplus)
- Popis souborové struktury a dat na kartě (karetní aplikace podle PKCS#15)

Personalizace - postup

- Demonstrace
 - StarMAG 3.1

- Reálný provoz
 - Aplikace pro vybrané personalizační zařízení

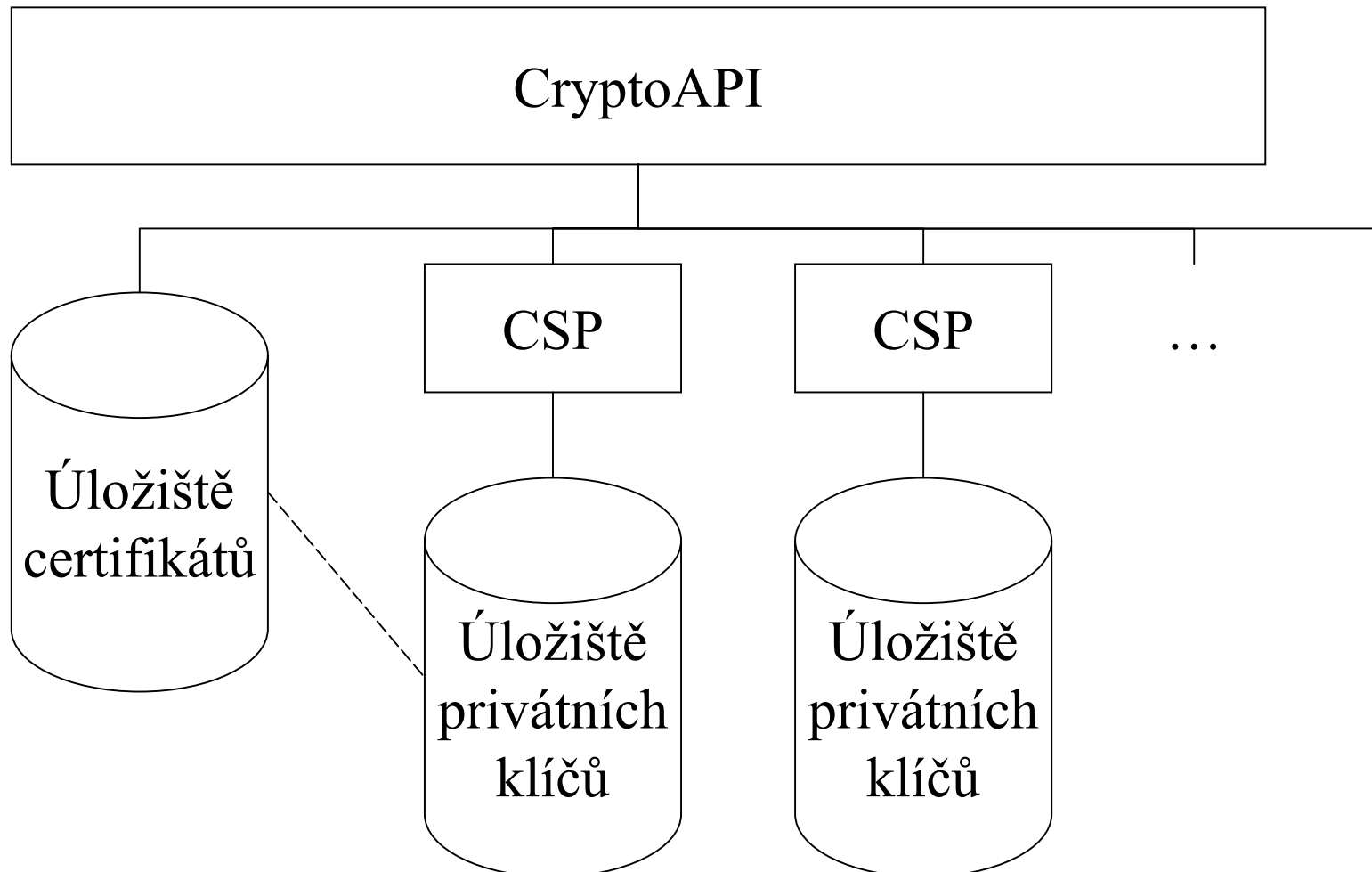
Žádost o certifikát - požadavky

- Windows 2000/XP
- Cryptographic Service Provider pro danou kartu (GDP11CSP 1.2)
- Podporovaná kontaktní čtečka čipových karet (GemPC Twin, Gemplus)
- Certifikační autorita (Microsoft Certificate Services)

Žádost o certifikát - postup

- Demonstrace
 - Webové rozhraní Microsoft Certificate Services
 - Všechny klíče generované na kartě
- Reálný provoz (příklad)
 - Dávkové zpracování
 - Některé (šifrovací) klíče může generovat CA
 - Nutnost znalosti rozhraní CA

Instalace certifikátu (1)



Instalace certifikátu (2)

- Odkaz na privátní klíč není součástí certifikátu
- Při generování žádosti o certifikát se vytvoří v úložišti certifikátů atrapa certifikátu s odkazem na odpovídající privátní klíč
- Při instalaci certifikátu se atrapa nahradí pravým certifikátem
- Problém při používání tokenu na více počítačích

Instalace certifikátu - postup

- Demontrace
 - Webové rozhraní Microsoft Certificate Services
 - Jeden počítač
- Reálný provoz
 - Proces nutno automatizovat, např.:
 - Aplikace na pozadí
 - Webová stránka (využívající CAPICOM)

Použití karty - požadavky

- Windows 2000/XP
- Cryptographic Service Provider pro danou kartu (GDP11CSP 1.2)
- Podporovaná čtečka čipových karet (MF RD 700, Philips Semiconductors)
- Internet Explorer, Outlook Express

Distribuce certifikátů pro šifrování

- Demontrace
 - Manuálně přiřazením certifikátu ke kontaktu
- Reálný provoz
 - Adresářová služba

Prostředí (1)

- Počítač TCA1
 - Windows 2000 Server
 - Certifikační autorita (<http://tca1/certsrv>)
 - Web server vyžadující klientský certifikát (<https://tca1/test>)

Prostředí (2)

- Počítač TCLIENT1
 - Windows XP Professional
 - Outlook Express 6.0
 - Internet Explorer 6.0
 - StarCOS Toolkit 2.5
 - ArgoSoft Mail Server 1.8
 - CSP pro StarCOS 2.5DI
 - Kontaktní a bezkontaktní čtečka čipových karet

Shrnutí

- Bezkontaktní provoz PKI karet je možný
- Nutno přizpůsobit konkrétním požadavkům
- Problémy k řešení:
 - Vydávání karet, personalizace
 - Generování klíčů mimo kartu
 - Automatizovaná instalace certifikátů z karty do systému

Zdroje, odkazy

- Microsoft Corporation, www.microsoft.com
- Giesecke & Devrient GmbH, www.gieseckedevrient.com
- ArGo Software Design, www.argosoft.com
- Gemplus, www.gemplus.com
- Philips Semiconductors, www.semiconductors.philips.com
- Dostálek L. a kolektiv: Velký průvodce protokoly TCP/IP – Bezpečnost, 2. vydání, Computer Press Praha, 2003