IMPLEMENTACE MICROSOFT PKI

NÁVRH, REALIZACE A PROVOZ PKI S TECHNOLOGIEMI MICROSOFT

NÁVRH A IMPLEMENTACE CERTIFIKAČNÍCH AUTORIT, ZAKÁZKOVÝ VÝVOJ PKI APLIKACÍ, NASAZENÍ A SPRÁVA ČIPOVÝCH KARET.

[IMPLEMENTACE CERTIFIKAČNÍCH AUTORIT]

Certifikační autorita (CA) slouží jako důvěryhodný zdroj elektronických certifikátů, které je možno využít v řadě klíčových bezpečnostních technologií založených na asymetrické kryptografii jako je například:

- Integrovaná vícefaktorová autentizace uživatelů (autentizace certifikátem v čipové kartě)
- Zabezepečení webových portálů a služeb pomocí serverových certifikátů
- Autentizace uživatelů k webům a webovým službám pomocí klientských certifikátů
- Autentizace počítačů, služeb a mobilních zařízení pomocí certifikátů
- Zabezpečení elektronické pošty - elektronický podpis a šifrování
- Šifrování síťové komunikace (IPSEC)
- Podpis kódu: např. podpis firemních maker Office, Powershell skriptů, instalačních balíčků, Java archivů ...)
- Šifrování souborů pomocí EFS (Encrypting File System)

V sítích Microsoft Active Directory nabízíme implementaci certifikačních autorit na bázi služby Active Directory Certificate Services (AD CS).

VLASTNOSTI A VÝHODY

- Úzká integrace MS PKI s ostatními technologiemi Microsoft
- Integrovaná vícefaktorová autentizace pomocí čipových karet
- Široká oblast využití certifikátů v bezpečnostních technologiích
- Integrace s MS Active Directory
- Možnost automatizace procesů registrace žádostí a vydávání certifikátů
- Nevyžaduje žádné dodatečné softwarové nebo klientské licence
- Možnost rozšíření vestavěné funkcionality pomocí zakázkových aplikací

[VÝHODY ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)]

Služba AD CS je bezplatnou komponentou Windows Serveru. Její instalace a provoz nevyžaduje žádné dodatečné serverové či klientské licence.
Další zásadní výhodou je úzká integrace s ostatními serverovými a klientskými technologiemi a aplikacemi Microsoftu jako je integrovaná Windows autentizace pomocí certifikátů, publikace uživatelských certifikátů do Active Directory, automatizované vydávání a obnova certifikátů uživatelů i počítačů atd.

[NABÍDKA IMPLEMENTACE CERTIFIKAČNÍCH AUTORIT]

Implementace certifikačních autorit zahrnuje jak nasazení příslušných SW a HW produktů, tak i analýzu a definici všech souvisejících technických a administrativních procesů, které společně vytváří tzv. infrastrukturu veřejných klíčů (PKI). Součástí nabídky implementace PKI je:

- Analýza prostředí a bezpečnostních potřeb zákazníka směřujících k nasazení PKI technologií
- Návrh architektury certifikačních autorit - kořenové a vydávající autority, návrh časové platnosti, zabezpečení soukromých klíčů certifikačních autorit pomocí hardwarových bezpečnostních modulů (HSM) atd.
- Návrh certifikačních politik a typů certifikátů pro vybrané technologie využívající certifikáty
- Návrh procesů vydávání klientských a serverových certifikátů a procesů správy a obsluhy CA
- Návrh konfigurace certifikačních autorit, správy, zálohování
- Konfigurace prostředí Active Directory a skupinových politik pro provoz PKI a návazných technologií
- Implementace CA a podpora provozu - audit, kontrola, obnova certifikátů CA, disaster recovery

[ZAKÁZKOVÝ VÝVOJ PKI APLIKACÍ]

Pro stávající či implementované PKI nabízíme vývoj zakázkových aplikací a nástrojů či konzultace k jejich vývoji. Může se jednat o nástroje usnadňující provoz a správu PKI technologií - např. aplikace pro výdej speciálních typů certifikátů, webové aplikace pro operátory certifikační autority (registrační autority), webové služby pro přístup interních bussiness aplikací ke službám certifikačních autorit atd.

Příkladem může být aplikace ICZ CaNotifier, která monitoruje databázi certifikační autority a v případě blížící se exspirace certifikátu uživatele či serveru rozesílá uživatelům e-mail s upozorněním.

Dalším příkladem je realizovaná zákaznická webová služba zprostředkující firemnímu ERP systému vystavování uživatelských certifikátů na certifikační autoritě MS.

Dále lze nabídnout vývoj koncových aplikací či komponent pro jiné aplikace vykonávající kryptografické funkce jako je šifrování či elektronický podpis dat.

[ČIPOVÉ KARTY]

Kontaktní čipová karta je nabízena jako bezpečné úložiště certifikátů a soukromých klíčů uživatelů. Uložením autentizačního certifikátu do čipové karty je dosaženo bezpečné dvoufaktorové autentizace (vlastnictví fyzického tokenu + znalost PINu).

Přínosy čipové karty

- Bezpečné úložiště certifikátů a soukromých klíčů (klíče nelze z karty zkopírovat)
- Bezpečná dvoufaktorová autentizace uživatelů do Windows či k webovým aplikacím
- Možnost uložení dalších tajných informaci (hesla či klíče jiných aplikací)

Standardně nabízíme čipové karty HID Crescendo C700, jejímž výrobcem je HID Global.

Čipovou kartu lze nabídnout ve formátu klasické plastové karty nebo jako USB token, který nevyžaduje čtečku.

Správa čipových karet

Pro nabízené čipové karty je k dispozici program ICardManager pro evidenci a správu kontaktní části čipových karet.

Základní parametry kontaktní části čipové karty

- JAVA karta
- Kapacita EEPROM 80 kB
- Podpora 2048 bit RSA klíčů
- Podpora algoritmů SHA1/2, AES 256, ECC
- Podpora kryptografických rozhraní Crypto API, PKCS#11.
- Integrace do Windows pomocí middleware SafeSign (cena middleware je v kupní ceně karty)

Karta je dodávána v kombinaci s nezávislou bezkontaktní částí volitelné technologie (iClass, HID, Mifare)

Základní funkce programu

- Evidence karet (sériové číslo, PIN, PUK atd.)
- Inicializace karet, změna PIN, PUK
- Přiřazení karty uživateli z Active Directory
- Enrollment certifikátů do čipové karty
- Tisk předávacích protokolů
- Odblokování PINu
- Vzdálené odblokování PINu po telefonu (pomocí challenge-response kódu)
- Software lze na zakázku přizpůsobit potřebám zákazníka

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@iczgroup.com