# IMPLEMENTÁCIA

MICROSOFT PKI

NÁVRH, REALIZÁCIA A PREVÁDZKA PKI S TECHNOLÓGIAMI MICROSOFT

NÁVRH A IMPLEMENTÁCIA CERTIFIKAČNÝCH AUTORÍT, ZÁKAZKOVÝ VÝVOJ PKI APLIKÁCIÍ, NASADENIE A SPRÁVA ČIPOVÝCH KARIET.

## [ IMPLEMENTÁCIA CERTIFIKAČNÝCH AUTORÍT ]

**VLASTNOSTI A VÝHODY**

` Úzka integrácia MS PKI s ostatnými technológiami spoločnosti Microsoft

` Integrovaná viacfaktorová autentizácia pomocou čipových kariet

` Široká oblasť využitia certifikátov v bezpečnostných technológiách

` Integrácia s MS Active Directory

` Možnosť automatizácie procesov registrácie žiadostí a vydávania certifikátov

` Nevyžaduje žiadne dodatočné softvérové alebo klientske licencie

` Možnosť rozšírenia zabudovanej funkcionality pomocou zákazkových aplikácií

Certifikačná autorita (CA) slúži ako dôveryhodný zdroj elektronických certifikátov, ktoré je možné využiť v rade kľúčových bezpečnostných technológií založených na asymetrickej kryptografii, ako je napríklad:

` Integrovaná viacfaktorová autentizácia používateľov (autentizácia certifikátom v čipovej karte)

` Zabezpečenie webových portálov a služieb pomocou serverových certifikátov

` Autentizácia používateľov do webov a webových služieb pomocou klientskych certifikátov

` Autentizácia počítačov, služieb a mobilných zariadení pomocou certifikátov

` Zabezpečenie elektronickej pošty – elektronický podpis a šifrovanie

` Šifrovanie sieťovej komunikácie (IPSEC)

` Podpis kódu: napr. podpis firemných makier Office, Powershell skriptov, inštalačných balíčkov, Java archívov ...)

` Šifrovanie súborov pomocou EFS (Encrypting File System)

V sieťach Microsoft Active Directory ponúkame implementáciu certifikačných autorít na báze služby Active Directory Certificate Services (AD CS).

## [ VÝHODY ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS) ]

Služba AD CS je bezplatným komponentom Windows Servera. Jej inštalácia a prevádzka nevyžaduje žiadne dodatočné serverové či klientske licencie.

Ďalšou zásadnou výhodou je úzka integrácia s ostatnými serverovými a klientskymi technológiami a aplikáciami Microsoftu, ako je integrovaná Windows autentizácia pomocou certifikátov, publikácia používateľských certifikátov do Active Directory, automatizované vydávanie a obnova certifikátov používateľov aj počítačov atď.

## [ PONUKA IMPLEMENTÁCIE CERTIFIKAČNÝCH AUTORÍT ]

Implementácia certifikačných autorít zahŕňa tak nasadenie príslušných SW a HW produktov, ako aj analýzu a definíciu všetkých súvisiacich technických a administratívnych procesov, ktoré spoločne vytvárajú tzv. infraštruktúru verejných kľúčov (PKI). Súčasťou ponuky implementácie PKI je:

` Analýza prostredia a bezpečnostných potrieb zákazníka smerujúcich k nasadeniu PKI technológií

` Návrh architektúry certifikačných autorít – koreňové a vydávajúce autority, návrh časovej platnosti, zabezpečenie súkromných kľúčov certifikačných autorít pomocou hardvérových bezpečnostných modulov (HSM) atď.

` Návrh certifikačných politík a typov certifikátov pre vybrané technológie využívajúce certifikáty

` Návrh procesov vydávania klientskych a serverových certifikátov a procesov správy a obsluhy CA

` Návrh konfigurácie certifikačných autorít, správy, zálohovania

` Konfigurácia prostredia Active Directory a skupinových politík pre prevádzku PKI a nadväzných technológií

` Implementácia CA a podpora prevádzky – audit, kontrola, obnova certifikátov CA, disaster recovery

**[ IMPLEMENTÁCIA MICROSOFT PKI ]**

## [ ZÁKAZKOVÝ VÝVOJ PKI APLIKÁCIÍ ]

Pre existujúce či implementované PKI ponúkame vývoj zákazkových aplikácií a nástrojov či konzultácie k ich vývoju. Môže ísť o nástroje uľahčujúce prevádzku a správu PKI technológií – napr. aplikácie na výdaj špeciálnych typov certifikátov, webové aplikácie pre operátorov certifikačnej autority (registračné autority), webové služby na prístup interných obchodných aplikácií k službám certifikačných autorít atď.

Príkladom môže byť aplikácia ICZ CaNotifier, ktorá monitoruje databázu certifikačnej autority a v prípade blížiacej sa exspirácie certifikátu používateľa či servera rozosiela používateľom e-mail s upozornením.

Ďalším príkladom je realizovaná zákaznícka webová služba sprostredkujúca firemnému ERP systému vystavovanie používateľských certifikátov na certifikačnej autorite MS.

Ďalej je možné ponúknuť vývoj koncových aplikácií či komponentov pre iné aplikácie vykonávajúce kryptografickej funkcie, ako je šifrovanie či elektronický podpis údajov.

## [ ČIPOVÉ KARTY ]

Kontaktná čipová karta je ponúkaná ako bezpečné úložisko certifikátov a súkromných kľúčov používateľov. Uložením autentizačného certifikátu do čipovej karty je dosiahnutá bezpečná dvojfaktorová autentizácia (vlastníctvo fyzického tokenu + znalosť PIN-u).

### Prínosy čipovej karty

` Bezpečné úložisko certifikátov a súkromných kľúčov (kľúče nie je možné z karty skopírovať)

` Bezpečná dvojfaktorová autentizácia používateľov do systému Windows či do webových aplikácií

` Možnosť uložiť ďalšie tajné informácie (heslá či kľúče iných aplikácií)

Štandardne ponúkame čipové karty HID Crescendo C700, ktorých výrobcom je HID Global.

Čipovú kartu je možné ponúknuť vo formáte klasickej plastovej karty alebo ako USB token, ktorý nevyžaduje čítačku.

### Správa čipových kariet

Pre ponúkané čipové karty je k dispozícii program ICardManager na evidenciu a správu kontaktnej časti čipových kariet.



### Základné parametre kontaktnej časti čipovej karty

` JAVA karta

` Kapacita EEPROM 80 kB

` Podpora 2048-bitových kľúčov RSA

` Podpora algoritmov SHA1/2, AES 256, ECC

` Podpora kryptografických rozhraní Crypto API, PKCS#11.

` Integrácia do Windowsu pomocou middleware SafeSign (cena middleware je v kúpnej cene karty)

Karta je dodávaná v kombinácii s nezávislou bezkontaktnou časťou voliteľnej technológie (iClass, HID, Mifare)

### Základná funkcia programu

` Evidencia kariet (sériové číslo, PIN, PUK atď.)

` Inicializácia kariet, zmena PIN, PUK

` Priradenie karty používateľovi z Active Directory

` Enrollment certifikátov do čipovej karty

` Tlač preberacích protokolov

` Odblokovanie PIN-u

` Vzdialené odblokovanie PIN-u cez telefón (pomocou challenge-response kódu)

` Softvér je možné na zákazku prispôsobiť potrebám zákazníka

**OBCHODNÝ 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:** [mark](mailto:marketing@iczgroup.com)[eting@iczgroup.com](mailto:eting@iczgroup.com)