

## Koreňová certifikačná autorita NBÚ od spoločnosti IBM

V roku 2002 vošiel do platnosti Zákon o elektronickom podpise 215/2002, ktorý upravuje vzťahy vznikajúce v súvislosti s vyhotovením a používaním elektronického podpisu. Cieľom zákona je vytvoriť legislatívne podmienky, potrebné na akceptáciu a používanie zaručeného elektronického podpisu, ktorý je ekvivalentom vlastnoručného podpisu. Zákon 215/2002 zb. z. dopĺňajú ďalšie vyhlášky (Vyhlášky 537, 538, 539, 540, 541, 542 z roku 2002).

Národný bezpečnostný úrad predstavuje zákonom stanovenú autoritu, ktorá:

- akredituje Certifikačné authority  
Akreditované certifikačné authority môžu vydávať kvalifikované certifikáty. Nutnou podmienkou pre vytváranie a overovanie zaručeného elektronického podpisu je použitie kvalifikovaného certifikátu a k nemu prislúchajúcemu súkromnému kľúču.
- vydáva kvalifikované certifikáty pre Akreditované certifikačné authority

Projekt vybudovania Koreňovej certifikačnej autority (KCA) pre NBÚ bol zameraný na dodávku rozsiahleho riešenia, ktorého jedným z cieľov je vydávanie kvalifikovaných certifikátov pre akreditované certifikačné authority (ACA) a poskytovanie akreditovaných certifikačných služieb pre ACA.

### **Cieľ spoločnosti IBM, divízie Global Services:**

Projekt realizácie, dodávka technického a programového vybavenia, spracovanie dokumentácie pre certifikačnú autoritu a jej implementácia pre ústredný orgán štátnej správy pre elektronický podpis (Národný bezpečnostný úrad).

### **Výzva:**

NBU vypísalo verejnú súťaž na partnera schopného tak nasadiť technologickú platformu, ako aj podporiť efektívne dosahovanie cieľov NBU.

### **Kľúčové technické otázky:**

Komunikácia s mnohými štátnymi inštitúciami s možnosťou využitia zaručeného elektronického podpisu.

### **Riešenie:**

IBM Global Services implementoval pre NBU riešenie Koreňovej certifikačnej autority (KCA), technickú infraštruktúru, technickú a bezpečnostnú dokumentáciu, potrebné pre plnenie úloh, ktoré stanovuje zákon 215/2002 a dopĺňujúce vyhlášky pre Národný bezpečnostný úrad.

### **Výsledok:**

IBM dodala komplexné riešenie pozostávajúce z nasledujúcich častí:

- dodávka, inštalácia a konfigurácia hardvéru a softvéru od rôznych výrobcov.  
Jedná sa o desiatky rôznych výrobcov HW a SW, napr:  
HW: IBM, SUN, Algoritm Research, Datakey, Cisco  
SW: Cybertrust (pôvodne Baltimore), SUN, IBM, Datum, Cisco, Microsoft
- návrh architektúry a realizácia riešenia KCA, ktorá zabezpečuje certifikačné služby:
  - o vydávanie kvalifikovaných certifikátov pre ACA
  - o publikovanie kvalifikovaných certifikátov na Internete
  - o vydávanie zoznamu zrušených kvalifikovaných certifikátov (CRL)
  - o publikovanie CRL na Internete
  - o rušenie kvalifikovaných certifikátov
  - o vydávanie časových pečiatok pre autorizované subjekty

- publikovanie dokumentácie o KCA na Webe v zmysle požiadaviek zákona 215/2002 a neskorších predpisov
- návrh a realizácia riešenia pre monitorovanie kritických procesov KCA,
- návrh a realizácia systému archivácie a zálohovania,
- zabezpečenie vysokej dostupnosti kritických procesov KCA,
- návrh a dodávka prevádzkových a bezpečnostných predpisov potrebných pre fungovanie Koreňovej certifikačnej autority a zodpovedajúcej technickej infraštruktúry.
- V rámci projektu boli dodané čipové karty typu Datakey na zabezpečovanie kryptografických funkcií PKI (generovanie kľúčov na karte, vytváranie a overovanie elektronického podpisu).

Cieľom projektu bolo vybudovanie technickej a netechnickej infraštruktúry, ktorú Národný bezpečnostný úrad potrebuje na riešenie úloh stanovených v Zákone o elektronickom podpise č 215/2002 a neskorších predpisov.

**Súhrn:**

Riešenie Koreňovej certifikačnej autority predstavuje robustný systém, ktorý svojou veľkosťou dosahuje resp. prevyšuje podobné riešenia implementované na Slovensku.

**Význam:**

Koreňová certifikačná autorita má celoslovenský význam, umožňuje štátom definovanej autorite pre elektronický podpis – Národného bezpečnostnému úradu – poskytovať akreditované certifikačné služby pre Akreditované certifikačné autority v zmysle zákona 215/2002 a neskorších predpisov.

Pre viac informácií kontaktujte Miroslava Lhotákovú.