Elektronické podpisovanie dokumentov

IBM

www.ibm.com/sk

Potreba vzniku elektronického podpisu vyplynula z postupnej elektronizácie spoločnosti, keď veľké množstvo agendy firiem, štátnej a verejnej správy sa postupne presúva do elektronickej podoby. Elektronický podpis v súčasnosti pokrýva rôzne bezpečnostné požiadavky, napr. autentifikáciu, integritu údajov, sledovateľnosť. Elektronický podpis je však veľmi široký pojem. V nasledujúcich riadkoch sa budeme zaoberať len elektronickými podpismi dokumentov, ktoré sa vytvárajú s pomocou X.509 certifikátov, ako ich definuje technický štandard RFC 3280. Nebude sa zaoberať elektronickými podpismi, ktoré sa vytvárajú pomocou PGP certifikátov podľa štandardu RFC 1991.

PREČO ELEKTRONICKÝ PODPIS

Najväčší a nezastupiteľný význam elektronického podpisu však spočíva v nepopierateľnosti – náhrade vlastnoručného podpisu v elektronickom styku. Ak používateľ vytvorí elektronický podpis dokumentu, nemôže v budúcnosti poprieť, že to vytvoril on. Na dosiahnutie nepopierateľnosti treba dodržať ďalšie podmienky – základnou je, aby jediným vlastníkom certifikátu a príslušného podpisovacieho kľúča bol určitý konkrétny používateľ. Potom možno dosiahnuť tzv. nepopierateľnosť pôvodu vytvorenia. Ak elektronický podpis obsahuje aj tzv. časovú pečiatku (ide takisto o elektronický podpis, ktorý je však vytvorený nezávislou treťou stranou a obsahuje aktuálny čas), možno dosiahnuť aj nepopierateľnosť času vytvorenia. S týmito dvoma atribútmi vieme, ak si budeme bezpečne uchovávať všetky elektronické podpisy, KTO vykonal danú akciu a KEDY (napr. podal daňové priznanie, schválil faktúru, atď.). Tieto dva atribúty („kto“ a „kedy“) vytvorili z elektronického podpisu dostatočne silnú technológiu na to, aby sa uvažovalo o náhrade vlastnoručného podpisu elektronickým podpisom. S týmto cieľom vydal Európsky parlament a Rada EÚ Smernicu 1999/93/ES (13. decembra 1999), ktorou stanovuje (okrem iného) členským štátom, aby zabezpečili podmienky na vytváranie takých elektronických podpisov, ktoré by boli ekvivalentom vlastnoručných podpisov. Podľa našej legislatívy (Zákon č.215/2002 Z. z.) sa takýto podpis nazýva „zaručeným elektronickým podpisom“.

ELEKTRONICKÝ PODPIS A ZARUČENÝ ELEKTRONICKÝ PODPIS

Ak organizácia cíti potrebu zvýšiť bezpečnosť svojich aplikácii o atribút nepopierateľnosti (či už s časovou pečiatkou alebo bez), musí zabezpečiť viacero podmienok. V nasledujúcej tabuľke je stručný popis niektorých z nich v závislosti od toho, či organizácia bude používať ZEP alebo bežný EP.

ČO PONÚKA IBM

IBM Slovensko má v oblasti implementácie elektronického podpisu bohaté skúsenosti. Medzi ponúkané služby a produkty patrí aplikácia Sign Tools na vytvorenie a overenie zaručeného elektronického podpisu (ZEP) v zmysle zákona o elektronickom podpise 215/2004 Z. z. a knižnice alebo hotová aplikácia na vytvorenie a overenie elektronického podpisu prispôsobené potrebám zákazníka. Knižnice, resp. aplikácie môžu byť prispôsobené potrebám zákazníka z pohľadu funkčnosti (spôsob vytvárania elektronického podpisu, čo všetko sa má overovať pri podpise), formátu elektronického podpisu (okrem XML napr. aj PKCS#7), prostredia (Java, C++, Lotus Notes), atď. Ďalšou službou je analýza, návrh a implementácia systému využívajúceho elektronický podpis a princípy Public Key Infrastructure (PKI).

APLIKÁCIA SIGN TOOLS

Sign Tools je Java aplikácia bežiaca v prostredí Windows 2000 a Windows XP. Jadrom aplikácie je Java aplet, ktorý umožňuje vytvorenie zaručeného elektronického podpisu a overenie zaručeného elektronického podpisu podľa platnej

Porovnanie bežného a zaručeného elektronického podpisu

	Bežný elektronický podpis	Zaručený elektronický podpis
Aplikácia	EP vytvára a overuje aplikácia, na ktorú sa nekladú žiadne špeciálne bezpečnostné a funkčné požiadavky. Aplikáciu netreba certifikovať ani pravidelne auditovať.	ZEP vytvára a overuje aplikácia, ktorá musí spĺňať funkčné a bezpečnostné kritériá stanovené slovenskou legislatívou a Národným bezpečnostným úradom. Aplikáciu na vytvorenie a overenie ZEP treba certifikovať, pričom certifikáciu zabezpečuje NBÚ. Certifikácia aplikácie ZEP je formalizovaný a pomerne jasný proces. Jeho súčasťou je audit aplikácie nezávislým auditorom. Proces certifikácie zvyšuje dôveryhodnosť aplikácie ZEP a zavádza štandardy pre formát zaručeného elektronického podpisu.
Požiadavky na prostredie	Bezpečnostné a funkčné požiadavky na prostredie, v ktorom aplikácia beží definuje výrobca aplikácie v závislosti od predpokladanej úrovne bezpečnosti, ktorá sa môže od prípadu k prípadu líšiť (napr. potreba používania/nepoužívania čipových kariet na uloženie súkromného kľúča, atď.).	Na vytvorenie ZEP však nestačí len samotná certifikovaná aplikácia, funkčné a najmä bezpečnostné požiadavky sa dotýkajú celého prostredia (zariadenie na vytvorenie el. podpisu, operačný systém, podporné aplikácie na zvýšenie bezpečnosti počítača (napr. antivírus, firewall), fyzický prístup k počítaču, atď.), čo podstatne zvyšuje prvotné a prevádzkové náklady.
Certifikáty	Na vytvorenie a overenie EP musí existovať certifikát vydaný certifikačnou autoritou na verejný kľúč zodpovedajúci súkromnému kľúču, pomocou ktorého sa EP vytvoril.	Na vytvorenie a overenie ZEP musí existovať kvalifikovaný certifikát vydaný Akreditovanou certifikačnou autoritou (ACA) v zmysle zákona č. 215/2002 Z. z. Činnosť ACA, proces akreditácie, ako aj ďalšie aspekty spojené s vydávaním kvalifikovaných certifikátov upravuje Zákon o elektronickom podpise 215/2002 Z. z. Zoznam akreditovaných CA je na stránkach NBÚ (www.nbusr.sk).
Bezpečnostná a prevádzková dokumentácia	Úroveň a rozsah dokumentácie pre uzatvorené systémy sa môže v jednotlivých prípadoch dosť líšiť. Organizáciu zväčša stojí veľké úsilie vytvoriť primeranú dokumentáciu popisujúcu technické a netechnické aspekty vytvárania a overovania elektronického podpisu.	Vo všeobecnosti úroveň dokumentácie pre aplikácie ZEP ovplyvňuje nezávislý audítor a Národný bezpečnostný úrad, pretože zhodnotenie dokumentácie je súčasťou certifikačného procesu aplikácie ZEP. Preto je pravdepodobné, že úroveň dokumentácie aplikácií ZEP je približne rovnaká. Pre aplikácie na vytvorenie a overenie ZEP na niektoré typy dokumentov už existujú, aplikácia sa im musí prispôsobiť (napr. formáty ZEP, podpisové politiky pre ZEP). Tieto dokumenty vydáva a aktualizuje Národný bezpečnostný úrad.

slovenskej legislatívy. Aplikácia pracuje s dokumentmi vo formáte XML a XHTML. Výsledný zaručený elektronický podpis vytvára a overuje vo formáte XML. Aplikácia Sign Tools dostala certifikát bezpečnostného produktu pre ZEP od Národného bezpečnostného úradu s číslom 963/2005/IBEP-010 (pozri http://www.nbusr.sk/NBU_SEP/certifikaty/37.jpg), čo je podmienkou jej využita na vytvorenie a overenie zaručeného elektronického podpisu v zmysle platnej slovenskej legislatívy. Certifikácia bezpečnostného produktu pre ZEP je proces, v ktorého rámci sa overuje úroveň bezpečnosti aplikácie a ďalšie technické parametre predpísané NBÚ. Z tohto dôvodu (štandardizácia, garantovaná vysoká úroveň bezpečnosti) môže byť aplikácia Sign Tools užitočná aj v oblastiach, kde sa nevyhnutnosť používania ZEP nepredpisuje legislatívou.

KNIŽNICE, APLIKÁCIE A PRINCÍPY PKI

V oblasti implementácie elektronického podpisu poskytuje IBM ďalšie aplikácie a knižnice pre prácu s elektronickým podpisom, ktoré môžu byť prispôsobené potrebám zákazníka z pohľadu funkčnosti (spôsob vytvárania elektronického podpisu, čo všetko sa má overovať pri podpise), formátu elektronického podpisu (okrem XML napr. aj PKCS#7), prostredia (Java, C++, Lotus Notes), atď.
IBM Slovensko ponúka: * knižnice (*.dll alebo *.jar) na elektronický podpis, ktoré môžu byť zahrnuté do koncovej aplikácie, * knižnice + demo aplikáciu, ktorá predvedie použitie dodaných knižníc, * knižnice + kompletnú PKI aplikáciu, využívajúcu elektronický podpis.

SLUŽBY NA IMPLEMENTÁCIU SYSTÉMU

V prípade, že sa zákazník rozhodne implementovať alebo nasadiť systém využívajúci princípy PKI a elektronického podpisu, IBM môže poskytnúť skúsených odborníkov vo všetkých etapách vývoja. Ide o analýzu možného nasadenia elektronického podpisu a ďalších funkcií spojených s certifikátmi X.509 v prostredí zákazníka, ďalej o zhodnotenie možností nasadenia elektronického podpisu a návrh riešenia využívajúceho elektronický alebo zaručený elektronický podpis a napokon o, implementáciu riešenia zameranú na funkcionalitu

vytvárania a overovania elektronického alebo zaručeného elektronického podpisu ako aj ďalších funkcií spojených s certifikátmi X.509 (napr. šifrovanie a dešifrovanie dokumentov pomocou asymetrickej šifry).

MOŽNOSTI VYUŽITIA EP A ZEP

Elektronický podpis (tzv. „bežný“) sa využíva najmä v uzatvorených systémoch. Uzatvorený systém môžeme chápať ako systém, v ktorom sú aktéri (ten, kto podpisuje aj ten, kto overuje) vopred známi. Zvyčajne existuje medzi nimi právny vzťah uzatvorený formou zmluvy. Medzi najčastejšie uzatvorené systémy využívajúce elektronický podpis patria e-Banking aplikácie, správa a obeh dokumentov v rámci organizácie, informačné systémy v zdravotníctve.

Zaručený elektronický podpis sa využíva najmä v otvorených systémoch, hoci môže byť výhodné využitie aj v uzatvorených systémoch. Otvorené systémy zväčša chápeme ako systémy, v ktorom aktéri nie sú vopred známi. Bežným príkladom otvorených systémov sú tie, ktoré zabezpečujú komunikáciu medzi občanmi a štátnou resp. verejnou správou, napr. elektronická podateľňa. Zaručený elektronický podpis predstavuje drahšie riešenie (vo všeobecnosti predpokladáme vyššie prvotné aj prevádzkové náklady). Pre klientov však môže predstavovať výhody štandardizovaného riešenia, ktorého úroveň (z pohľadu bezpečnosti, funkčnosti a ďalších technologických aspektov) je hodnotená nezávisle audítorom a Národným bezpečnostným úradom. ■

IBM SOFTVÉR – bezpečná platforma pre riadenie procesov

Elektronický podpis s využitím čipových kariet v Slovenských elektrárňach, a. s.

„Využitie čipových kariet na elektronický podpis v systéme schvaľovania faktúr výrazne zvýšilo bezpečnosť systému a dôveru našich zamestnancov pri jeho používaní. Inštitút elektronického podpisu plánujeme využiť aj v ďalších procesoch, napríklad pri schvaľovaní a vyúčtovaní cestovných príkazov.“

Ing. Ladislav Cocher
výkonný riaditeľ pre informatiku a telekomunikácie, SE, a. s.

Vedenie informatiky v Slovenských elektrárňach, a. s., už dávnejšie realizovalo projekt používania identifikačných kariet zamestnancov na zabezpečenie vstupov do objektov. Tieto karty je však možné využiť aj na ďalšie účely, napríklad verifikáciu operácií pri údajoch v informačných systémoch, t. j. interný elektronický podpis.

V rámci reštrukturalizácie Slovenských elektrární sa zefektívnili a centralizovali podnikové procesy spracovania faktúr. Bolo potrebné vyriešiť proces schvaľovania takýchto dokladov bez potreby kolobehu papierových dokumentov. Tento problém bol vyriešený pomocou elektronického podpisu. Riešenie navrhla firma PosAm, spol. s r. o., spolu s firmou EMM, s. r. o.

■ Elektronický podpis a schvaľovanie

Proces spracovania faktúr v Slovenských elektrárňach vyžaduje pripojiť k faktúre likvidačný list faktúry podpísaný zodpovednými za jej likvidáciu. Ak sa tento proces realizuje mimo informačného systému, v organizácii kolujú stovky papierov a proces je neprehľadný. Ako je možné zmeniť túto situáciu? Využiť inštitút interného elektronického podpisu.

Elektronický podpis je spôsob, ako elektronickými prostriedkami zabrániť nepovolaným osobám predstierať cudziu identitu alebo zmeniť dokument. Podmienkou bezpečnosti je to, aby privátny kľúč vlastnil iba samotný používateľ. Z tohto dôvodu je z hľadiska bezpečnosti najlepším miestom na uloženie kľúča čipová karta.

■ Implementácia elektronického podpisu na čipovej karte a prínosy

V Slovenských elektrárňach sa na prevádzku Kancelárskeho informačného systému už od roku 1996 využíva platforma Lotus Notes/Domino od firmy IBM. Táto platforma poskytuje elektronický podpis spolu s podporou čipových kariet. Riešenie využíva Lotus Notes klienta vo verzii 6.0.2. so serverom Lotus Domino vo verzii 6.5.4. a aplikáciu pre workflow faktúr, vyvinula firma PosAm. Čipové karty použité pri riešení sú typu Schlumberger Cryptoflex, dodala ich firma EMM, spol. s r. o., ktorá realizovala aj aplikačnú podporu pre správu záznamov na čipovej karte.

Výsledkom riešenia je odstránenie zdĺhavého a nákladného procesu obehu dokumentov v papierovej forme a zabezpečenie jednoduchého, bezpečného a dohľadateľného kolobehu schvaľovania faktúr chráneného interným elektronickým podpisom. V súčasnosti má schvaľovanie faktúr a samotný prístup do Kancelárskeho informačného systému pomocou čipovej karty k dispozícii viac ako 1 000 používateľov. Slovenské elektrárne plánujú v krátkom čase využiť mechanizmus workflow s interným elektronickým podpisom aj pre ďalšie aplikácie.