

Digitální podpis

Až nás podepíše počítač...

Mluvit o digitálním podpisu, zejména o jeho využití ve státní správě, patří dnes k dobrému tónu – ne každý však ví, o čem je vlastně řeč. Na konferenci ISSS '99 (píšeme o ní na jiném místě) zazněla následující přednáška našeho kmenového autora, po jejímž přečtení určitě „budete v obraze“.

Príspevek se zabývá problematikou šifrování dat, ověřováním pravosti elektronických dokumentů, prevencí neoprávněného přístupu k chráněným údajům atd. Ukazuje, že technologie jsou připraveny řešit mnoho úkonů státní správy a samosprávy elektronickou cestou. Aplikace navrhovaných řešení by vedla k usnadnění života občana a zrychlení jeho styku s úřady, navíc by zpřehlednila mnoho dotčených systémů, což by vedlo k ohromným finančním úsporám. Bezpečná digitalizace našeho života je připravena, ale bez finanční a legislativní podpory státu a bez jeho koordinační úlohy to bude trvat velmi dlouho. Příklady z evropských zemí však ukazují, že to jde.

Seznámíme se nyní se základními pojmy a obrovskými možnostmi, které šif-

rovací technologie nabízejí pro řešení různých potřeb informační společnosti. Řada šifrovacích mechanismů je standardizována mezinárodní organizací pro

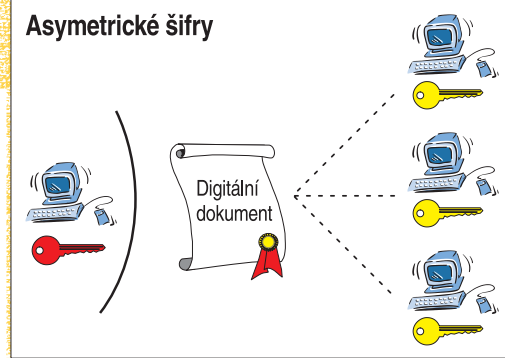
Šifrovací algoritmy

Šifrovací algoritmus je transformace, která převádí otevřená data na data zašifrovaná a naopak. Tato transformace je řízena **šifrovacím klíčem**. Při zašifrování se použije klíč pro zašifrování, při odšifrování klíč pro odšifrování. Jestliže oba tyto klíče jsou totožné, hovoříme o **symetrickém** šifrovacím algoritmu, jestliže jsou různé, o **asymetrickém** nebo také o šifrovacím algoritmu s **veřejným klíčem**.

Symetrické algoritmy se používají přímo k šifrování velkých objemů dat. Jejich klíče je nutné chránit a držet v tajnosti. Znalost šifrovacího klíče umožňuje

přístup k zašifrovaným datům a jeho nezalost tomuto přístupu zabraňuje. Neoprávněná osoba, která se dostane k uloženým zašifrovaným datům, je bez znalosti šifrovacího klíče nemůže odšifrovat a získat tak původní informaci. Pro pohodlí uživatelů je u mnoha těchto systémů šifrovací klíč uložen v chráněném hardwaru, například v čipové kartě, SIM kartě nebo obecně v tzv. **tokenech**. To jsou zařízení realizovaná jako drobné předměty nejrůznějších tvarů i podob – přívěsky na klíče, miniaturní infračervené ovladače, čipy v prstenu, tzv. dotykové paměti, čipové karty ap. Jejich uživatel si klíč nemusí vůbec pamatovat a v některých případech ho ani nemusí znát.

U **asymetrických šifer** se jiný klíč používá pro zašifrování a jiný klíč pro odšifrování. Oba klíče tvoří pár, takže jeden pracuje proti druhému – pozoruhodnou vlastností zde ale je, že jeden z nich může být **zcela veřejný** (u digitálních podpisů ho můžeme nazvat **ověřovací klíč**), aniž by z něj bylo možné odvodit odpovídající tajný klíč (u digitálních podpisů ho můžeme nazvat **podepiso-**



Asymetrické šifry.

standardizací ISO nebo národními standardizačními úřady, například NIST a ANSI. Bez šifrovacích funkcí by nemohly existovat například mobilní telefony GSM, platební karty, elektronický obchod, bezpečný přístup na internet ani bezpečná výměna dat.



Takhle se pořizuje digitální podpis u průkazu.





vací). Asymetrickým šifráem se proto také říká kryptosystémy s **veřejným klíčem**. Ukážeme si, že jejich použití (doucejme, že už brzo) změní náš občanský život k lepšímu. Základem všech těchto příjemných změn je digitální podpis.

Digitální podpis

Digitální podpis není ani „verš z nějaké domluvené básničky, který se připojí za text“, ani „naskenovaný a digitalizovaný vlastnoruční podpis“, jak se mnozí domnívají. Digitálně lze podepsat nejen text, ale libovolný soubor dat, přístupová práva, položku v databázi, lékařský záznam nebo fotografii.

Digitální podpis vytváří „signatář“ použitím svého tajného klíče na podepisovanou data. Digitální podpis je tedy číslo vypočítané v závislosti na podepisovaných datech, a není proto možné kopírovat jej z jednoho dokumentu na druhý. Podpis nemůže vytvořit nikdo jiný, než vlastník tajného podepisovacího klíče. Všichni ostatní mohou ale podpis ověřit, protože ověřovací klíč je veřejný – a zpravidla bývá šířen přímo s příslušným (otevřeným) dokumentem. Digitální podpis je široce využíván a mezinárodně standardizovaná technika; například v USA byl vydán vládní standard DSS (Digital Signature Standard), vytvořený pro potřeby digitálního podepisování v celé státní správě. Podrobněji si oněm můžete přečíst hned za tímto příspěvkem na str. 40.

Konečně konec papírování?

Digitální podpis se dá využít všude tam, kde je dnes nutné úřední razítko či ruční podpis občana nebo úředníka. Všechny dokumenty, které zatím známe v papírové podobě, můžeme převést na dokumenty elektronické a všechny podpisy občanů, úředníků a razítka úřadů umíme převést na jejich digitální formu! Umíme tak podepisovat i ověřovat podpisy nesrovnatelně rychleji a efektivněji, umíme podepsat dokonce i to, co lze ručně velmi těžko – obsah diskety, fotografii osoby, plán objektu, dotaz do databáze ap. Jakékoliv současné papírové dokumenty lze dnes už vydávat v digitální podobě!

Nevěříte? Snad vás o výhodách informační společnosti přesvědčí jedna z možných představ využití digitálního podpisu – stačí jen trochu popustit uzdu



Nosiče digitálních dokumentů mohou mít různou formu.

fantazii a vydat se s námi do – doufejme – blízké budoucnosti.

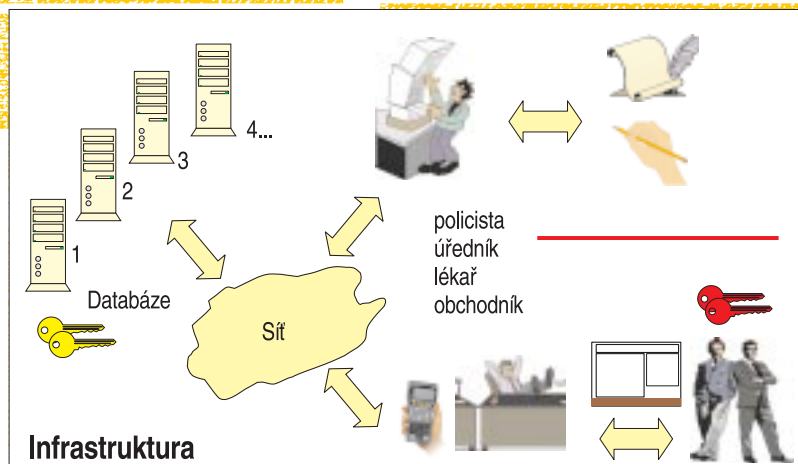
Univerzální elektronická karta

Digitální podpis je založen na složitých matematických (kryptografických) funkcích, které musí provádět mikropočítač, a do jeho paměti je také nutné uložit podepisovací a ověřovací klíče. Zařízení, které obsahuje mikropočítač, nazvěme **univerzální elektronickou kartou**

slušná rozhraní – například infračervený či sériový kanál, bezkontaktní čip, dotykovou paměť ap. UEK může být před odcizením chráněna přístupovým heslem nebo PIN, podobně jako platební karty.

Terminály

Na všech úřadech a poštách, v lékárnách, obchodech, bankách, v zaměstnání, v dopravních prostředcích i v domácnostech mohou být stacionární nebo mobilní **terminály**, které slouží pro komunikaci s UEK (tj. pro čtení a zápis informací). UEK může s některými terminály komunikovat **automaticky** (například při průchodu občana do objektu, dopravního prostředku ap.) nebo **manuálně** (vložením, pohybem, dotykem, infračerveně, dálkovým ovládním). Terminály mohou mít různou formu – od velmi malých ručních čteček v terénu přes čtečku čipových karet nebo infračervený port osobních počítačů až po informační kiosky s velkým dis-



Infrastruktura je tvořena centrálními databázemi, terminály a digitálními doklady.

(UEK). Může mít formu čipové karty nebo tokenu velikosti minikalkulačky (silnější čipové karty) s velkou pamětí a eventuálně s miniklávesnicí a mini-displejem (v pokročilé verzi třeba i se snímačem otisků prstů). Občan nosí UEK u sebe místo průkazů, drobných peněz a různých klíčů. UEK musí mít pro komunikaci s okolím (tj. s terminály) pří-

plejem, reproduktorem nebo pomůckami pro nevidomé.

Komunikační prostředí terminálu může být heterogenní. Jako velmi vhodné se pochopitelně jeví využití internetu. Některé terminály mohou mít vlastní (lin-



kové, rádiové) spojení s centrální databází. Spojení může být on-line, občasně nebo zcela off-line. Cílem je zajistit spojení mezi UEK, terminály a centrální databází.

Koncepce UEK

UEK obsahuje paměť rozdělenou na listy, přičemž každá aplikace si vyhradí vlastní list, odkud čte nebo kam zapisuje informace. Nic nového, řeknete asi – podstatné však je, že každý z těchto záznamů je digitálně podepsán příslušným úřadem nebo oprávněnou osobou.

Každá aplikace může dále mít svoji centrální databázi, zcela nezávislou a zcela oddělenou od ostatních a spravovanou odpovědným úřadem. V případě potřeby dochází k on-line nebo off-line výměně dat mezi UEK a centrální databází. Některé aplikace mohou čerpat informace i z několika databází.

Podobně jako data, také práva jednotlivých aplikací (např. číst z listů jiných aplikací, zápis do centrální databáze) jsou digitálně podepsána oprávněnými subjekty. Ochrana dat i digitální podpisy jsou řešeny standardizovanými kryptografickými prostředky a celý systém je na požadované bezpečnostní úrovni podle platných norem.

Centrální databázi si zajišťuje každý úřad nebo komerční instituce (banky, telekomy...) samostatně. Vzájemné interakce mezi databázemi jsou vytvářeny a schvalovány jejich vlastníky. Každá centrální databáze si podle potřeb může vést aktuální stav obsahu listu dané aplikace v UEK každého jejího uživatele – mimo jiné i pro jednoduchou obnovu obsahu UEK při jeho ztrátě.

Možné aplikace

Každý občan může mít obsah UEK jiný, podle toho, do jakých aplikací je zahrnut. Aplikace může například digitálně zajišťovat:

- ▀ úřední listy – rodný, oddací, úmrtní atd.;
- ▀ doklady o vzdělání – vysvědčení, diplomy, certifikáty;

- ▀ průkazy – občanský, řidičský, technický, knihovní, vysokoškolský, o zdravotním a sociálním pojištění, MHD, cestovní pas;

- ▀ platební prostředky – elektronické peněženky (EP), závodní a školní stravování, telefonní karty ap.;

la ho k proplacení pojišťovně. Nedošlo k neoprávněnému vykazování úkonů, neoprávněným platbám, výdeji léků, padělání receptů. Příkladů využití UEK je velmi mnoho a jistě si dovedeme představit, jak by nám takový systém ulehčil život.



- ▀ klíče – pro šifrování a podepisování elektronické pošty, k otevírání dveří (dům, auto, kancelář), přístup do vyhrazených prostor, přihlašovací hesla do sítí, šifrovací a autentizační klíče, klíče pro bankovní operace atd.;

- ▀ další „průběžné“ doklady, např. lékařské recepty aj.

Možných aplikací je samozřejmě ještě mnohem více.

Příklad použití

Ukažme si nyní pro názornost konkrétní způsob použití UEK, dejme tomu ve zdravotnictví. Při návštěvě lékaře vložíme UEK do jeho čtečky. Na monitoru lékaře se objeví naše fotografie a osobní údaje, v centrální databázi vidí své zápisy z poslední návštěvy. Úkony, které provede, vloží do databáze a vystaví digitální recept. Odejeme do lékárny, představíme se svou UEK. Lékárník vidí v centrální databázi vystavený recept (nebo, pokud chceme, může být uložen přímo do UEK), vydá léky a odečte si z naší EP příslušný poplatek.

Toť vše. Nepotřebovali jsme průkaz pojištěnce, recept, drobné. Nikdo nevypisoval zbytečné údaje. Lékař ani lékárník nepsali žádná hlášení pro zdravotní pojišťovnu. Úkony jsou zdokumentovány a zúčtovány mezi centrálními databázemi. Lékař viděl, že máme platný průkaz pojištěnce, jeho úkony byly pro naši pojišťovnu zaznamenány a jím podepsány. Recept byl podepsán lékařem, lékárna ho ověřila, zaznamenala na něm vydání léku a podpis lékárníka. Odesla-

Legislativa a projekty

Podívejme se nyní, do jaké míry se naznačenému ideálu blíží některé vyspělé země a jak jsme daleko u nás. Poznamenejme ale hned úvodem, že v EU zatím neexistují harmonizované zákony pro ochranu dat a elektronických transakcí. Byla však například vydána Direktiva EU o ochraně databází a další ně-

kteří normy, které mají zatím charakter doporučení.

Spolková republika Německo

V oblasti legislativy je v Evropě nejdále SRN, která má svůj zákon o digitálním podpisu. Byl přijat v souvislosti se zákonem o informacích a telekomunikacích a vstoupil v platnost v roce 1997. Německo se tak stalo historicky prvním státem, který zákonem upravil rámcové podmínky pro ověření platnosti digitálního podpisu a používání nezbytných kryptografických prostředků.

Konkrétně to znamená, že zákon mj.:

- ▀ stanoví pravidla pro vznik systému certifikačních autorit (CA) na základě volné soutěže a pravidla pro jejich uznávání a kontrolu, definuje minimální požadavky na bezpečnost CA;
- ▀ zakotvuje průkaznost digitálního podpisu v souvislosti s používáním elektronických dokumentů;
- ▀ neomezuje použití technických prostředků pro digitální podpis na žádné národní standardy, a vytváří tak široké možnosti pro budoucí integraci tohoto systému do mezinárodního prostředí;
- ▀ uznává privátní podepisovací klíč jako unikát, kterým je možno jednoznačně prokázat autenticitu jeho použití danou osobou, a zároveň stanovuje požadavek ochrany tohoto klíče „všemi dostupnými technickými a organizačními prostředky“.



Rakousko

Ministerstvo školství Rakouska zavedlo *elektronické studentské průkazy* (tzv. INDEX). INDEX je technicky založen na čipové kartě (smart card), kterou studenti používají jako index, autentizační prostředek k prokazování své identity, pro plánování přednášek a placení ve studentské jídelně. Další projekt počítá s vybavením každého pracujícího v Rakousku kartou, která bude sloužit jako *průkaz občana pro sociální a důchodové pojištění* a podobné účely.

Belgie

Každý občan Belgie obdrží nyní víceúčelovou elektronickou kartu, která obsahuje jméno nositele, datum narození, identifikační číslo sociálního zabezpečení, údaje o jeho pojištěních, vybrané zdravotní údaje, záznamy o předchozích zaměstnavatelích, době nezaměstnanosti, úrazech apod. Vydáním této tzv. *sociálně-identifikační karty* (v tomto roce 10,5 milionu kusů) chce příslušné ministerstvo zabránit podvodům občanů a institucí v oblasti sociálního zabezpečení. Majitelům terminálů v nemocnicích, lékárnách, podnicích, pojišťovnách, bankách a jinde karta umožní, aby se spojili s databází ministerstva sociálních věcí a zjistili si potřebné údaje. Předpokládá se, že systém usnadní přenos informací mezi zaměstnavateli, sociálními a daňovými úřady a znemožní různé podvody, mj. i zaměstnat někoho bez pracovního povolení.

Česká republika

Jak jste nejspíš očekávali, současný stav české legislativy není pro použití digitálního podpisu ideální. Zákon o účetnictví č. 156/1991 Sb. sice připouští prokazování autentičnosti některých dokumentů jiným prokazatelným způsobem než jenom klasickým podpisem, ale vlastnosti digitálního podpisu nejsou nikde specifikovány. Na druhé straně zákon tento způsob podepisování nezakazuje. V obchodním styku mohou být uznávané digitálních podpisů i další způsoby autentizace smluvně dohodnuty mezi zúčastněnými stranami. Podobně to řeší zákon o telekomunikacích č.110/1964 Sb., který ponechává výběr metod ochrany, autentizace a důkazu autenticity na

zúčastněných stranách. K ochraně dat existuje zákon č. 256/1992 Sb., který provozovatelům informačních systémů ukládá chránit osobní data. Některé současné legislativní iniciativy usilují o zavedení pravidel pro ochranu databází, pro právní uznání elektronických transakcí, digitálních dokumentů, certifikačních autorit a digitálního podpisu.

Závěr

Pokusili jsme se ukázat možné využití šifrovacích technologií pro ochranu dat a digitální podpisy. Nastínili jsme možnosti technické realizace a výhody, které by z uplatnění této technologie plynuly pro stát a občana. Na závěr jsme uvedli stav legislativy a příklady konkrétních projektů evropských zemí, které dokazují, že se dnes už nejedná o žádné vize, ale o realitu.

Určitě není bez zajímavosti, že – jak vplynulo z kuloárové diskuse po proslovení tohoto příspěvku na ISSS '99 – jenom odstranění určitých nesrovnalostí v oblasti zdravotního pojištění, které by nastalo v důsledku zavedení digitálních průkazů, by u nás zaplatilo tento projekt během jednoho roku. Vtírá se otázka, zda je to žádoucí a pro koho...

Na závěr bych ještě rád vyjádřil poděkování ing. Škopové z firmy Decros za poskytnutí cenných informací, zejména k otázkám legislativy a existujících projektů.

Pokud vás problematika digitálního podpisu zaujala hlouběji, na následujících stránkách se můžete seznámit s jednou z jeho možných technických realizací.

VLASTIMIL KLÍMA (VKLIMA@DECROS.CZ)

O autorovi:

RNDr. Vlastimil Klíma (42) vystudoval Matematicko-fyzikální fakultu Univerzity Karlovy v Praze a v oboru matematika tamtéž získal titul doktora přírodních věd. Od roku 1982 se věnuje kryptologii a ochraně dat, v současné době ve firmě Decros. Je členem mezinárodní asociace pro kryptologický výzkum, častým přednášejícím na konferencích a publicistou v oblasti ochrany dat a šifrování. Podílel se též na tvorbě řady šifrovacích prostředků.