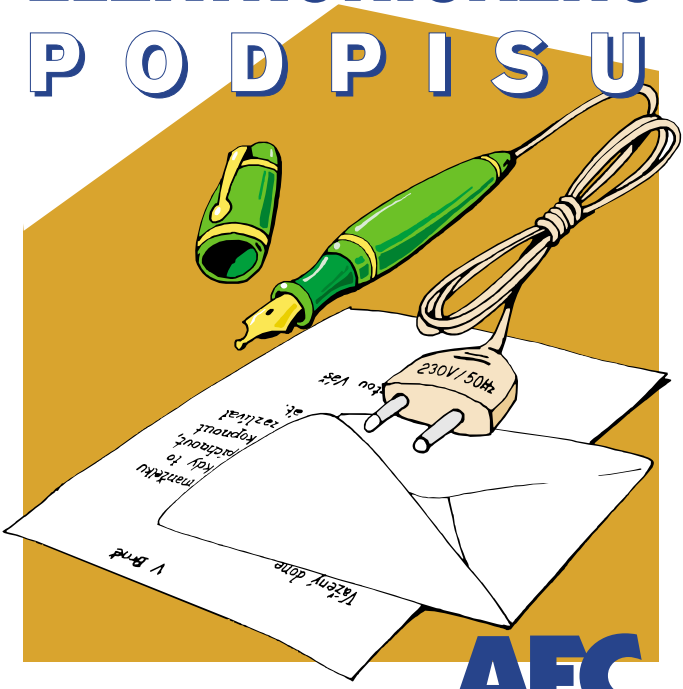
PC WORLD

SVĚT ELEKTRONICKÉHO PODPISU



Tomáš Přibyl
a kolektiv

AEC
DATA SECURITY COMPANY

Tomáš Přibyl a kolektiv

SVĚT ELEKTRONICKÉHO PODPISU

OBSAH

ÚVOD ANEB RIZIKA "ŽIVOTA" V KYBERNETICKÉM PROSTORU

Vítejte v kyberprostoru, milí přátelé!

Možná vám toto úvodní zvolání bude připadat ze stejné říše vědy a fikce (tedy sci-fi) jako zvolání kapitána mezihvězdného korábu tuctového amerického seriálu, když posádce oznamuje: Vítejte v meziprostoru, přátelé!

Ovšem kyberprostor už dávno nepatří do říše představ vizionářů. A v tom je právě jeho největší nebezpečí. Zatímco o existenci reálného světa snad nikdo nepochybuje, v případě kybernetického prostoru si málokdo dokáže představit něco konkrétního.

V reálném světě jsou jasně daná pravidla, viditelné následky a důsledky našeho chování - a navíc v něm žijeme od narození. Naproti tomu kybernetický prostor není definovaný, chybí v něm pevná pravidla a vstupujeme do něj teprve dříve či později z reálného světa.

Rozdíl mezi reálným a kybernetickým světem si asi nejlépe uvědomíte v okamžiku, kdy vám někdo odcizí počítač. Smutek nad jeho ztrátou a s tím spojenou nutností nákupu nového hardware zakrátko přebolí, ovšem vyvstane otázka jiná: Co moje data? I v případě, že jste pravidelně a důsledně zálohovali, není vyhráno. Vaše data a informace se totiž dostala do rukou nepovolaných osob. Ke komu se asi dostane vaše účetnictví, kontakty na vaše (nejen) obchodní partnery a partnerky... Když už nic jiného, bude otřesena důvěra okolí ve vás, neboť jste nebyli schopni zabránit zneužití těchto citlivých dat...

Tato brožurka byla napsána s cílem co nejvíce minimalizovat možná rizika související s pohybem v kybernetickém prostoru. Přečtěte si ji pozorně a zamyslete se. Zamyslete se nad sebou a svými daty v elektronické podobě. Těžko kdy uděláte pro jejich bezpečí všechno, ale alespoň na základní opatření by pamatováno býti mělo...

Tomáš Přibyl, srpen 2000
tomas.pribyl@aec.cz

P.S. Chtěl bych alespoň touto cestou poděkovat všem, kdo mi s přípravou této publikace pomohli, ať již radou nebo poskytnutím informací či jakýmkoliv jiným způsobem. Jsou to (v abecedním pořadí) Milan Černoch, Petr J. Drahovzal, Miloš Kuchař, Jiří Mrnuštík, Jan Novotný, Jaroslav Pinkava, Alena Řezníčková a Leoš Vojíř. Zvláštní dík za trpělivost patří také mé drahé manželce Katce.

Všechny chyby a nepřesnosti v této publikaci obsažené ovšem padají plně na mou hlavu.

Autor

ŠIFROVÁNÍ: PROČ?

Pravděpodobně většinu z nás někdy napadla dětská otázka: Proč? Proč šifrovat, když je to něco, co není nezbytně nutné, komplikuje nám to život, zdržuje od práce, přidává další starosti, kterých už máme beztak nad hlavu... Jenže toto všechno není tak docela pravda.

Ano, je pravdou, že svět bez šifrování by byl jednodušší. Ale na druhé straně šifrováním...

...chráníte citlivá data. Ani v případě, že dojde k odcizení hardware či "pouze" k hackerskému průniku do vašeho systému, nemusíte mít obavu, že by citlivá data padla do rukou nepovolaným osobám.

...zajišťujete kontrolu přístupu k datům. Stanovíte jasná pravidla, kdo má k jakým informacím přístup. Pak se omezí na minimum situace "já nic, já muzikant". Jasná pravidla znamenají také jasnou odpovědnost.

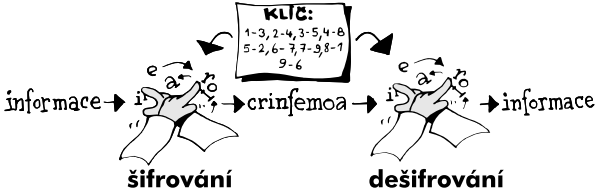
...chráníte se před útoky počítačových virů. Zašifrované informace totiž viry nedokáží napadnout - a pokud se o to přece jen pokusí, šifrovací program ihned pozná, že data byla pozměněna.

...zvyšujete svou vlastní důvěryhodnost, neboť dbáte na ochranu citlivých údajů a informací. Ostatně, jak se díváte z hlediska důvěryhodnosti na instituci, z níž unikají informace všemi možnými i nemožnými směry?

A takto bychom mohli pokračovat. Ještě pochybujete o užitečnosti šifrování a ochrany dat vůbec?

SYMETRICKÉ ŠIFRY A ŠIFROVÁNÍ

Jak již samotný název napovídá, symetrické (tedy "souměrné") šifry používají stejný šifrovací klíč jak pro proces zašifrování dat, tak pro jejich návrat do původní podoby (tedy dešifrování). Výhodou symetrického šifrování je potřeba pouze jednoho jediného klíče - ten se používá ke všem úkonům se zpracovávanými daty (ruku v ruce s tím souvisí i vyšší rychlost práce počítače při šifrování a dešifrování). Ovšem tato výhoda je na druhé straně i nevýhodou, neboť ve chvíli, kdy dochází k prozrazení tohoto klíče, jsou de facto "odkryta" všechna jím zašifrovaná data. V praxi se symetrické šifry využívají především pro zašifrování zálohovaných dat apod.



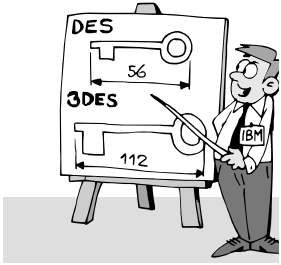
Obrázek nám názorně představuje princip šifrování za použití symetrického klíče. Na vstupu potřebujeme data, která chceme zpracovat do

zašifrované podoby, a šifrovací klíč. Tím nám vznikne zašifrovaná informace, přičemž přístup k datům v ní získáme využitím šifrovacího klíče.

Mezi nejznámější symetrické šifry patří následující algoritmy:

DES. Byl vyvinutý v laboratořích firmy IBM již v sedmdesátých letech, následně se v roce 1977 stal americkou vládní normou pro šifrování. Používá klíče, který má délku 56 bitů. Vzhledem k tomu, že vývoj výkonu výpočetní techniky se za poslední dvě desetiletí vydal vpřed šíleným tempem, DES již přestává dostačovat současným požadavkům. Dokonce se tuto šifru podařilo "rozbít", a to za pomoci "hrubého útoku" (zkoušením všech možných kombinací - podobně jako když chcete zjistit nastavení číselného kódu trezoru a zkoušíte všechny možné kombinace). Byť k tomuto "rozbití" bylo nasazeno obrovské množství kapacity počítačů, a tudíž nepředstavuje ve skutečném světě větší hrozbu, šifra přece jen přišla o svou "nevinnost" a do budoucna jako "nevěsta" postrádá perspektivu.

3DES (Triple-DES). Jde o zesílenou variantu algoritmu DES, při jejímž použití jsou data šifrovaná algoritmem DES jednoduše "přešifrována" třikrát. Zatímco původní DES má (jak bylo výše uvedeno) klíč dlouhý 56 bitů, TripleDES pracuje s dvojnásobným (112 bitů) nebo trojnásobným klíčem (168 bitů). Při použití dvojnásobného klíče jsou data šifrována tak, že je z klíče vzata první polovina a data jsou jí přešifrována. Vzápětí poté jsou druhou polovinou klíče data zašifrována podruhé. A do třetice - data jsou potřetí zašifrována první částí klíče. Algoritmus je poměrně pomalý, nicméně bezpečný. Tento algoritmus byl vyvinut, protože starší systémy pracující s DESem potřebovaly silnější algoritmus a s přechodem na TripleDES bylo nejméně potíží s kompatibilitou.



IDEA. Je to poměrně perspektivní algoritmus (klíč dlouhý 128 bitů). Z hlediska uživatele nesmírně příjemnou vlastností je vysoká rychlost práce - při nesrovnatelně vyšším stupni bezpečnosti je několikanásobně rychlejší než DES (o TripleDES ani nemluvě). Na rozdíl od výše uvedeného DESu se kryptologové dosud marně snaží najít slabinu tohoto algoritmu a "rozbít" jej. (Stav k 31. srpnu 2000 - kryptologie jde kupředu mílovými kroky a příliš si nepotrpí na dogmata stylu "šifra je nerozbitná".)

BlowFish. Algoritmus pro symetrické šifrování s proměnnou délkou klíče, a to od 32 do 448 bitů. Obvykle je ovšem implementován s délkou klíče 128 bitů. BlowFish je rychlý a bezpečný, navíc jej lze volně užívat, neboť není patentovaný.

CAST (zkratka z prvních písmen jmen jeho autorů, jimiž jsou Carlisle Adams a Stafford Taverns). Co se rychlostní i bezpečnostní charakteristiky týká, je velmi podobný výše uvedenému algoritmu BlowFish. Obvykle se používá s délkou klíče 128 bitů, jsou ale možné i jiné délky. CAST (zkratka z prvních písmen jmen jeho autorů, jimiž jsou Carlisle Adams a Stafford Taverns). Co se rychlostní i bezpečnostní charakteristiky týká, je velmi podobný výše uvedenému algoritmu BlowFish. Obvykle se používá s délkou klíče 128 bitů, jsou ale možné i jiné délky.

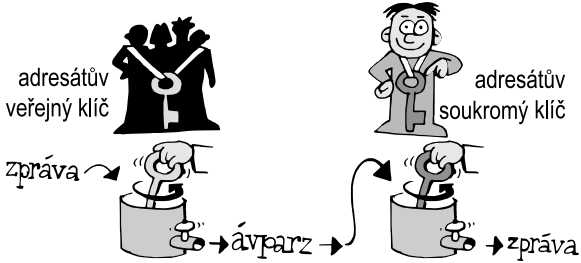
ASYMETRICKÉ ŠIFRY A ŠIFROVÁNÍ

V předchozí pasáži jsme se lehce seznámili se symetrickými šiframi, v jejichž případě se pro šifrování i dešifrování využívá stejného klíče. Jak už název asymetrického (nesouměrného) šifrování napovídá, při tomto způsobu zabezpečení informací jsou používány dva klíče - jeden pro zašifrování, druhý pro dešifrování. Při generování klíče pomocí speciálního počítačového programu přitom jde o jeden klíč, který se později "rozdělí" na dvě části.

První z těchto částí nese přízvisko "veřejný klíč" a poskytne se všem, od koho chceme dostávat šifrovaná data. Druhou část (soukromý klíč) si

ovšem musíme chránit jako oko v hlavě! Pokud by k němu někdo získal přístup, získal by přístup i k datům určeným pouze pro nás! (Soukromý a veřejný klíč společně nazýváme klíčový pár.)

Než si na naší pomyslné cestě tajemným zámkem šifer a šifrování ukážeme další komnatu, je zapotřebí zodpovědět jednu základní otázku týkající se bezpečnosti. Pokud má veřejný klíč k dispozici prakticky kdokoliv, nemůže s jeho pomocí nějakým způsobem dešifrovat informace určené



pouze pro mě (vždyť veřejný a soukromý klíč byly původně jedno!)? Odpovědí je jednoznačné NE! Tato obava není na místě, neboť asymetrické algoritmy využívají pro svou činnost matematické postupy, jejichž reverzní funkce je neproveditelná (při současném stavu vývoje). Vrátíme-li se do lavic základní školy, jistě si vzpomeneme na dělení se zbytkem. Vezměme si příklad jedenáct děleno třemi se rovná tři, zbytek je dva. A pokud si vezmeme za základ k dalšímu výpočtu pouze onen "zbytek", nemáme pražádnou šanci získat původní číslo. Ze zbytku prostě původní číslo bez znalosti dalších informací (kde je ovšem vzít?) prostě nevytvoříme...

Výše uvedené dělení se zbytkem je hodně primitivní příklad a se skutečnou kryptografií nemá zhola nic společného, ale pro ilustraci nevratných matematických funkcí je dostatečné.

Vraťme se ovšem od otázky bezpečnosti asymetrických šifer k otázce jejich principu. Opět nám k tomu pomůže obrázek. Tentokrát potřebujeme kromě informací, které chceme zašifrovat, také dvojici klíčů - veřejný a soukromý. Data veřejným klíčem může zašifrovat prakticky kdokoliv, ovšem přečíst si je dokáže pouze držitel soukromého klíče.

Mezi nejznámější asymetrické šifry patří následující algoritmy:

RSA. Jedná se o algoritmus nejen pro výměnu klíčů, ale i tvorbu elektronického podpisu, přičemž patří mezi neoficiální standardy. Jedná se o algoritmus patentovaný pro severní Ameriku do roku 2000. Bezpečnost algoritmu RSA je založena na skutečnosti, že je nesmírně obtížné rozložit velká čísla (z nichž každé je součinem dvou velkých prvočísel). Mimo to ovšem záleží také na délce použitého klíče. Pokud má délku 384 bitů, "rozbije" jej prakticky každá odborná firma. Klíč dlouhý 512 bitů představuje úkol pro instituce jako je FBI či CIA. Předpokládá se, že dlouho bezpečné nebudou ani klíče dlouhé 768 bitů - nikoliv však kvůli nedokonalosti algoritmu, ale zásluhou překotného rozvoje možností výpočetní techniky. Klíče o délce 1024 bitů budou bezpečné, pokud nebude dosaženo zásadních pokroků v řešení úloh faktorizace. A klíč 2048 bitů? Pokud se nestane nějaký absolutní zázrak, vydrží po několik desetiletí...

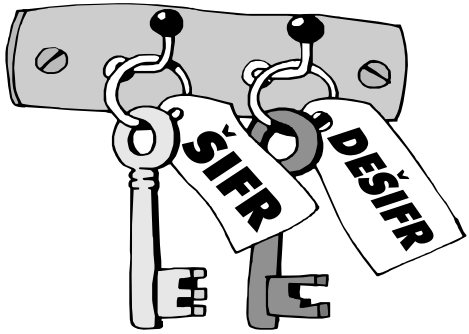
Eliptické kryptosystémy (ECC). Jedná se o moderní algoritmy založené na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. Světový vývoj nasvědčuje tomu, že v nich je skryta budoucnost asymetrických šifrovacích algoritmů. Jejich hlavní výhodou je značná bezpečnost při použití poměrně krátkého klíče (reklamní letáky by asi psaly, že mají skvělý "poměr cena/výkon"). Pro srovnání: K dosažení stejné bezpečnosti jako RSA s délkou klíče 2048 bitů potřebují eliptické křivky klíč dlouhý 160 až 180 bitů!!!

TYPY ŠIFROVÁNÍ

Podle toho, co a jakým způsobem potřebujeme chránit, rozlišujeme několik typů šifrování, a to

- on-line šifrování,
- off-line šifrování,
- on-demand šifrování.

Podívejme se nyní na jednotlivé typy podrobněji.



On-line šifrování - Jde o technologii, která zajišťuje šifrování/dešifrování informací v reálném čase. Jinak řečeno - na disku jsou uložené zašifrované informace. Uživatel k nim požádá o přístup, přičemž příslušný program ověří, zda na takovouto žádost má nárok (tedy zdali má právo disponovat s příslušným šifrovacím klíčem - ten může mít buď ve svém počítači, nebo může být někde na serveru, a nebo může jít o skupinový klíč, který je přiřazený několika uživatelům - všichni jej pak mohou využívat pro přístup ke společným datům). Pokud má na přístup k šifrovanému souboru

nárok, počítač jej dešifruje a příslušné aplikaci umožní přístup k datům (textový či tabulkový dokument apod.). V případě ukládání změn je postup opačný - dojde k zašifrování a uložení. Na disku se tak stále vyskytují pouze zašifrované informace, z nichž je do "čitelné" podoby dešifrována pouze malá část, kterou právě příslušná osoba vyžaduje.

Off-line šifrování - Tato technologie je založena na jiné filozofii než on-line šifrování, nešifruje data v reálném čase. Jejich dešifrování probíhá jednorázově např. při přihlášení uživatele do systému nebo na vyžádání. Zašifrování pak probíhá při odhlášení nebo opět na vyžádání v případě potřeby. Výhodou je, že jsou k dispozici okamžitě veškerá data bez nutnosti je v průběhu práce šifrovat a dešifrovat, nevýhodou je potřeba před a po práci dešifrovat/zašifrovat veškerá data, což je časově poněkud náročnější úkon.

On-demand šifrování (šifrování na vyžádání). Jedná se o nejjednodušší variantu zajištění bezpečnosti informací šifrováním. Používá se především v případě, kdy je potřeba něco "mimořádně" zašifrovat. V systému Windows bývají tyto funkce zpravidla k dispozici po stisknutí pravého tlačítka myši (máte-li ovšem nainstalovaný příslušný šifrovací program). "Lepší" šifrovací programy umožňují i šifrování do tzv. samorozbalovacích (Self-Extract) souborů s příponou exe. Při šifrování zadáme heslo, bez jehož znalosti není možné soubor rozbalit. Zašifrovaný soubor poté pošleme třeba elektronickou poštou nebo předáme na disketě příjemci, přičemž mu musíme sdělit i heslo (nejlépe dohodnuté osobně nebo jinou cestou; posílat e-mailem spolu se zašifrovaným souborem heslo je stejně bezpečné jako si na bankovní kartu psát PIN...). Po doručení exe souboru a pokusu o jeho spuštění bude adresát dotázán na heslo: Pokud jej zná, data budou rozšifrována, pokud nikoliv, nikdy se k nim nedostane. Výhodou tohoto řešení je skutečnost, že umožňuje předávat šifrovaná data i prakticky komukoliv, tedy nejenom lidem vlastnícím šifrovací program. Tato metoda je použitelná i v případě, kdy potřebujeme zašifrovat zálohy dat a informací.

Nemusíme pak mít obavu, že v případě ztráty šifrovacího klíče o data přijdeme - stačí pouze znát heslo, jehož ošetření je přece jenom o chlup snadnější (zvláště z dlouhodobého hlediska) než v případě softwarového klíče. Nepleťte si toto šifrování do EXE souboru se "zipováním" pod heslem! V našem případě je heslová fráze použita k vygenerování šifrovacího klíče a je (na rozdíl od Zipu) použita standardní silná šifra.

MÝTY O ŠIFROVÁNÍ

Také patříte k jedincům, kterým se při vyslovení slova "kryptografie" nebo "šifrování" nedělá dobře? Také si ihned vybavíte svět špiónů se všemi jeho příjemnými i odvrácenými stránkami? Dost možná, že ano. V očích veřejnosti totiž vznikla a dosud koluje o kryptografii řada mýtů a tajemství, které se pokusíme objasnit.

Tak tedy není pravdou, že

- **Kryptografie se zabývá jen šifrováním** - Kryptografie má prostředky pro dosažení několika cílů. Všichni intuitivně předpokládáme, že kryptografie se hodí výhradně na šifrování a odšifrování textu, a to tak, aby jej nebyl schopen číst nikdo, kdo nezná správný klíč a šifrovací algoritmus. Kryptografie vám však může nabídnout i další služby - například prostředky pro zajištění integrity dat - tj. zajištění kontroly nad tím, zda zpráva nebyla během své cesty změněna. Další možností je zajištění autenticity zprávy - tj. dává nám takový prostředek, abychom byli schopni ověřit, zda zpráva pochází skutečně od příslušné osoby a nebyla podvržena během své cesty.
- **Aplikace kryptografie jsou složité na užívání** - Už slovo kryptografie v nás vzbuzuje pocit něčeho nadmíru složitého. Ano, abychom plně porozuměli principu činnosti šifrovacích algoritmů, potřebovali bychom rozsáhlé matematické znalosti. Ty však nepotřebujeme k tomu, abychom tyto algoritmy mohli bez problému používat. Celá složitá matematika pak

bývá skryta pod jediným tlačítkem, které po stisknutí zařídí vše potřebné. Takže většina aplikací šifrovacích algoritmů je důmyslně skryta a pracuje zcela automaticky.

- **Utajovaný algoritmus je bezpečnější než veřejný** - V minulosti se již několikrát stalo, že šifrovací algoritmus byl prolomen díky chybě v jeho návrhu. Proto principy dnes používaných algoritmů jsou obvykle veřejně dostupné. Je to proto, aby se k nim mohl kterýkoli z kryptologů vyjádřit a případně upozornit na jeho slabá místa. Proto jsou tyto algoritmy obecně považovány za bezpečnější, než algoritmy, jejichž princip je tajen. Proto se dnes ve velké většině používají algoritmy, jejichž princip je veřejně znám.
- **Kvalita zabezpečení informace je dána pouze délkou šifrovacího klíče** - Tento mýtus vznikl obecnou neznalostí principu použití šifrovacích algoritmů. Kvalita šifrovacího algoritmu je samozřejmě velice důležitá, ale neméně důležité je i například místo, kde se ukládají šifrovací klíče a způsob jakým jsou chráněny. V dnešní době jsou ve velké míře používány systémy PKI pro zajištění bezpečného ukládání šifrovacích klíčů. Zase zde platí totéž, co u předchozího bodu. Nejbezpečnější je řešení realizované podle veřejně známých mezinárodních norem.
- **Šifrovací algoritmy se používají jen pro speciální účely** - Aniž bychom si toho byli vědomi, kryptografické prostředky nás obklopují v každodenním životě. Využívají se například u mobilních telefonů GSM, pro kódování placených televizních kanálů, pro zabezpečení elektronické pošty apod. Stále více také pronikají do světa našich počítačových sítí, kde nám pomáhají zajistit cenná data před jejich vyzrazením či nelegálním pozměnění.

SVĚT SE TOČÍ KOLEM ELEKTRONICKÉHO PODPISU

Jedním z nejdůležitějších nástrojů, kolem nichž se (obrazně řečeno) bude v příštích letech "točit" kybernetický svět, je bezesporu elektronický podpis.

Co je to tedy elektronický podpis? Je to prostředek k zajištění elektronické autentizace autora (podepisovatele) a integrity podepisovaných dat. Význam digitálního podpisu roste přímo úměrně s významem komunikací prostřednictvím elektronických médií.

Jedná se o aplikaci schopnou s mnohem vyšší mírou důvěryhodnosti než běžný rukou psaný podpis potvrdit nějakou skutečnost. Přitom použití elektronického podpisu je mnohem širší, než si vůbec dokážeme představit - mimo oblíbených příkladů s podáváním daňových přiznání po Internetu bude možné elektronicky podepisovat např. kusy programového kódu, a tak nepopiratelně prokazovat jejich autorství. Elektronický podpis je též nesmírně silnou zbraní v boji proti počítačovým virům (především proti

tzv. červům, které se šíří pomocí e-mailové pošty), neboť bude možné bezpečně rozlišit, který e-mail je skutečně od odesílatele a který je podvržen k tomu, aby "vypustil" škodlivý kód. A takto bychom mohli do nekonečna pokračovat, aniž bychom vyčerpali všechny možnosti, neboť časem se objeví další a další možnosti použití elektronického podpisu.

Jediný, kdo asi spláče nad výdělkem, budou sběratelé podpisů a autogramů slavných osobností... (Hluboký povzdech autora této publikace, který je "v civilu" vášnivým sběratelem podpisů astronautů a kosmonautů...)

ELEKTRONICKÝ PODPIS V KOSTCE

Elektronický podpis je v oblasti digitálních dat tímtéž, čím je běžný podpis v "normálním" životě. Zatímco o účelnosti a smysluplnosti "ručního" podpisu nepochybuje snad nikdo (slouží k podložení nejrůznějších úkonů jako ověření, stvrzení apod.), s jeho mladším elektronickým bratříčkem je to horší.

Nejprve si uvědomme, k čemu všemu vlastně podpis v běžném životě slouží (byť je jeho váha mnohdy zlehčována - viz žádost "sem se mi podepište" a nikoliv "podívejte se na to a, pokud s tím souhlasíte, podepište"). Podpis

- poskytuje důkaz, že se podepsaná osoba cítí být obsahem dokumentu vázána,
- potvrzuje autorství textu dokumentu,
- potvrzuje svůj úmysl ztotožnit se s obsahem dokumentu, který sestavil někdo jiný,
- prokazuje skutečnost, že tato osoba byla přítomna na stanoveném místě.

S podobnou autentizací u elektronických dokumentů je to horší. Jak chcete podepsat dokument napsaný v textovém editoru? Pokud tam vepíšete pouze své jméno, nezůstává materiál sice anonymní, ale přece jen - zfalšovat podpis může absolutně každý. Proto je zapotřebí si pod pojmem

"elektronický (resp. digitální) podpis" představit něco jiného. (Pro úplnost dalšího výkladu: Každý elektronický dokument napsaný pomocí libovolného textového editoru si lze jednoduše představit jako datový soubor.)

V podstatě se jedná o implementaci určité matematické funkce prostřednictvím specializovaného programu, jejímž připojením k určitému dokumentu dochází k ověření jeho pravosti.

Jinými slovy: Elektronické podepisování zprávy probíhá tak, že se pomocí jednocestné funkce (hash funkce) vytvoří tzv. otisk zprávy, který je zašifrován soukromým klíčem a přidán k této zprávě. Příjemce dešifruje získaný zašifrovaný otisk veřejným klíčem (obsaženým v certifikátu) a opět za pomoci hash funkce vygeneruje ze zprávy nebo datového souboru nový otisk, přičemž oba porovná a pouze v případě, že jsou totožné, je zřejmé, že nedošlo k žádným úpravám zasílaných informací a odesilatel byl identifikován a ověřen.

Ověření pravosti tohoto podpisu se děje obdobným způsobem. Elektronický podpis je příslušným počítačovým programem ověřen v případě, že kontrolní výpočty souhlasí při jejich porovnání s původními hodnotami. Pokud k této kontrole nedojde, znamená to, že "někdo" (a může to být třeba i odesílatel zprávy) data modifikoval či do nich jakkoliv zasahoval - elektronický podpis v takovémto případě pozbývá platnosti.

V praxi to představuje například přijetí elektronicky podepsané e-mailové zprávy. Ještě před tím, než si ji přečte příjemce, se k jejímu obsahu dostane osoba se zlými úmysly a pokusí se příjemce (i odesílatele) poškodit provedením změn v e-mailu (přidání souborů, změna údajů apod.). Při ověřování elektronického podpisu však dojde k tomu, že příslušný software jej neověří - a to příjemce varuje, že v e-mailu došlo k zásahům, s nimiž se odesílatel neztotožňuje. (Pozor - nežádoucí osoba se k e-mailové zprávě může dostat nejen přímo fyzicky u počítače příjemce, ale v podstatě kdekoliv na cestě - na serveru, u poskytovatele připojení, přes nějž zpráva jde atd.)

V praktickém životě jsou elektronické podpisy nasazovány převážně ve spojitosti s e-mailovou poštou. Takovéto systémy jsou často realizovány jako plug-in (zásuvné moduly) do oblíbených e-mailových programů. Jedině takto lze dosáhnout kýženého cíle - maximálně zjednodušit zabezpečení a podpis zpráv pro koncové uživatele. Aby nebylo možné zneužít takto "vestavěného" elektronického podpisu, bývá obvykle vyžadováno ještě před samotným použitím soukromého klíče heslo. Toto heslo může být volitelně zadáváno buď z klávesnice nebo prostřednictvím čipových karet či jiných autentizačních předmětů. Pak již nic nebrání tomu, aby byla zpráva zašifrována a elektronicky podepsána, a to nejlépe včetně všech připojených souborů. Jedná se tak i o jistý způsob antivirové ochrany - mnoho počítačových virů se připojuje k e-mailové zprávě bez vědomí odesílatele a příjemce věřící dané osobě je pak bezelstně spustí. Dojde-li k připojení viru až po provedení elektronického podpisu, je ohrožená osoba varována, že něco není v pořádku.

Ale bylo by špatné si myslet, že podpisů může být využíváno pouze u elektronické pošty. (Připomeňme, že základní komunikační protokol sítě

Internet - TCP/IP je otevřený a sám o sobě nepočítá s jakoukoli bezpečností.) V praxi se například používá podepisování souborů stahovaných pomocí FTP - protože jedině tak můžete mít jistotu, že soubory pocházejí skutečně od toho, od koho čekáte. Představte si například možné škody způsobené tím, že si z Internetu stáhnete neautorizovanou verzi svého oblíbeného programu, která ale ve skutečnosti nebude pocházet od výrobce, ale od někoho úplně jiného. Automaticky a dobrovolně si takto nainstalujete na váš počítač software, o kterém nic nevíte a který může způsobit naprosto fatální škody v celém systému. A přitom je řešení tak jednoduché - stačí jen registrovaným uživatelům poskytnout nové verze software opatřené elektronickým podpisem. Ten zajistí, že po ověření podpisu můžete mít jistotu, že program pochází skutečně od našeho správného dodavatele.

Ale to stále ještě není všechno. V poslední době se používá elektronických podpisů například také pro podepisování částí programového kódu. Výrobci software se takto chrání před porušováním autorského zákona - ve kterém je napsáno, že nikdo mimo autora nemá právo jakkoli zasahovat do jeho díla. Program takto snadno a bezpečně vyhodnotí, zda například dll knihovna, jejíž funkci právě hodlá zavolat, skutečně pochází od autorizovaného výrobce.

Podtrženo, sečteno: Elektronický podpis je metodou pro bezpečnou komunikaci, jejíž pomocí zjišťujeme, zda se zprávou či datovým souborem nebylo nijak manipulováno a zda byla zajištěna integrita. Ve spojení s certifikátem elektronický podpis potvrzuje, že se jedná o zprávu skutečně z předpokládaného zdroje.

PROČ POTŘEBUJEME ELEKTRONICKÝ PODPIS?

Elektronický podpis má oproti klasickému podpisu několik zásadních výhod. Pokusme se shrnout alespoň některé z nich:

- Na rozdíl od klasického podpisu je prakticky nemožné jej zfalšovat. Díky využití nejmodernějších algoritmů pro zabezpečení elektronického

podpisu je čas potřebný na zfalšování řádově 1,6x1018 MIPS za rok (tj. pokud by bylo použito deseti tisíc PC s výpočetním výkonem 1000 MIPS (Million Instruction Per Second), trval by výpočet 1011 let - což je více než doba existence našeho vesmíru...)

- Nespornou výhodou je také poměrně jednoduché ověření pravosti podpisu - při každém ověřování podpisu je možné dojít k jednoznačnému a správnému rozhodnutí, zda je podpis platný, či ne. Připomeňme, že pro ověřování klasického podpisu (například v bance) je nutný podpisový vzor, a uvědomme si, jak reálná je možnost přehlédnutí některých detailních rozdílů porovnávaných podpisů.
- Je zaručena neporušenost zprávy. Díky této vlastnosti můžeme snadno ověřit, jestli obsah zprávy je stejný s obsahem v době podpisu. Tato vlastnost je nazývána "ověřování integrity zprávy".
- V kombinaci se šifrováním zpráv lze navíc dosáhnout efektu, díky kterému je možné ověření podpisu provést až po úspěšném rozšifrování zprávy - tj. zpráva je účinně chráněna před vyzrazením jejího obsahu.
- Poslední vlastností elektronického podpisu je "nepopiratelnost". V praxi to znamená, že není možné podepsat "prázdný papír", jehož obsah bude doplněn později. Díky této vlastnosti podepsaná osoba nemůže popřít, že nebyla seznámena s obsahem dané zprávy a že ji neodeslala ona.

ELEKTRONICKÝ PODPIS VERSUS DIGITÁLNÍ

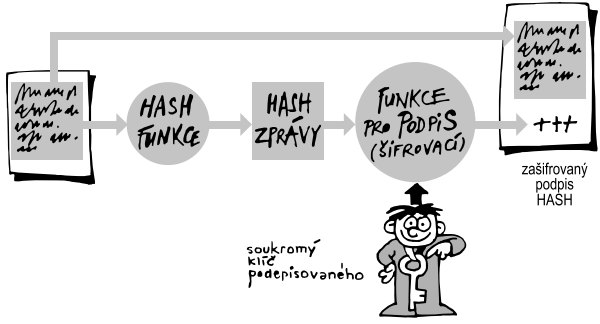
V souvislosti s elektronickou autentizací se většinou objevuje termín "elektronický", ovšem někdy také "digitální" podpis. Zákonitě v této souvislosti vyvstává otázka: Jaký je rozdíl mezi digitálním a elektronickým podpisem? Elektronický podpis je poněkud širší termín, zahrnuje mimo výše uvedených případů také např. biometrické prokazování totožnosti (pomocí otisku prstu, snímáním oční rohovky...) či jiné prokázání totožnosti (čipovou kartou...). Digitální podpis je pak speciálním případem elektronického, kdy dochází k ověření původu dokumentu na bázi šifrování.

JAK FUNGUJE ELEKTRONICKÝ PODPIS?

Byť v předchozí pasáži byl princip elektronického podpisu v náznacích podán, zvídavému čtenáři je jasné, že takto jednoduché to v praxi nebude. Ano, je to tak, a proto se na princip fungování elektronického podpisu podívejme podrobněji.

Nejprve si objasněme pojem "hash", který se objevil již v předchozím textu. Hash funkce je matematická funkce, kterou lze v jednom směru (přímém) snadno spočítat, zatímco v opačném směru (inverzní zobrazení) probíhají výpočty velmi obtížně. Výsledkem hash funkce je 128 nebo 160 bitů dlouhá sekvence jednoznačně charakterizující vstupní blok dat. V případě elektronického podpisu je pro hash funkci vstupní informací podepisovaný dokument. Z celé řady jeho typických znaků je poté spočítán hash.

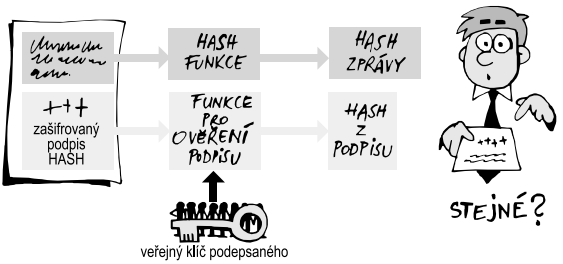
A nyní si opět na pomoc vezmeme ilustrační obrázek.



Na počátku elektronického podpisu jsou vždy nějaká data v elektronické podobě, která chceme podepsat. Za pomoci hash funkce vypočítáme hash zprávy. V tu chvíli vstupuje do hry soukromý klíč podepisovaného člověka. Speciální počítačový program připojí k datům "podpis" na základě hashe a soukromého klíče. Tento "podpis" tak zaručuje, že dokument podepsal

vlastník soukromého klíče a že s podepsanými daty nebylo manipulováno, což je nesmírně důležité! Z toho totiž plynou všechny další vlastnosti elektronického podpisu jako nepopiratelnost apod.

Obdobným procesem probíhá i ověření elektronického podpisu na straně příjemce. Nestačí se totiž pouze spokojit s konstatováním, že data jsou elektronicky podepsána, je nutné ověřit, zdali je podpis platný a zdali do přijaté zprávy nebylo zasahováno (třeba někde cestou, nebo ještě dodatečně po podepsání).



Speciální počítačový program si informace rozdělí na dvě části. Jednak je to podepsaná datová část a jednak vlastní elektronický podpis. Postupně spočítá hash zprávy. Posléze si spočítá hash z elektronického podpisu, přičemž využije veřejného (a tudíž všeobecně známého) klíče podepsaného. Následuje porovnání obou hashů: Datového i podpisového. Pokud jsou stejné, je vše v pořádku a zpráva byla skutečně podepsána taková, jaká je. Pokud je ovšem nalezena byť jen drobná neshoda, něco není v pořádku a uživatel je neprodleně upozorněn na neplatnost elektronického podpisu! Nezáleží přitom na tom, kde, kdo a jak zprávu modifikoval - skutečností zůstává pouze fakt, že elektronický podpis není platný.

ZÁKON O ELEKTRONICKÉM PODPISU

Vzhledem k tomu, že přípravu a schvalování Zákona o elektronickém podpisu (platit by měl začít k 1. říjnu 2000) byla nesmírně náročná, podívejme se na něj trochu podrobněji - už proto, že bude ovlivňovat spoustu oblastí našeho života po dlouhou dobu a zásadním způsobem.

Nejprve se soustřeďme na mezinárodní arénu, kde je situace s bezpečností dat a elektronickým podpisem bouřlivě diskutována (téměř stejně bouřlivě jako v naší republice). Základní příčinou rozvoje legislativy, norem a doporučení v mezinárodním měřítku je snaha o akceleraci vývoje elektronického obchodu. Je lépe vnímat pojem elektronický obchod jako e-všechno, protože vyjmenování jednotlivých e-služeb je stále zdlouhavější a jejich seznam stále roste. Elektronický obchod, jehož kolečka jsou dobře mazána světovým kapitálem, je hlavní příčina bouřlivého technologického rozvoje v oblasti bezpečnosti informačních technologií, z nichž je elektronický podpis a šifrování dat jen jednou součástí. Je však třeba přiznat, že nosnou.

Na jedné straně existuje ve světe široce uznávaný soubor pravidel známý pod jménem UNCITRAL Model Law on Electronic Commerce (přijatý v roce 1996), který nabízí množinu mezinárodně uznávaných předpisů, jak začít budovat platné systémy použití informací v datové formě.

Na druhé straně však existuje i jiný model, který poskytuje vysoký stupeň vládní regulace těchto služeb. Poskytuje vládě možnost protěžovat jednu či více forem elektronického podepisování, a to definováním speciálních technických požadavků. Jde o direktivu European Union's Electronic Signatures Directive schválenou v roce 1999. A právě o tuto direktivu se také opírá (resp. pokouší opírat) náš zákon.

Je zajímavé, že již při schvalování zákona se spekulovalo s perspektivou řady prováděcích vyhlášek a novelizací! Zákon totiž nerespektuje základní požadavky zmíněné EU Direktivy, a to především v otázce státní regulace. Stejně jako v období komunistické vlády budeme v tomto případě státně zcela regulováni a posléze (ve chvíli, kdy to nebude fungovat) zahrnuti výjimkami (pro výjimečné?).

Jeden příklad za všechny, formulace paragrafu 11 příslušného zákona: "V oblasti veřejné moci je možné používat pouze zaručené elektronické podpisy a kvalifikované certifikáty, vydávané **akreditovanými** poskytovateli certifikačních služeb." V kombinaci se zněním § 6.1.j: "Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty je povinen používat **bezpečné systémy a nástroje** elektronického podpisu a zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují. Nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou."

Právě tyto formulace bohužel znamenají, že jeho využitelnost v oblasti "veřejné moci" (podávání daňových přiznání apod.), se odsouvá daleko do vzdálené budoucnosti. V dohledné době lze totiž zajistit pouze to, aby v praxi fungovali běžní poskytovatelé certifikačních služeb. Poskytovatelé certifikačních služeb vydávající kvalifikované certifikáty si budou muset

POČKAT na zákonem vyžadované a vyhláškami definované "bezpečné systémy a nástroje elektronického podpisu"...

Na použití elektronického podpisu ve vztahu ke státním institucím si tak budeme muset ještě nějaký ten pátek počkat. To ale v žádném případě nebrání možnosti používat elektronický podpis mimo státní sféru - namátkou jmenujme bankovnictví, obchod na Internetu či bezpečnou komunikaci elektronickou poštou.

P.S. Pokud vás zajímají další podrobnosti o historii vývoje Zákona o elektronickém podpisu, můžete navštívit webovské stránky **www.trustcert.cz**.

CERTIFIKÁTY

V předchozích pasážích jsme se seznámili především s použitím asymetrických šifrovacích algoritmů a také s problematikou elektronického podpisu. S tímto ovšem souvisí jeden obrovský problém, a tím je záruka, že nabízený veřejný klíč, kterým dojde k zašifrování informací, skutečně náleží osobě, jíž jsou informace a data určena.

Jakákoliv záměna klíčů (nechtěná či záměrná) by způsobila, že data by nemohl číst skutečný příjemce zprávy, ale majitel příslušného soukromého klíče. V případě zlého úmyslu by tak vlastně docházelo k tomu, že budeme důležitá data šifrovat tak, aby je mohl rozšifrovat pouze útočník, který klíč zaměnil!

Aby k takovéto situaci nemohlo dojít, vznikají certifikační autority. To jsou (obrazně řečeno) notářství na počítačových sítích, která vydávají doklad o vazbě mezi totožností uživatele a jeho veřejným klíčem. Tento doklad se nazývá certifikátem.

Certifikační autority fungují (zjednodušeně řečeno) tak, že svým soukromým klíčem podepisují žadatelův veřejný klíč a údaje o jeho vlastníkovi, a svým vlastním podpisem zaručují, že jeho majitelem je skutečně ten, kdo je v popisu klíče uveden. Certifikát tak pomáhá zabránit podvržení

klíče s cílem vydávat se za někoho jiného (většinou za stranu, které případný příjemce důvěřuje).

Ve své nejjednodušší podobě obsahuje certifikát veřejný klíč a jméno majitele klíče. Obecně používané certifikáty obsahují rovněž:

- dobu vypršení platnosti (podobně jako např. bankovní karta je certifikát platný pouze "od-do");
- jméno certifikační autority, která vydala certifikát (to je důležité až nezbytné z hlediska důvěryhodnosti certifikátu);
- pořadové číslo (důležité pro evidenci certifikátu);
- digitální podpis vydavatele certifikátu (vlastně nejdůležitější část certifikátu, neboť jen díky ní certifikační autorita ručí za to, že certifikát je v pořádku).

Díky použití certifikátů se řetězec důvěry/nedůvěry redukuje na důvěru/nedůvěru v jednu jedinou instituci - certifikační autoritu. Certifikační autorita si důvěru zasluhuje tím, že provádí svou činnost otevřeně, nabízí k nahlédnutí certifikační politiku (pravidla, podle kterých se certifikáty vydávají), svoje prováděcí pravidla a CPS - Certificate Practice Statement (tj. pravidla, jak se certifikáty vydávají).

Certifikáty nesmí být možné padělat, musí být získány bezpečnou cestou a musí být vytvářeny tak, aby je potenciální narušitel nemohl zneužít. Vydání certifikátu musí rovněž probíhat bezpečným způsobem a musí být odolné proti všem možným útokům.

Nejrozšířenějším akceptovaným formátem pro certifikáty je formát definovaný mezinárodní normou CCITT X.509 v.3. Tyto certifikáty pak mohou být čteny či psány libovolnou aplikací vytvořenou ve shodě s X.509. Normu X.509 využívá řada protokolu, např. PEM, PKCS, S-HTTP a SSL.

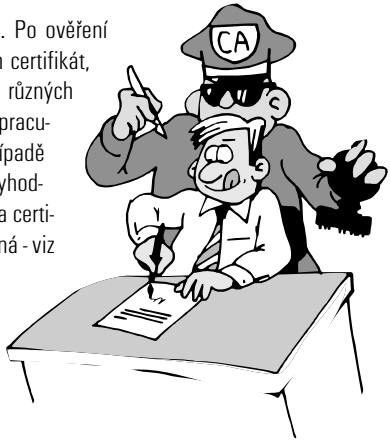
ODVOLÁVÁNÍ CERTIFIKÁTŮ

Certifikační autorita (viz níže) vydává svým klientům certifikáty s určitou platností a po jejím vypršení může certifikáty obnovit. V praxi však může dojít například k vyzrazení soukromého klíče uživatele. Pokud se útočník dostane k vašemu soukromému klíči, může za vás podepisovat poštu a co je horší, může například v elektronickém obchodě podepisovat příkazy k úhradě z vašeho konta... Je to situace podobná ztrátě kreditní karty a vyzrazení kódu PIN. Proto při podezření na vyzrazení soukromého klíče můžete požádat certifikační autoritu o zneplatnění certifikátu (což odpovídá bankovní operaci zablokování karty). Autorita poté odvolaný certifikát zařadí do seznamu neplatných certifikátů a nebude dále potvrzovat vaši autenticitu (spojení uživatele s tímto klíčem). Povinností každého, kdo si ověřuje certifikát, je totiž zkontrolovat, zdali nefiguruje u certifikační autority na seznamu odvolaných certifikátů. Pokud je certifikát uveden v seznamu odvolaných certifikátů, certifikační autorita nemá zodpovědnost za jakékoliv škody způsobené akceptováním tohoto neplatného certifikátu.

SEZNAMTE SE: CERTIFIKAČNÍ AUTORITA

Certifikační autorita obecně je důvěryhodná třetí strana, která spojuje veřejný klíč s uživatelem a ověřuje jeho totožnost (autenticitu). V podstatě jde o instituci používající svůj vlastní klíčový pár (soukromý a veřejný) pro potvrzování totožnosti ostatních uživatelů.

Jak? Veřejné klíče uživatelů jsou jednoduše digitálně podepsány certifikační autoritou. A co je třeba udělat, aby se z vašeho klíče stal certifikát, podepsaný některou známou certifikační autoritou? Obvykle je nejprve třeba vyplnit formuláře s požadavkem na vystavení certifikátu a připojit k nim svůj veřejný klíč. Formuláře i prostředek pro zaslání klíče obvykle naleznete přímo na WWW stránce příslušné autority. Poté jste certifikační autoritou vyzváni k osobní návštěvě některé z jejích kanceláří (registrační



autority) s dokladem totožnosti. Po ověření vaší totožnosti vám bude zaslán certifikát, a to obvykle hned v několika různých formátech pro různé programy pracující podle různých norem. (V případě žádostí o certifikáty nižší důvěryhodnosti někdy není osobní návštěva certifikační či registrační autority nutná - viz níže pasáž Třídy certifikátů.)

Pokud poté obdržíte elektronickou poštou zprávu, která je podepsaná uživatelem, je u ní přiložen i certifikát. Pokud je podpis platný, můžete si ověřit i platnost certifikátu dotazem u příslušné certifikační auto-rity v tzv. seznamu odvolaných certifikátů (Revocation List).

Certifikační autoritu tedy tvoří nejenom program pro podepisování veřejných klíčů žadatelů a databázový server (v něm jsou všechny platné i již neplatné certifikáty uloženy), ale hlavně certifikační politika. Jedná se o soubor pravidel, podle kterých se certifikáty vydávají - tj. autorita může například vydávat certifikáty několika úrovní podle jejich důvěryhodnosti:

- Certifikát podepsaný certifikační autoritou bez ověření totožnosti - nejméně důvěryhodný certifikát. Žádost je obvykle vystavena na WWW stránkách a certifikát je odeslán zpět bez osobní návštěvy. Tyto certifikáty v podstatě neposkytují žádné záruky totožnosti uživatele a slouží pouze k vyzkoušení. Tato skutečnost bývá na certifikátu zdůrazněna. Podobné funkce nabízejí i některé placené autority, kterým ale stačí zaslat fotokopii pasu nebo občanského průkazu například faxem a zaplatit příslušný poplatek. Takto vydané certifikáty mají pouze velmi omezenou důvěryhodnost.

- Důvěryhodný certifikát podepsaný certifikační autoritou. Tato služba je obvykle placená. Pro vystavení certifikátu je nutná osobní návštěva v některé z kanceláří autority. Uživatel zde po zaslání příslušných formulářů obdrží plnohodnotný certifikát. Platnost certifikátu je podobně jako platnost jakéhokoliv osobního dokladu (pas, občanský průkaz apod.) časově omezena. Těsně před vypršením platnosti je možné požádat certifikační autoritu o obnovení certifikátu. Pro vyřízení této žádosti již však obvykle není nezbytně nutná osobní návštěva. Stačí jen zaslat digitálně podepsaný formulář s příslušnou žádostí. Certifikáty tohoto typu jsou vyžadovány například u aplikací elektronického obchodu, kde jednotlivé objednávky a příkazy pro samotné platby musejí být podepsány uživatelem, který vlastní platný certifikát a jehož totožnost je možné ověřit u příslušné certifikační autority.

V praxi se vytváří celé sítě certifikačních autorit, které mohou mít různou strukturu a v závislosti na ní pak různý stupeň důvěryhodnosti. Jedna certifikační autorita pak může ověřovat důvěryhodnost autority druhé, a tím zajistit akceptování daných certifikátů. Toho je využíváno hlavně u e-commerce aplikací (elektronický obchod), kde obchod díky Internetu nezná hranic.

DŮVĚRYHODNOST CERTIFIKAČNÍ AUTORITY

Certifikační autorita a její důvěryhodnost jsou základními aspekty, které jsou spojené s bezpečnou komunikací. Někdo její význam přeceňuje, někdo jiný zlehčuje... Častým argumentem je také, že při komunikaci se stranou, kterou důvěrně znám, žádné certifikáty nepotřebuji. Proti takové argumentaci se nedá nic namítnout, hovoříme-li ovšem o velmi úzké skupině účastníků. Ovšem těžko si představit třeba elektronický obchod, který by obcházel své zákazníky a osobně se s nimi seznamoval... (Když už nic jiného, tak se jedná o popření principu elektronického obchodování.)

Samozřejmě, že i v rámci kanceláře lze šifrovanou poštu používat, ale mnohem zásadnější je, že lze prostřednictvím Internetu komunikovat prakticky s kýmkoliv kdekoliv. Díky službám certifikačních autorit si totiž mohu být jistý, s kým komunikuji. V okamžiku, kdy např. něco po Internetu prodávám nebo nakupuji, takovouto jistotu ocením. V případě, že vzniknou přes dodržení všech předepsaných pravidel potíže s identitou osoby prokazující se certifikátem, je možné se "hojit" na certifikační autoritě, která by měla být pro podobné případy pojištěná.

Důvěryhodnost certifikační autority je pro bezpečnou komunikaci za pomoci certifikátů jedním z nejdůležitějších faktorů. Důvěryhodnost obdrženého certifikátu totiž nevychází jen z třídy, kterou se vyznačuje (viz níže), ale především z důvěryhodnosti autority, která za jejím vydáním stojí. V praxi se pak vytvářejí celé sítě vzájemně propojených autorit, které navzájem potvrzují svoji důvěryhodnost (křížová certifikace), popřípadě potvrzují důvěryhodnost svých podřízených certifikačních autorit. Aby některá z důvěryhodných certifikačních autorit podepsala certifikát autority jiné, musí tato autorita splnit jisté (a to velmi přísné) požadavky, jako je například bezpečnostní audit nebo pojištění.

Je pochopitelné, že se za takový podpis platí, a to stejně tak jako za později vydané certifikáty.

Certifikační autorita, která je z hlediska bezpečnosti považována za důvěryhodnou, není vázána na místo, ze kterého provádí svoje operace. Většina certifikačních autorit totiž provádí své operace celosvětově. Z hlediska smyslu internetové komunikace je to pochopitelné a důvěra, vyjádřená certifikační autoritě celosvětově, je do jisté míry i vyšší než důvěra "místní". To se samozřejmě týká globální komunikace. V praxi se totiž ustanovují (například v rámci prostředí bank nebo jiných institucí) pouze lokální certifikační autority, které si však do značné míry mohou "hrát" podle vlastních pravidel, přičemž to většinou dělají.

REGISTRAČNÍ AUTORITY

V souvislosti s certifikačními autoritami byl zmíněn také pojem "registrační autority". Jedná se o důvěryhodné subjekty, které jsou zřizovány pro provádění činností potřebných pro správnou činnost certifikační autority. Registrační autorita je autorizovaná ke sběru a ověřování informací o identitě uživatelů žádajících o certifikát a k určování informací, které je možné certifikační autoritou vložit do vytvářených certifikátů. Registrační autorita je v daný časový okamžik zásadně podřízena jediné certifikační autoritě. Hlavní úlohou registrační autority je přiblížit služby vydávání certifikátů zákazníkům - vzhledem k poměrně přísným podmínkám spojeným s provozování certifikační autority (mj. fyzické zabezpečení objektu), je jednodušší pro sběr údajů a informací vytvořit síť registračních autorit.

TŘÍDY CERTIFIKÁTŮ

V několika předchozích pasážích jsme slibovali objasnění pojmu "třídy certifikátů". Je celkem logické, že existuje několik kategorií certifikátů - od těch s menší váhou až po ty s vyšším stupněm důvěryhodnosti.

Některé certifikační autority omezují svou působnost pouze na jednu třídu certifikátů. Jiné zase rozdělují důvěryhodnost do detailnějšího dělení. Ovšem mezinárodně uznávaný způsob dělení je popsaný níže. Certifikáty jsou děleny do jednotlivých tříd (Class):

- **Class 1 Trial**: Tato úroveň je vydávána pouze pro testovací účely, přičemž certifikáty jsou platné pouze po limitovanou dobu. Certifikační autorita nedrží žádnou záruku za používání těchto certifikátů. Jejich použití a údaje v nich uvedené jsou plně na zodpovědnosti žadatele. Certifikáty jsou bezplatné.
- **Class 1**: Tato úroveň je užívána pro aplikace, které zpracovávají informace poměrně nízké hodnoty v prostředích, které se vyznačují nízkou úrovní rizika. Certifikáty této úrovně nezajišťují podrobnosti o svém

ELEKTRONICKÝ PODPIS VERSUS DIGITÁLNÍ

V souvislosti s elektronickou autentizací se většinou objevuje termín "elektronický", ovšem někdy také "digitální" podpis. Zákonitě v této souvislosti vyvstává otázka: Jaký je rozdíl mezi digitálním a elektronickým podpisem? Elektronický podpis je poněkud širší termín, zahrnuje mimo výše uvedených případů také např. biometrické prokazování totožnosti (pomocí otisku prstu, snímáním oční rohovky...) či jiné prokázání totožnosti (čipovou kartou...). Digitální podpis je pak speciálním případem elektronického, kdy dochází k ověření původu dokumentu na bázi šifrování.

JAK FUNGUJE ELEKTRONICKÝ PODPIS?

Byť v předchozí pasáži byl princip elektronického podpisu v náznacích podán, zvídavému čtenáři je jasné, že takto jednoduché to v praxi nebude. Ano, je to tak, a proto se na princip fungování elektronického podpisu podívejme podrobněji.

Nejprve si objasněme pojem "hash", který se objevil již v předchozím textu. Hash funkce je matematická funkce, kterou lze v jednom směru (přímém) snadno spočítat, zatímco v opačném směru (inverzní zobrazení) probíhají výpočty velmi obtížně. Výsledkem hash funkce je 128 nebo 160 bitů dlouhá sekvence jednoznačně charakterizující vstupní blok dat. V případě elektronického podpisu je pro hash funkci vstupní informací podepisovaný dokument. Z celé řady jeho typických znaků je poté spočítán hash.

A nyní si opět na pomoc vezmeme ilustrační obrázek.

Na počátku elektronického podpisu jsou vždy nějaká data v elektronické podobě, která chceme podepsat. Za pomoci hash funkce vypočítáme hash zprávy. V tu chvíli vstupuje do hry soukromý klíč podepisovaného člověka. Speciální počítačový program připojí k datům "podpis" na základě hashe a soukromého klíče. Tento "podpis" tak zaručuje, že dokument podepsal vlastník soukromého klíče a že s podepsanými daty nebylo manipulováno,

zaci jednat a podepisovat se, jejíž jméno je uvedeno v certifikátu, a která se také identifikuje vůči registrační autoritě. Je možno jej použít pro bezpečný elektronický obchod, pozitivní identifikaci jeho uživatele, k bankovním transakcím a podobně.

- **Osobní - Class 3** certifikát poskytuje potvrzení identity osoby pomocí její fyzické přítomnosti v kanceláři registrační autority. Jiný typ certifikátu je certifikát vydaný pro osobní identifikaci úředníka registrační autority a slouží pouze za uvedeným účelem.

- **Pro organizaci - Class 3** certifikáty mohou provádět identifikaci různých veřejných nebo soukromých organizací.

- **Class 4**: Tato úroveň je vyžadována pro aplikace, které zpracovávají informace střední hodnoty v prostředí s vysokou úrovní rizika. Certifikáty vydané v této třídě poskytují nejvyšší možné ověření identity jejich vlast-

níka. Při vydávání certifikátu je třeba, aby se budoucí vlastník dostavil na registrační autoritu a předložil požadované dokumenty, u nichž mohou být vyžadovány další vlastnosti (minimální zbývající délka platnosti apod.). Je požadováno předložení rodného listu. Příslušné klíče jsou uchovávány v hardwarových zařízeních.

- **Class 5**: Tato úroveň se stanovuje pro aplikace, které zpracovávají informace vysoké hodnoty v prostředích, které se vyznačují vysokou mírou rizika. Požadavky na identifikaci jsou stejné, jako u Class 4. Dalším požadavkem je ovšem použití hardwarových modulů pro provádění kryptografických operací.

Většina bezpečnostních programů umožňuje také vytváření Self Signed Certificate - jedná se o certifikát, který je podepsaný sebou samým. Veřejný klíč a připojené informace nejsou podepsány žádnou z certifikačních autorit, ale pouze uživatelem samým. Význam takovéhoto podpisu spočívá pouze v kontrole integrity samotného certifikátu. Důvěryhodnost takovéhoto certifikátu, pokud jeho uživatele neznáte a nejste schopni jeho totožnost ověřit osobně, je nulová.

Certifikáty dle jednotlivých tříd:

třída certifikátu	rizikovost prostředí	hodnota informací	použití HW modulů
CLASS 1	nízká	nízká	ne
CLASS 2	Nízká	střední	ne
CLASS 3	Nízká	vysoká	ne
	Střední	střední	
CLASS 4	Střední	vysoká	ano - pouze uchování klíčů
CLASS 5	Vysoká	vysoká	ano - provádění kryptografických operací

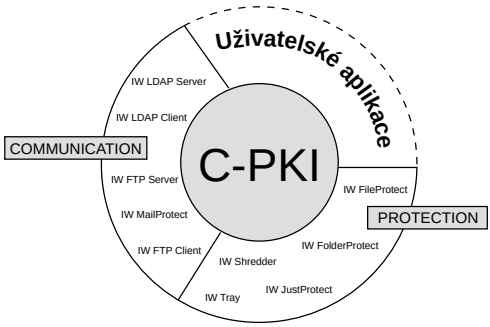
SMLOUVA O UŽÍVÁNÍ JEDNOTLIVÝCH CERTIFIKÁTŮ

V celém procesu užívání, odvolávání a generování digitálních certifikátů hraje právě smlouva o jejich užívání podstatnou roli. Je to totiž právě tato smlouva, která ozřejmuje práva a povinnosti uživatele a certifikační autority v detailnější formě. Generování digitálních certifikátů a možnost jejich následného používání je totiž službou, kterou poskytuje certifikační autorita uživateli, který za ni platí. V okamžiku žádosti o vydání digitálního certifikátu a jejího přijetí certifikační autoritou tak vstupují obě strany (uživatel a certifikační autorita) do smluvního vztahu, který se musí řídit jistými pravidly. Ve smlouvě o užívání certifikátu tak nejsou jen informace, kolik uživatel za danou službu zaplatí, ale také informace o době platnosti smluvního vztahu a přesně definovaná pravidla pro použití certifikátu. Certifikační autorita nemůže nést odpovědnost za škody způsobené užitím certifikátu za jiným účelem, než za kterým byl vydán. Ve smluvním vztahu jsou rovněž definována pravidla pro způsob uložení soukromého klíče, neboť právě toto uložení má na důvěryhodnost certifikátu a bezpečnost dat, chráněných takovým certifikátem, zásadní vliv.

BEZPEČNOSTNÍ ŘEŠENÍ IRONWARE® SECURITY SUITE

Šifrujte! Používejte elektronický podpis! Blokujte přístup k citlivým datům nepovolaným osobám! Takováto a desítky dalších doporučení slyšíme dnes a denně. Zcela logicky ovšem zákonitě s nimi vyvstává otázka: Jak na to? V současné době je k dispozici velice široká paleta programů nabízejících na vyšší či nižší úrovni možnost zabezpečit data a informace. Ke světové špičce patří původní český bezpečnostní software IronWare® Security Suite, který vyvíjí firma AEC, spol. s r.o. **(www.aec.cz)**.

IronWare® Security Suite (dále jen IronWare® či IW) je modulární systém - to znamená, že se skládá z několika částí na sobě více či méně nezávislých. Pro svou činnost využívá silné a ověřené algoritmy, jejichž spolehlivost je prokázána světovou komunitou expertů v oblasti kryptologie. Nevyužívá tedy žádná nedostatečně prověřená vlastní řešení, která mohou obsahovat některé nedostatky či dokonce nebezpečné vlastnosti umožňující vyzrazení chráněného obsahu.



IronWare® je založen na PKI, což je zkratka z anglického Public Key Infrastructure. Volně přeloženo to znamená "správa veřejných klíčů". Systém založený na PKI si tedy můžeme zjednodušeně představit jako databázi veřejných klíčů vybavenou řadou nástrojů pro jejich správu a používání.

IronWare® jde dokonce ještě o krok dále, neboť necentralizuje pouze správu samotných klíčů, ale komplexně celou správu uživatelských účtů. To ovšem neznamená, že aplikaci nelze nainstalovat samostatně - např. do jednoho jediného počítače nebo do notebooku, který je stále na cestách, a tudíž není trvale připojen k síti. Tímto způsobem se ovšem pozbývají některé výhody plynoucí z PKI.

PKI je svým způsobem "srdcem" systému IronWare®, jehož jednotlivé moduly (viz popis níže) se k tomuto "základu" připojují přes otevřené standardizované rozhraní. To mj. umožňuje připojit dle potřeby další bezpečnostní součásti k tomuto systému (ať již od jiného výrobce či dodatečně připravené dle potřeb konkrétního řešení) - pokud podporují toto standardizované rozhraní.

"Správa veřejných klíčů" (alias PKI) aplikovaná v IronWare® je vytvořena v souladu se světovými standardy, přičemž používá symetrické i asymetrické kryptografie. Databáze je uchovávána v šifrované formě, přičemž je použito symetrického algoritmu CAST s délkou klíče 128 bitů. Přístup do ní je možný pouze po zadání správného hesla či použití hardwarového identifikačního prostředku.

Součástí systému IronWare® jsou dvě základní oblasti - Protection a Communication. Zatímco první z nich slouží k ochraně dat a informací, druhá najde své uplatnění v oblasti bezpečného komunikování.

Protection se skládá mj. z následujících modulů:

- **IW FileProtect** (šifrování adresářů technologií on-line)
- **IW FolderProtect** (šifrování adresářů technologií off-line)
- **IW JustProtect** (šifrování souborů na vyžádání - např. do samorozbalovacích *.exe souborů)
- **IW Shredder** (elektronická skartovačka dat)

Communication se skládá z aplikací:

- **IW MailProtect** (ochrana elektronické pošty šifrováním)
- **IW FTP Client** (ochrana souborů posílaných pomocí FTP)
- **IW FTP Server** (ochrana souborů posílaných pomocí FTP)

Upozorňujeme, že na následujících řádcích není bezpečnostní řešení IronWare® popsáno do detailů a že zde nejsou představeny všechny jeho součásti ani všechny možnosti představených součástí. Je to dáno především rozsahem této publikace, která si přináší za cíl pouze základní seznámení s tímto řešením. V případě zájmu o podrobnější informace můžete navštívit **www.aec.cz**, stránky certifikační autority Trustcert **www.trustcert.cz** nebo kontaktovat přímo **AEC (Bayerova 30, Brno 60200, tel 05-41235466-7, fax 05-41235038, e-mail: info@aec.cz)**.

IW GINA - HLÍDACÍ PES V POČÍTAČI

IW Gina je modul sloužící pro přihlášení uživatele k centrální nebo lokální databázi. Slouží rovněž ke kontrole přístupu do systému IronWare® či do počítače vůbec.

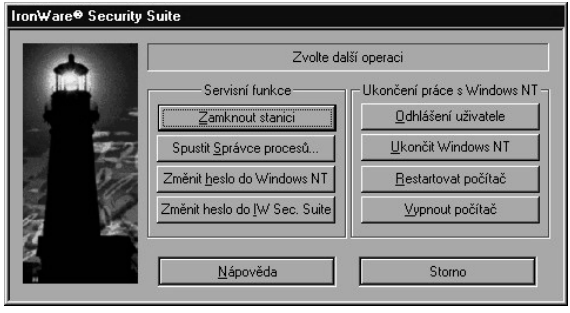
IW Gina po identifikaci uživatele (heslem nebo identifikačním předmětem - čipové karty, biometrická zařízení apod.) hledá, kde se nachází IW Management Server (viz níže), který obsahuje databázi klíčů a certifikátů.

Pokud se nepodaří IW Management Server zkontaktovat, lze se připojit k lokální databázi- z hesla či identifikačního předmětu je vyroben dešifrovací klíč, který odšifruje záznamy uživatele. Bez znalosti hesla či vlastnictví identifikačního klíče (ideální je ovšem kombinace obojího) se tak nepovolaná osoba do systému nedostane.

IronWare® zkontroluje již při prvotním stanovení hesla, zda splňuje podmínky minimální složitosti (tedy má-li minimálně sedm znaků, užívá-li kombinaci malých a velkých písmen a neabecedních znaků).

K připojení k IW Management Serveru dochází pomocí třícestné autentizace a heslo (jakožto citlivý údaj) NENÍ PO SÍTI POSÍLÁNO V OTEVŘENÉ FORMĚ!

Součástí IW Gina je rovněž funkce IW ScreenWall, která po krátkou dobu blokuje počítač. Už vás někdy napadlo, kdo všechno má k datům v počítači přístup po dobu, kdy jste na obědě nebo když prostě na pár minut vyslyšíte "volání přírody"? Jde o to, že je zbytečné na několik minut při opuštění pracoviště vypínat počítač - funkce IW ScreenWall po vyžádání uživatelem (např. po stisku příslušné kombinace kláves nebo po vyjmutí hardwarového identifikačního zařízení ze čtečky) spustí speciální "šetřič obrazovky". Ten poté blokuje přístup do počítače až do okamžiku opětovné identifikace oprávněným uživatelem.



IW KEYMANAGER - PRO SPRÁVU ŠIFROVACÍCH KLÍČŮ

IW KeyManager je modul, který má v "popisu práce" správu uživatelských práv, klíčů, certifikátů apod. V celém systému IronWare® se přitom mohou vyskytovat pouze tři typy uživatelů:

- **Běžný uživatel** - má běžná práva, která mu byla určena systémem a nad rámec těchto práv jeho možnosti nesahají. Některé z funkcí jsou mu tudíž nepřístupné a mimo to mu rovněž administrátor určí, do jaké "skupiny" uživatelů bude patřit a jaký stupeň důvěryhodnosti (viz níže) mu bude přidělen. Administrátor mu rovněž přiřadí skupinový klíč, nebo i více skupinových klíčů. Každý z uživatelů může měnit svoje heslo a plné jméno, stejně jako generovat a rušit svoje klíče (ale pouze svoje vlastní, nikoliv skupinové!).
- **Administrátor** - je uživatelem s nadstandardními právy. V systému může být i více administrátorů. Administrátor může vytvářet/rušit účty uživatelů, měnit jejich přístupová práva a důvěryhodnost, generovat skupinové klíče, předávat skupinové klíče (ke kterým má přístup) jiným administrátorům nebo uživatelům. Má přístup ke všem nastavením, nesmí však měnit log soubory (soubory se záznamy o vykonaných činnostech).
- **Auditor** - má z hlediska přístupu stejná práva jako běžný uživatel, v systému však vystupuje jako kontrolní autorita a z tohoto důvodu má možnost měnit log soubory.

O tom, který uživatel bude patřit do které kategorie, rozhoduje administrátor (kromě auditorů, které může vytvářet pouze auditor). Ten také jako jediný má práva provádět změny v jednotlivých účtech. Přitom platí, že každý uživatel se může vyskytovat pouze v jedné kategorii - auditor tak nemůže být zároveň administrátor apod.

Při vytváření účtu nového uživatele je zapotřebí stanovit, k jak citlivým datům bude mít přístup. Samozřejmě, že je možné toto nastavení dle potřeby měnit - ale pouze administrátorem. K dispozici jsou základní čtyři úrovně přístupu k datům:

- vyhrazeným (classified)
- důvěrným (confidential)
- tajným (secret)
- přísně tajným (top secret)

IW KeyManager také obsahuje možnost správy klíčů, přičemž správa umožňuje generování klíčů pro symetrickou kryptografii (tajné klíče), generování klíčů (resp. klíčových párů) pro asymetrickou kryptografii (soukromé a veřejné klíče), včetně generování certifikátů (self-signed, tedy certifikátů podepsaných sebou samým, tudíž s nejnižší možnou mírou důvěryhodnosti) nebo žádostí o certifikát, které mohou být poslány vybrané certifikační autoritě pomocí elektronické pošty, či doručeny jiným způsobem.

IW CONFIGMANAGER - NASTAVENÍ DLE LIBOSTI

IW ConfigManager je modulem, který slouží k nastavení ostatních modulů a aplikací systému IronWare®. Má otevřené rozhraní umožňující právě přidávání jednotlivých "nepovinných" aplikací. Umožňuje nakonfigurování IW Giny, IW ScreenWallu a spoustu dalších užitečných funkcí.

Za zmínku stojí funkce nastavení privilegovaných uživatelů. Tito mají možnost "obnovení hesla" - mnohokrát se totiž stane, že uživatel počítače změní zaměstnání či onemocní a zůstane po něm počítač plný zašifrovaných dat. Právě "privilegovaní uživatelé" mají možnost tato data zachránit. Při instalaci produktu je nutné, aby tři "privilegovaní uživatelé" zadali do systému svoji identifikaci (jméno) a heslo. Pak se při vkládání nového uživatele do systému, a rovněž při každé změně jeho hesla, toto heslo za použití asymetrické kryptografie zašifruje a uloží. V případě potřeby je pak možné za použití hesel libovolných dvou (různých) "privilegovaných uživatelů" heslo kteréhokoliv z uživatelů rekonstruovat a zobrazit.

CERTIFIKAČNÍ AUTORITA TRUSTCERT - VÍCE NEŽ DŮVĚRA

Nedílnou součástí bezpečnostních řešení založených na PKI je certifikační autorita. Její význam, funkce a důvěryhodnost byly rozebrány v předcházejících pasážích, takže se nyní zaměřme na jednu konkrétní autoritu, která je součástí řešení IronWare®.

Společnost AEC byla jednou z prvních českých společností, která se rozhodla svými zkušenostmi přispět k bezpečné komunikaci tím, že vytvořila projekt vlastní certifikační autority - **TrustCert**. V tomto projektu se pak pochopitelně rozhodla jít cestou, která zabezpečí vysokou důvěryhodnost vydávaných certifikátů. Certifikační autorita AEC TrustCert poskytuje svým klientům široké možnosti v oblasti ochrany elektronické komunikace. Na internetové adrese **www.trustcert.cz** je možné si vygenerovat nebo zažádat si o vydání nejen osobních digitálních certifikátů různých úrovní, ale také certifikátů serverových.

IW FILEPROTECT - ŠIFROVANÁ JISTOTA

Modul IW FileProtect je založen na on-line šifrování souborů tajnými nebo sdílenými (skupinovými) klíči. Zabezpečená data jsou přitom uložena na cílovém disku v zašifrované podobě zvoleným symetrickým šifrovacím klíčem (tajným nebo sdíleným více uživateli). Při pokusu o čtení souboru si IronWare® nejprve ověří, zda aktuálně přihlášený uživatel má k dispozici příslušný šifrovací klíč. Pokud ne, je přístup k šifrovaným souborům odmítnut. Pokud však uživatel patří mezi vlastníky příslušného šifrovacího klíče, pak je tento klíč použit pro automatické rozšifrování souboru při jeho čtení

do operační paměti. Aplikace, která soubor požaduje (například Word při otevírání dokumentu), dostane v tomto případě od operačního systému soubor již v rozšifrované podobě.

Pravidla, která jsou nastavená pro daný adresář se přitom vždy aplikují i na nově zakládané soubory v těchto adresářích nebo na soubory, které jsou do nich přesouvány či kopírovány. Při kopírování souboru do šifrovaného adresáře se tedy soubor automaticky zašifruje a při jeho zpětném kopírování do nešifrovaného adresáře automaticky rozšifruje. Šifrování probíhá na pozadí, takže uživatel při své práci nepozná, že data, se kterými pracuje, jsou šifrována. Všechny funkce pro nastavení šifrování jsou soustředěny ve standardním dialogovém okně vlastností adresáře, které lze vyvolat například pomocí pravého tlačítka myši.

Jednotlivé adresáře (nebo celé stromové struktury) lze zašifrovat buď jedním tajným klíčem nebo jedním sdíleným klíčem. U adre-sářů, které není vhodné přiřazovat k šifrování (adresáře s operačním systémem apod.), lze šifro-vání zakázat.

Praktický význam všech možností je shrnut v následujících bodech:

- **Šifrování tajným klíčem** - soubory v takto nastaveném adresáři jsou zašifrovány klíčem, který vlastní pouze jediný uživatel. V praxi se toto nastavení používá pro přidělení adresářů se soukromými daty jednotlivých uživatelů - např. domácí adresáře na souborovém serveru či stromové struktury s dokumenty na lokálním pevném disku.
- **Šifrování sdíleným klíčem** - soubory v tomto adresáři jsou zašifrovány klíčem, který je sdílen více uživateli. V praxi se používá např. pro nastavení adresáře, jehož obsah je nutné sdílet mezi pracovníky např. určitého oddělení. Konkrétně se může jednat např. o databázi zákazníků sdílenou obchodním oddělením nebo data účetního softwaru používaná účetním oddělením.
- **Vyhrazení adresářů** - takovýto adresář nemůže být přidělen k šifrování. V praxi se používá např. pro adresáře obsahující operační systém nebo některé části programů. Pokud bude k šifrování přidělen adresář nadřazený takto označenému podadresáři, bude tento podadresář při šifrování vynechán.

Z bezpečnostního hlediska jsou takto zajištěné soubory účinně chráněny proti porušení důvěrnosti před každým, kdo nepatří mezi jejich vlastníky (tedy jak proti ostatním nepovolaným zaměstnancům, tak proti vnějšímu narušiteli). Významnou vlastností je, že soubory jsou vždy rozšifrovány až v operační paměti koncové stanice - tj. až těsně před předáním dat koncové aplikaci. Díky tomu jsou data účinně chráněna proti odposlechu při přenosu jakoukoli sítí (ať již LAN či WAN).

IW FileProtect počítá i s možností, že dojde k vygenerování nových klíčů. Kdyby na tuto variantu nebylo pamatováno, mohla by být po vygenerování nových klíčů nenávratně ztracena data zabezpečená klíči starými. IW FileProtect nově zakládané soubory šifruje novým klíčem, ale soubory původní dešifruje stále původním klíčem. Na požádání je ovšem možné všechny soubory "přešifrovat" novým klíčem.

V praxi obvykle používá jeden počítač jediný uživatel, a tak data na lokálním disku není třeba dělit pro několik kategorií uživatelů. Jediným nepřítelem, proti němuž je nutné data zabezpečovat, je tak vnější narušitel. Toto platí především pro přenosné počítače, u nichž je nebezpečí zcizení poměrně vysoké. Z tohoto důvodu je výhodné rozdělit pevný disk (pro zjednodušení předpokládejme, že počítač je vybaven jen jedním diskem) na dva logické oddíly: "C" obsahuje operační systém a programy, "D" obsahuje data, která je potřeba chránit. Poté je vhodné nastavit šifrování pomocí IW FileProtect na kořenový adresář disku D: (včetně podadresářů). Pokud je vzhledem k malé velikosti disku či z jakýchkoliv jiných důvodů obtížné rozdělit jej na dva logické oddíly, lze nastavit adresáře obsahující operační systém a programy jako vyhrazené - tedy jako takové, které nebudou šifrovány. Poté necháme zašifrovat všechny ostatní adresáře tajným klíčem uživatele.

Podobným způsobem jako je šifrování celých disků lze nastavovat i šifrování výměnných médií. Po prvním vložení výměnného disku nastavíme kořenový adresář výměnného média jako šifrovaný. Poté všechny soubory a adresáře zapisované na toto výměnné médium budou automaticky šifrovány příslušným klíčem. V případě požadavku na šifrovaný CD-ROM lze využít následujícího postupu: Připravíme data na pevný disk, kde nastavíme šifrování pro všechny požadované adresáře, poté soubory zašifrujeme. Pak speciální volbou v IW ConfigManageru vypneme on-line rozšifrovávání a CD-ROM vypálíme na příslušné médium. Poté můžeme znovu aktivovat ovladač on-line šifrování a začít používat hotové CD-ROM s vypálenými šifrovanými soubory.

Obr. Vypnutí on-line šifrování

Pozor! K dešifrování dat v budoucnu budete samozřejmě potřebovat příslušný klíč! Proto není možné tímto způsobem např. zálohovat data a poté přeinstalovat operační systém včetně bezpečnostního software (bez problémů je to možné, pokud jsou klíče uloženy na IW ManagementServeru). V takovém případě musíte společně se zálohovanými daty zazálohovat i dešifrovací klíče!

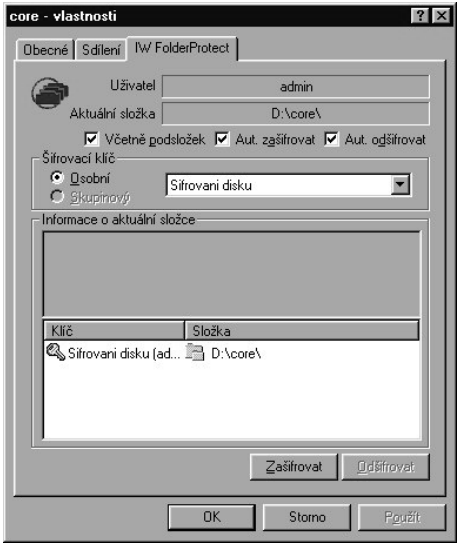
IW FOLDERPROTECT - PRO BEZPEČÍ ADRESÁŘŮ

Tento modul zajišťuje ochranu dat před neautorizovanými osobami prostřednictvím technologie off-line šifrování dat v adresářích na lokálním pevném disku počítače, kde je nainstalován (na rozdíl od IW FileProtectu, který "umí" i síťové disky a výměnná média). Bližší informace o technologii off-line šifrování - viz pasáž Typy šifrování. Jen pro stručné zopakování:

Technologie off-line šifrování na rozdíl od on-line (IW FileProtect) nešifruje data v reálném čase, nýbrž jednorázově při spuštění nebo vypnutí operačního systému (Windows NT), resp. na vyžádání (Windows NT, Windows 9x).

Automatická funkce odšifrování/zašifrování funguje ve Windows NT následovně: Při spuštění počítače se soubory v nastavených adresářích odšifrují, při vypnutí se naopak zašifrují. Proces šifrování jednotlivých nastavených adresářů lze spustit buď při každém přihlášení majitele příslušného šifrovacího klíče (tajného nebo sdíleného klíče, kterým jsou data šifrována) nebo explicitně na požádání. Zašifrovaný soubor je opatřen speciální příponou ".ciphered" připojenou za konec názvu souboru.

Modul IW FolderProtect stejně jako IW FileProtect umožňuje šifrovat data v adresáři buď tajným nebo sdíleným klíčem. Protože klíče jsou jednoznačně



vázány na jednotlivé uživatele nebo jejich skupiny, lze na stejném počítači uchovávat svá tajná data oddělená pro jednotlivé uživatele. V praxi se IW FolderProtect obvykle používá pro šifrování menšího objemu dat uložených na lokálním disku. Při práci s podadresáři platí stejná pravidla jako u modulu IW FileProtect. Přidělování adresářů pro šifrování tajným klíčem smí provádět uživatel (majitel tajného klíče) nebo administrátor (může provést vyčlenění adresářů z šifrování); přidělování adresářů pro šifrování sdíleným klíčem nebo označení adresáře jako "nedovoleného pro šifrování" smí provádět pouze administrátor.

Technologie off-line šifrování zabezpečuje soubory pouze ve chvíli, kdy jsou šifrovány. Ve chvíli, kdy mají být soubory použity aplikací, musí být rozšifrovány a uloženy na disk v otevřeném tvaru. V této chvíli soubory nejsou jakkoli chráněny. Použití tohoto modulu je vázáno na znalost principu technologie off-line uživatelem.

Modul IW FolderProtect není určen k současnému použití s modulem IW FileProtect, a proto oba moduly není možné instalovat současně.

IW JUSTPROTECT - ŠIFROVÁNÍ TADY A TEĎ

Modul On-demand šifrování (na požádání - viz kapitola Typy šifrování) s názvem IW JustProtect umožňuje šifrovat soubory ve vybraných adresářích a adresářových strukturách na libovolných lokálních nebo síťových discích. V praxi pracuje následujícím způsobem: V libovolném správci souborů vybereme jeden nebo několik souborů nebo adresářů, které chceme šifrovat. Stiskneme pravé tlačítko myši, abychom vyvolali kontextové menu a zde zvolíme volbu zašifrovat vybrané soubory. Poté zvolíme, jakým klíčem zvolené soubory budeme šifrovat. K dispozici jsou následující možnosti:

- **Vybereme tajný klíč konkrétního uživatele**. Z každého vybraného souboru pro šifrování vznikne šifrovaný soubor. Soubor bude moci rozšifrovat pouze vlastník tajného klíče, tj. ten, kdo soubory zašifroval.

Výsledek šifrování je kompatibilní s IW FolderProtect a může jím napří-klad být odšifrován a samozřejmě naopak. IW JustProtect na kliknutí myši může odšifrovat soubory zašifrované IW FolderProtectem: ovšem za předpokladu, že uživatel je oprávněný vlastník šifrovacího klíče.

- **Zvolíme sdílený klíč skupiny uživatelů**. Každý šifrovaný soubor bude nahrazen šifrovaným obrazem. Dešifrovat zpět je může kterýkoli uživatel, který má k dispozici sdílený klíč.
- **Vytvoříme samorozbalovací EXE soubor obsahující všechny vybrané soubory a adresáře v zašifrované podobě**. Jako klíč je použito heslo zadávané při vytváření tohoto souboru. V takto vzniklém souboru jsou uloženy všechny zašifrované soubory a adresáře i s kódem šifrovacího

algoritmu. Soubor je následně možné zaslat adresátovi, který nemusí mít instalován žádný šifrovací software. Adresátovi je nutné pouze doručit bezpečnou cestou heslo pro rozbalení obsažených souborů a adresářů. Rozbalení lze provést jednoduše spuštěním vzniklého souboru a zadáním hesla. Vzniklý spustitelný EXE soubor je 32bitová DOS aplikace, kterou je možné spouštět pouze z prostředí 32-bit Windows (Windows95, 98 a NT). Díky tomu jsou archivované soubory ukládány a obnovovány včetně svých dlouhých názvů. Pro tento druh šifrování je napevno implementován 128 bitový algoritmus CAST.

Soubory šifrované pomocí modulů IW FolderProtect a IW JustProtect jsou vzájemně kompatibilní. Modul IW JustProtect je vhodný pro šifrování dat určených pro archivaci nebo v případech, kdy není možné použít on-line technologie. Je výhodný zejména pro svou jednoduchost.

Modul IW JustProtect je možné instalovat a využívat i samostatně bez využití celého systému IronWare®.

IW SHREDDER - BEZPEČNÁ LIKVIDACE DAT

Protože běžné operační systémy na bázi Windows neumožňují neobnovitelné smazání dokumentu, vznikl modul IW Shredder, který slouží k neobnovitelnému mazání souborů nebo disků. Běžný operační systém soubory maže tím způsobem, že poupraví pouze hlavičku souboru ve FAT nebo NTFS a označí místo, které soubor zabíral, jako volné místo. Soubor ale fyzicky stále leží na disku - a pokud útočník poopraví hlavičku zpět, je soubor obnoven. Princip neobnovitelného smazání souborů spočívá v několikanásobném přepsání obsahu souborů, jeho zkrácení na nulovou délku a teprve poté smazáním operačním systémem. Několikanásobné přepisování se provádí kvůli rezistenci magnetických médií (magnetické médium umožňuje obnovování i přepsaných záznamů pomocí měření zbytkových magnetických proudů). Soubory jsou proto přepisovány

několikrát (až 26krát). Počet přepsání i řetězec, který bude použit pro přepisování dat, lze v programu nastavit nebo generovat náhodně.

Modul je složen z následujících částí:

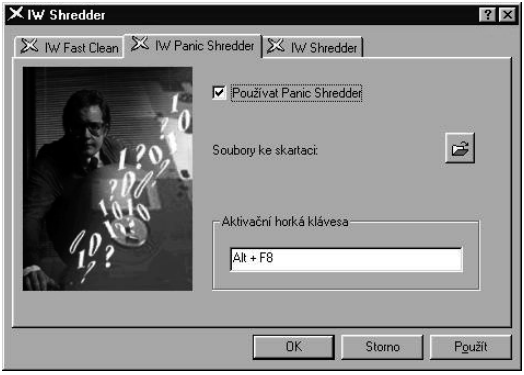
IW Shredder - po instalaci do kontextového menu, které se standardně aktivuje na pravé tlačítko myši, přibude funkce skartace vybraného souboru nebo adresáře. Po zvolení této akce jsou vybrané soubory nebo adresáře skartovány.

IW FastClean - funkce pro skartování určitých souborů na požádání. Na jednotlivých discích lze nastavit okamžitou jednorázovou skartaci odkládacích a dočasných souborů SWP a TMP, skartaci standardního koše Windows nebo volného místa na disku. Lze nastavit smazání určitého konkrétního seznamu souborů a adresářů pro skartaci, skartaci historie otevíraných souborů, dočasných souborů systému Windows nebo internetových prohlížečů WWW.

IW PanicShredder - umožňuje nastavení seznamu souborů, souborových masek nebo celých adresářů, které budou bezpečně smazány při každém

stisku určité kombinace kláves. Zaručuje, že v případě nenadálého ohrožení bude možné citlivá data okamžitě zlikvidovat, avšak nepadnou do nepovolaných rukou.

Modul IW Shredder je možné instalovat a využívat i samostatně bez využití celého systému IronWare®.



IW MAILPROTECT - PRO ELEKTRONICKOU POŠTU A DIGITÁLNÍ PODPIS

IW MailProtect je aplikace určená k šifrování, dešifrování, autentizaci a kontrole integrity zpráv a k nim připojených souborů zasílaných elektronickou poštou (e-mail).

Program sdílí lokální nebo vzdálenou databázi šifrovacích klíčů a certifikátů, přičemž po přihlášení uživatele je v databázi vyhledán a dán k dispozici odpovídající soukromý klíč (slouží k vytváření digitálního podpisu a odšifrovávání přijatých zpráv). Podobně systém pracuje i při vyhledání potřebného odpovídajícího certifikátu (slouží k zašifrování zprávy). V tomto případě však používá jako identifikaci e-mailovou adresu zamýšleného adresáta. Uživatel tedy jen zadá tuto adresu a potřebné šifrovací klíče a certifikáty jsou samy automaticky vyhledány. (Podporované protokoly jsou jak SMTP, tak i Microsoft Mail.)

Poštovní zprávy a jejich přílohy mohou být před odesláním komprimovány tak, aby se zmenšila jejich velikost a mohly být rychleji a pohodlněji doručeny. Kompresní algoritmus je velmi podobný známému PKZIP algoritmu a jeho kompresní poměr je v závislosti na typu dat minimálně dva ku jedné (použití komprese však vylučuje kompatibilitu s jinými bezpečnostními programy). Postup je takový, že zpráva a příloha jsou nejdříve zkomprimovány a potom, před převedením na formát transportního protokolu (SMTP nebo Microsoft Mail), zašifrovány a digitálně podepsány.

Nastavení IW MailProtect se provádí v záložce IW ConfigManageru. Zde se nastavuje předdefinovaný soukromý klíč - je-li jich více, pak je možné vybrat ten, který bude primárně přednastavený při startu. Současně je zde možné nastavit preferovaný symetrický šifrovací algoritmus a hash funkci. Také je zde umožněno ukládat odesílané e-maily do speciální složky

v nezašifrovaném tvaru, protože zašifrovaný mail smí číst pouze příjemce a odesilatel by se tak k jeho obsahu již nikdy nedostal. K dispozici jsou i další vlastnosti.

IW MailProtect je k dispozici v podobě modulu pro Microsoft Exchange nebo Microsoft Outlook nebo jako samostatný program pracující

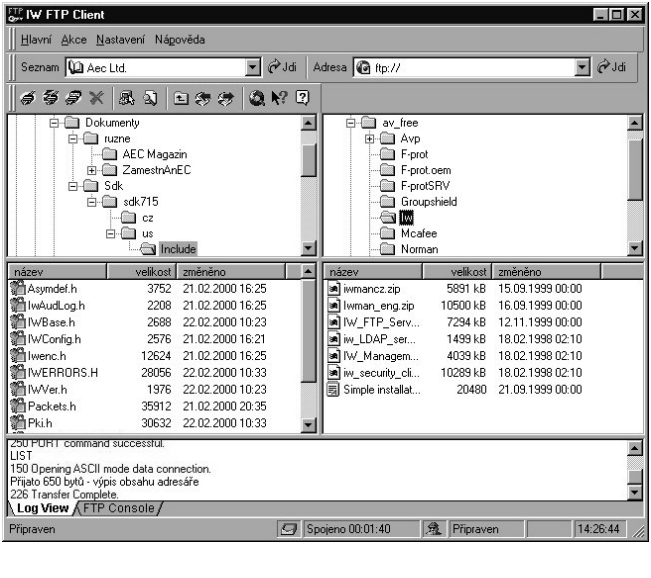
s Windows schránkou (clipboard) a aktuálním oknem pro všechny ostatní poštovní klienty.

Přijatá zpráva je uložena na disk v zašifrované podobě a teprve při svém otevření je dešifrována. Zpracování přijaté zprávy je přitom zcela automatické: Je postupně ověřena její pravost, provedeno dešifrování, dekomprimace a ověřena její celistvost. Uživatel tak nemusí do celého procesu vůbec zasahovat a je upozorněn vlastně jen v okamžiku, kdy něco není v pořádku (např. když byla zpráva v průběhu cesty modifikována a elektronický podpis je tudíž neplatný).

IW FTP CLIENT - PRO BEZPEČNÉ SPOJENÍ

Aplikace IW FTP Client je základem celého systému bezpečného přenosu dat, neboť může být využita samostatně nebo může spolupracovat s IW FTP Serverem. Samozřejmě se dá použít i jako zcela běžný FTP prohlížeč. Svým uživatelským rozhraním připomíná IW FTP Client Windows Explorer, nicméně pro zkušené uživatele je k dispozici konzola s příkazovým řádkem. Od běžného FTP prohlížeče se IW FTP Client mimo jiné odlišuje třemi základními vlastnostmi. Jednou je zabezpečení souborů šifrováním, druhou vytváření vlastního adresáře "oblíbených" FTP serverů (address book) a třetí tzv. "queueing" systém.

Začněme od onoho exotického slůvka "queueing". Queueing je vytváření fronty pro odeslání nebo stažení souborů, přičemž jde o významnou



vlastnost IW FTP Clientu. Jeho uživatel si může jednoduchým způsobem připra-vit seznam souborů, které budou odeslány nebo staženy, a pak (například v době, kdy je zatížení sítě nejmenší) je najednou odeslat/stáhnout. Soubory, které jsou ve frontě, zůstávají uloženy po celou dobu "čekání" na původním místě. Až po příkazu k odeslání jsou načteny do paměti, kde mohou být zašifrovány a opatřeny digitálním podpisem a pak odeslány. Informace o uložení těchto souborů, o jejich cílových adresářích a informace nezbytné pro šifrování (který certifikát má být použit pro šifrování a který klíč pro podpis) si IW FTP Client drží po dobu své aktivity v paměti. Chcete-li např. pro další použití uchovat informace o frontě i po ukončení programu IW FTP Client, je možné je uložit do souboru s příponou "que".

Jak bylo uvedeno výše, IW FTP Client "umí" také zabezpečit soubory šifrováním. Samotné šifrování souborů probíhá v paměti počítače, takže samotné soubory zůstávají na pevném disku v nezašifrovaném tvaru. Před odesláním je soubor načten do paměti počítače, zde může být napřed zkomprimován, následně je zašifrován a digitálně podepsán. Potřebné šifrovací klíče a certifikáty jsou vyhledány v databázi PKI. Soubor je poté převeden do formátu FTP protokolu a odeslán FTP službou. Odeslán může být na libovolný FTP server, který je uživateli přístupný, a na něm je uložen. Na serveru tedy leží v zašifrované podobě a nemůže být otevřen neoprávněnou osobou. Soubor je automaticky dešifrován až po stažení ze serveru, které provede oprávněný uživatel. "Oprávněný uživatel" je ten, který má k dispozici potřebný dešifrovací klíč.

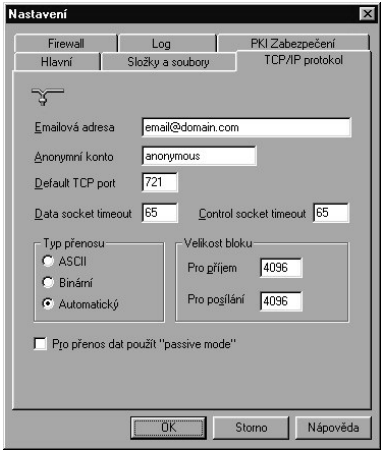
IW FTP Client umožňuje ustavit tzv. bezpečný tunel mezi sebou samým a IW FTP Serverem. To poskytuje možnost zřídit šifrované spojení. Při použití bezpečného tunelu jsou data stahovaná ze serveru před svým odesláním automaticky zašifrována, takže putují v bezpečné formě třeba Internetem, po příchodu na IW FTP Client jsou automaticky dešifrována a naopak. Protože data jsou na obou stranách spojení automaticky

dešifrována a ukládána v otevřené formě, je zřejmé i využití takového spojení v případech jako je např. bezpečné propojení informačních toků mezi centrálou a pobočkami jedné firmy.

IW FTP SERVER - BEZPEČNÉ SPOJENÍ PODRUHÉ

IW FTP Server je klasickým FTP serverem rozšířeným o šifrovací a autentizační moduly. Spouští se buď jako aplikace ve Windows 95/98 nebo jako systémová služba ve Windows NT.

IW FTP Server umožňuje vytvořit libovolný počet tzv. virtuálních serverů (fyzicky, na jednom hardware může současně pracovat několik virtuálních FTP serverů s různými názvy); rozlišují se přitom dva druhy virtuálních FTP serverů - administrativní server (pro vzdálenou správu FTP serveru) a ostatní servery. Administrativní server může být vytvořen pouze jeden, počet ostatních je limitován možnostmi hardware. Každý virtuální FTP server je definován portem a IP adresou, přičemž jejich kombinace musí být jedinečná.



Dejte přednost jistotě!

AEC - společnost s desetiletou tradicí v oblasti software a služeb pro komplexní zabezpečení a ochranu dat.

- bezpečnostní analýzy
- studie a projekty
- komplexní návrhy řešení včetně jejich realizace
- konzultace
- audit bezpečnostních řešení
- odborná školení a semináře
- certifikační autorita „na klíč“

AEC

DATA SECURITY COMPANY

BRNO: AEC, spol. s r.o., Bayerova 799/30, 602 00 Brno, tel.: 05/4123 5466-7
fax: 05/4123 5038, e-mail: info@aec.cz, www.aec.cz

PRAHA: AEC, spol. s r.o., Vinohradská 184, 130 52 Praha 3
tel./fax: 02/6731 4326, 6731 1402, e-mail: praha@aec.cz, www.aec.cz

Bratislava: AEC Bratislava, s.r.o.
Pribinova 25, P.O.Box 79, 810 11 Bratislava, Slovenská republika,
tel: + 421 2 50633 027, fax: + 421 2 50633 029, e-mail: bratislava@aec.sk

AEC

DATA SECURITY COMPANY

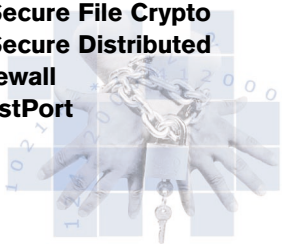
Máme pro Vás řešení!

Antivirový software

- F-Secure AntiVirus
- Kaspersky AntiVirus
- Panda Antivirus
- Antivirové produkty Network Associates
- Sybari

Bezpečnostní řešení

- Cyber Cop
- F-Secure VPN+
- F-Secure SSH
- F-Secure File Crypto
- F-Secure Distributed Firewall
- TrustPort



Služby a servis klientům

- Bezpečnostní analýzy
- Semináře a školení
- TrustCert
- Certifikační autorita „na klíč“

BRNO: AEC, spol. s r.o., Bayerova 799/30, 602 00 Brno, tel.: 05/4123 5466-7
fax: 05/4123 5038, e-mail: info@aec.cz, www.aec.cz

PRAHA: AEC, spol. s r.o., Vinohradská 184, 130 52 Praha 3
tel./fax: 02/6731 4326, 6731 1402, e-mail: praha@aec.cz, www.aec.cz

Bratislava: AEC Bratislava, s.r.o.
Pribinova 25, P.O.Box 79, 810 11 Bratislava, Slovenská republika,
tel: + 421 2 50633 027, fax: + 421 2 50633 029, e-mail: bratislava@aec.sk