Důvěřuj, ale prověřuj

Víte vůbec, kdo je na druhém konci? – kybernetická identita – 2. díl

PATRIK MALINA

V první části našeho článku o nezpochybnitelné identitě v kybernetickém světě, jejž najdete v minulém vydání PC WORLDu, jsme se věnovali zvláště základním principům a ukázkám, jak vlastně vypadá certifikát a jakým způsobem s ním lze pracovat. V minulém dílu našeho článku jsme si objasnili základní vlastnosti asymetrické kryptografie a přiblížili jsme si její principiální vlastnosti, jejichž výhod v současné době využíváme. Jednou ze zásadních aplikací tohoto univerzálního schématu je postup, běžně zjednodušeně označovaný jako digitální podpis. Protože se jedná o funkci klíčového významu, blíže si zde osvětlíme její podstatu, a v následujících odstavcích pak předvedeme praktické nasazení při poštovní komunikaci. Pokud jsme pár veřejný a privátní klíč dosud využívali při šifrování, postup byl vždy jednoznačný: veřejný klíč adresáta-příjemce posloužil pro operaci zašifrování a jeho příslušný privátní klíč pak posloužil k rozšifrování utajených dat. Tento postup tedy vyřeší utajení, ovšem naší snahou je zajistit ještě neméně důležitý druhý cíl, kterým je ověření pravosti odesílatele a potvrzení, že zprávu v průběhu cesty nic nepozměnilo a nepoškodilo, tedy nebyla např. podvržena.

Právě tuto fázi zajistí digitální podpis, při němž jsou klíče použity odlišným způsobem. Na rozdíl od šifry musí při podpisu odesílatel mimo jakoukoliv pochybnost prokázat, že zpráva pochází od něj. To znamená, že ji musí označit nějakým „otiskem", jehož autorem nemůže být nikdo jiný. Pomocí čeho to provede? Hádáte správně – jediná utajená „věc", kterou má každý uživatel ve své absolutní moci a střeží ji jako tajemství, je privátní klíč. Myšlenka je tedy taková, že sestavená zpráva je v zásadě podepsána privátním klíčem odesílatele a posléze vypuštěna do internetu běžnou cestou (v případě, že netrváte na utajení, nemusíte obsah šifrovat – to je zcela nezávislá možnost). Jakmile příjemce obdrží tradičním způsobem váš e-mail, zjistí, že jeho náplň lze ověřit pomocí platnosti elektronického podpisu. Jak to provede? Ano, samozřejmě použije veřejný klíč odesílatele, neboť to je jediná část systému, jež se cizímu příjemci může dostat do ruky. A otázka, kde jej vezme, je pro poctivé čtenáře z minula snadná: veřejný klíč odesílatele digitálně podepsaného e-mailu je obsažen v certifikátu, jejž vám samotný odesílatel do zprávy může přiložit. Takže máme doručenou zprávu, „přešifrovanou" privátním klíčem odesílatele, jeho veřejný klíč, jemuž důvěřujeme (ověřili jsme si pravost certifikátu, jak víme z minula), a nic nám nebrání provést dešifrování. Pokud se operace podaří a obdržíme původní, korektní zprávu, je vše v pořádku a původnost je ověřena.

Jenže jistě zde cítíte určité drobné nedostatky, jež bude potřeba vyřešit. V první řadě, asymetrická kryptografie je poměrně pomalá, a rutinní šifrování celých zpráv (třeba včetně objemných příloh) by bylo tak obtížné, že bychom se možná dostali na hranici použitelnosti. Dále je tu jiný nedostatek v podobě skutečnosti, že celou digitálně podepsanou zprávu, jejíž původní verzi jsme získali díky použití veřejného klíče odesílatele, nemáme s čím srovnat – nemáme zkrátka referenční verzi téže zprávy. Naštěstí se celý postup odehrává ve skutečnosti v trošku upravené verzi.

Pokud se odesílatel pokusí digitálně podepsat odchozí zprávu, dojde nejprve k provedení určité výpočetní funkce, jejímž výsledkem je jedinečný otisk, běžně označovaný jako hash. Jde o jakýsi zhuštěný vzorek, jenž se vyznačuje důležitými vlastnostmi. V první řadě má konstantní délku, která je typicky velmi malá v poměru k objemu celé zprávy, a pochopitelně právě toto značně urychlí následné kryptografické operace. Dále je hash prakticky jedinečným obtiskem a platí, že drobounká změna původní zprávy vyvolává značnou změnu vystupující hashe. A v neposlední řadě platí další důležitá skutečnost, a to že výpočet hashe je jednosměrná operace, takže z její hodnoty nelze zpětně rekonstruovat obsah zprávy. Přesněji řečeno, při snaze o zpětné sestavení výchozí podoby zprávy by vám nevznikla jediná varianta, ale řada verzí, z nichž byste stejně nic kloudného nevybrali, a navíc byste vše počítali velmi dlouho.

Celý postup se díky hashi projasňuje a dostává pevné obrysy. Odesílatel tedy ve skutečnosti sestaví kolekci, zahrnující původní zprávu, certifikát se svým veřejným klíčem a vypočtenou hash, zašifrovanou svým privátním klíčem. A příjemce? Asi tušíte, že uchopí doručenou zprávu, vypočte dohodnutým postupem svou variantu hashe (algoritmus je veřejný a nijak to neohrožuje bezpečnost), následně z certifikátu odesílatele vytáhne jeho veřejný klíč, s jeho pomocí dešifruje doručenou hash a pak obě varianty porovná. Pokud se odeslaná – podepsaná – varianta hashe shoduje s verzí, kterou si příjemce pořídil sám pod vlastní kontrolou, pravost obsahu zprávy je stvrzena a její přenos je považován za důvěryhodný.

Postup je názornou ukázkou, že samotné šifrování není jediným využitím asymetrické kryptografie a její geniální podstata nabízí i další, velmi důležité aplikace. Dodejme, že příklad, popsaný na elektronické poště, popisuje obecnější schéma, neboť digitálně podepisovat lze celou řadu jiných entit, jako třeba programové komponenty, instalační balíky či třeba ovladače pro zařízení v operačním systému.

Podepisujeme a šifrujeme poštu

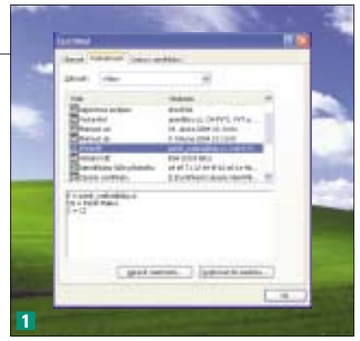
Jedním z nejdůležitějších využití prostředků pro elektronickou identifikaci a silné asymetrické kryptografie je nasazení pro posílení důvěryhodnosti v oblasti e-mailové komunikace. Elektronická pošta se stala běžnou součástí našeho života, a protože se ve výchozí podobě v podstatě jedná o velmi nedůvěryhodný komunikační kanál (podvrhnout e-mail je neuvěřitelně snadné), je nasazení certifikátů žádoucí. Použití elektronické identity a šifry s sebou přináší řadu výhod a kýžených vlastností: příjemce si může ověřit pravost odesílatele, jenž zároveň nemůže dodatečně autenticitu své zprávy popřít (jeho „značka" je nezaměnitelná), a obsah zprávy je pochopitelně možno ochránit silnými šifrovacími postupy, čímž navíc zajistíte naprostou privátnost přenášených dat. Použití certifikátu pro uvedené účely je umožněno díky zavedení protokolu S/MIME, což je prostředek pro přímé začlenění možností asymetrické kryptografie do programů pro zasílání elektronické pošty. Řada klientských aplikací, včetně produktu Outlook Express, tento protokol podporují, a nabízejí uživatelům pohodlné rozhraní, jež tyto jinak poměrně komplikované postupy zajistí. Nemusíte se obávat, vše je dobře zvládnutelné.

Obr. 1: Postup zavedení chráněné komunikace si ukážeme na příkladu MS Outlook Expressu, přesněji v jeho verzi 6.00, jež je součástí MS Internet Exploreru 6.0, vše v operačním systému MS Windows XP. Základem úspěchu je v první řadě existence certifikátu uživatele, jenž chce svou poštu chránit. Pro pokusné účely si můžete potřebný certifikát nechat zdarma vystavit např. certifikační autoritou I.CA, podobně jako jsme to udělali my (na adrese *http://Lobkowiczova/cer_ test_standardnostmi*). Takto či jinak získaný osobní certifikát se musí vyznačovat jednou zásadní vlastností: jako předmět se musí v jeho záznamech vyskytovat právě ta e-mailová adresa, kterou hodláte příslušným veřejným klíčem z certifikátu podepisovat či šifrovat. Nejde o formalitu, neboť Outlook Express vám použití nekorektně vystaveného certifikátu nedovolí a celá procedura nebude funkční, přesněji bude nedostupná. Pokud na uvedené webové stránce vyplníte testovací žádost včetně zadání e-mailu, bude vám autoritou obratem zaslán takovýto certifikát, jejž lze následně otestovat.

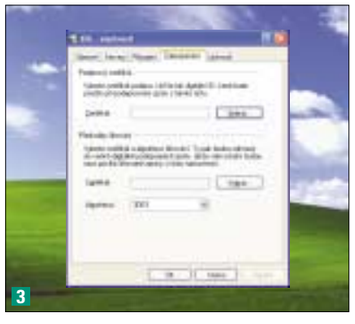
Obr. 2: Doručený osobní certifikát je nutno po uložení na disk nejprve naimportovat do osobního úložiště. Toho dosáhnete dvojklikem na samotný soubor (máte-li jich více variant, což je běžné, pak vyberte třeba ten s příponou .der), načež v následujícím průvodci importem pro jistotu ručně zadejte, že cílem certifikátu je úložiště Osobní (Personal). Dokončením této procedury jsme dosáhli výchozí konfigurace, totiž toho, že náš „podepisovací a šifrovací e-mailový" certifikát je uložen v operačním systému a můžeme jej předhodit poštovnímu programu. Než pokročíme dále, vzpomeňte si ještě na minulý díl a případně si do operačního systému obdobným postupem naimportujte certifikát samotné vydavatelské certifikační autority, v našem případě tedy I.CA. Však víte, důvěryhodný kořen je základem!

Obr. 3: Takto vybaveni můžeme vstoupit do poštovní aplikace, v tomto případě Outlook Expressu. Ještě než začneme, vezměte na vědomí jednu drobnost: tvůrci systému si příliš nelámali hlavu s názvoslovím, a proto vás nesmí zmást, že standardní struktuře jménem certifikát se občas v programu říká Digitální ID. Nuže k věci. Zde bude prvním krokem napojení certifikátu na konkrétní, existující poštovní účet. Vstupte pomocí volby *Nástroje/Účty* do dialogu *Účty v Internetu*, vyberte příslušné e-mailové konto a stiskněte tlačítko *Vlastnosti*. V následujícím dialogu přejděte na kartu *Zabezpečení*, neboť právě zde se ono propojení provádí. Jak je patrné i z obrázku, máte možnost k otevřenému účtu přiřadit dva certifikáty, nezávisle pro podepisování a šifrování zpráv. Pochopitelně lze přiřadit jediný pro obě operace. Ve výchozí podobě jsou pole prozatím prázdná.

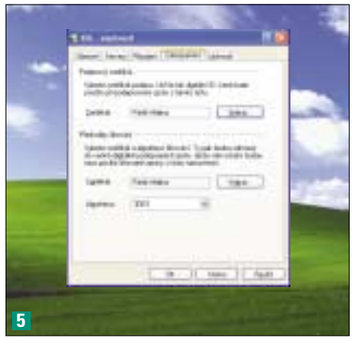
Obr. 4: Zvolte tedy v jednom z případů tlačítko *Vybrat*, a vstoupíte tak do vlastního dialogu pro výběr konkrétního certifikátu. A právě zde dochází na „lámání chleba": pokud bude otevřený seznam prázdný, znamená to, že Outlook Express nenašel žádný použitelný certifikát, a vy se nemůžete pohnout dále a operaci dokončit. Jak se toto mohlo stát? Možností je několik: buďto jste Osobní prozatím vůbec nenaimportovali (pak to udělejte dle postupu výše), nebo jste certifikát naimportovali na špatné místo mimo úložiště Osobní (což je ta méně pravděpodobná varianta, pokud jste byli důslední), případně jste využili osobní certifikát, jehož Předmět (Subject) obsa-

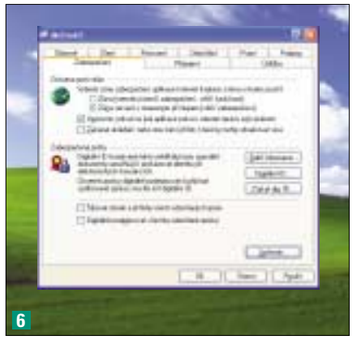

1

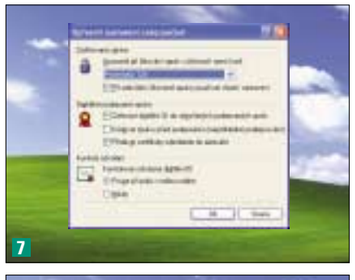

2


3


4


5


6


7

huje jinou e-mailovou adresu, než jaká je zapsána v právě ošetřovaném účtu (typická situace). Nepříjemné je, že Outlook Express neoznámí chybu, ale prostě pouze nenabídne žádný certifikát k přiřazení, a na vás je vypátrání důvodu. Pokud vše proběhlo korektně, bude v seznamu alespoň jedna dostupná položka, jako na našem obrázku.

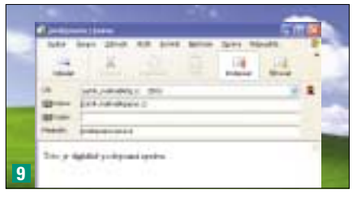
Obr. 5: je vše v pořádku – případně si certifikát pro kontrolu prohlédněte a následně potvrďte výběr tlačítkem *OK* – bude karta *Zabezpečení* realizované připojení signalizovat připojeným jménem držitele certifikátu. Naprosto identickým postupem pak přiřaďte též certifikát pro šifrování obsahu zpráv. V dolní části karty si povšimněte volby *Algoritmus*, v jejímž menu máte možnost ovlivnit, jakým postupem se bude provádět utajení poštovních zpráv. Pamatujte si především fakt, že nejsilnější zde dostupnou variantou je 3DES. Po úspěšném nastavení by karta měla vypadat asi jako na našem obrázku.

Obr. 6: Po úspěšné přípravě zázemí můžeme přistoupit ke konkrétní ochraně jednotlivých zpráv. Ještě jednou si připomeňme, že pokud se vám procedura s přiřazením certifikátů nezdařila, následující funkce nebudou korektně dostupné.

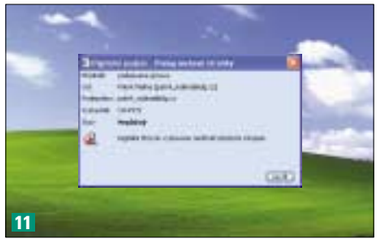
Samotný proces šifrování a podepisování zpráv lze řídit ručně pro každý jednotlivý případ či nastavit všeobecně, pro všechny odesílané e-maily. Nejdříve tedy přejděte do menu *Nástroje/Možnosti* na kartu *Zabezpečení*, kde v dolní části můžete využít zaškrtávacích polí pro výchozí ovlivnění všech zpráv. Vřele doporučujeme obzvláště šifrování na tomto místě nezapínat a řešit jej případ od případu, na druhou stranu digitální podpis všem e-mailům nijak zásadně nemůže uškodit.

Obr. 7: Pomocí tlačítka *Upřesnit* dále přejděte do podrobnějšího dialogu s větším množstvím parametrů, jejichž prostřednictvím dále můžete ovlivnit chování programu. Horní část pojednává o šifrování a dovoluje v rolovacím menu definovat úroveň zabezpečení, jíž v příchozích zprávách očekáváte. Pokud nastavíte laťku vysoko, příchozí e-maily se slabší šifrou budou varovně označeny jako „slabší" a vy budete moci posoudit, zda-

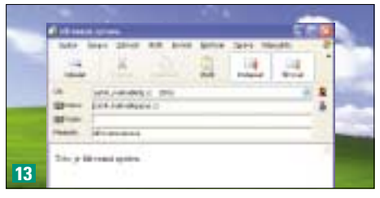

8


9


10


11


12


13

li jejich utajení věříte. V praxi klidně používejte pravidlo, že co je nad 128 bitů, je pro běžnou komunikaci velmi bezpečné. Nastavení v prostřední sekci ovlivňují nakládání programu s certifikáty. Obzvláště první a třetí volba jsou důležité a využívejte jich – příjemci vaší pošty rovnou obdrží krom podpisu i certifikát s vaším veřejným klíčem, a pokud vám doručené e-maily budou certifikáty odesílatelů také zahrnovat, budou tyto automaticky uloženy do systému do příslušného zásobníku. Poslední dolní volba spouští klíčovou funkcionalitu, o níž jsme si důkladně pohovořili minule, a to je Kontrola odvolání certifikátů (revokace). Chcete-li zajistit seriózní důvěryhodnost, měli byste kontrolu zapnout.

Obr. 8/9: Takto vybaveni již můžeme konečně napsat a odeslat první digitálně podepsanou zprávu. Postup při sestavení e-mailu je pochopitelně standardní, takže prostě udělejte, na co jste zvyklí, a zastavte se před odesláním. Pokud chcete aplikovat elektronický podpis, poslouží vám k tomu tlačítko obálky s pečetí, po jehož stisku se vedle pole *„Od:"* objeví malý grafický symbol, znázorňující že se chystáte odeslat digitálně podepsaný e-mail.Teď můžete poštu běžným postupem zaslat příjemci.

Obr. 10/11: Co nastane v případě doručení takovéto zprávy protistraně? V každém případě bude příjem podepsané zprávy avizován příslušnou ikonou v jejím záhlaví. Další situace bude především závislá na skutečnosti, zda příjemce e-mailu důvěřuje stejnému vydavateli certifikátů, od nějž obdržel odesílatel ten svůj. O významu důvěryhodných kořenových autorit jsme hovořili minule, takže vám jistě neušlo, že důvěryhodnost digitálního podpisu závisí na prestiži autority, jež jej posvětila. Pokud příjemce prozatím autoritě nedůvěřuje, dostane se mu varovné zprávy, že něco není v pořádku, přičemž případné nejasnosti lze okamžitě zjistit.

Obr. 12/13: Pokud příjemce i odesílal v případě otevírání e-mailu již důvěřují stejné autoritě, poštovní program nebude poukazovat na potíže a korektně naznačí, zdali doručená zpráva je v pořádku, tedy zda nebyla platnost podpisu narušena


14


15


16


17


18


19


20


21

v průběhu přepravy jakýmkoliv vnějším zásahem. Velmi důležitá je skutečnost, že pokud vám odesílatel poskytnul jako přílohu svůj certifikát s veřejným klíčem, uložením jeho identifikačních údajů do adresáře aplikace dojde také k současnému archivování certifikátu pro budoucí využití.

Obdobným způsobem jsou prováděny potřebné operace v průběhu šifrování zprávy. Na počátku je opět odesílatel, jeho nový e-mail a tlačítko, jež pro změnu obsahuje visací zámek. Zprávu lze zároveň zašifrovat i podepsat, čímž v podstatě využijeme dostupné možnosti pro její ochranu.

Obr. 14: Zde, v případě šifrování, však mohou nastat obtíže již při snaze e-mail odeslat. Jak správně tušíte, při snaze o ukrytí dat šifrou vás může zaskočit absence certifikátu příjemce, bez nějž nemáte šanci získat jeho veřejný klíč, pro šifrování nezbytný. Jak situaci řešit? Jednou z možností je nechat si protějškem zaslat potřebný certifikát jako přílohu, pochopitelně v pěkně podepsaném e-mailu…

Obr. 15/16: Naplníte-li předpoklady a zprávu korektně před odesláním zašifrujete, situace u příjemce bude opět odpovídat provedené operaci – příchozí e-mail bude opatřen ikonkou, indikující ochranu, a po otevření se vám může dostat vysvětlující informace o dešifrovací proceduře.

Obr. 17/18/19: Pokud je vše v pořádku, obdržíte po stisku tlačítka již tradiční okno s přijatou zprávou, jejíž obsah je běžně zobrazen, jako by šifra neexistovala. V případě, že jste využili obou možností – podpisu i šifry – budou se výsledné dialogy a vzhled obdržených zpráv mírně lišit dle aktuální varianty.

Obr. 20/21: Grafické rozhraní, jež nabízí zobrazení takto ošetřených poštovních zpráv, však není jen kosmetickou parádou – ikony podpisu (pečeti) a šifry (zámku) lze totiž využít pro zobrazení detailních informací o celé proceduře. Pokud kliknete na jednom ze symbolů (pečeti, zámku), jsou vám dostupné v následném dialogu na kartě *Zabezpečení* detailní informace o provedené kontrole celistvosti přenesených dat a jejich ukrytí. Využijete-li navíc tlačítko *Zobrazit certifikáty*, máte možnost detailně prozkoumat důvěryhodnost autora e-mailu, jím využité předvolby a navíc zde lze snadno vytvořit novou položku v adresáři, pochopitelně včetně potřebných certifikátů.

Jak již bylo uvedeno výše, pro nastolení automaticky ověřovaného důvěryhodného vztahu mezi stranami, jež si zasílají digitálně podepsané e-mailové zprávy, je klíčová shoda a podložená důvěra v případě kořenové certifikační autority.

Pokud se komunikující strany shodnou buďto na stejném vydavateli certifikátů, nebo považují navzájem autoritu svého protějšku za důvěryhodnou, mohou tento vztah stvrdit instalací certifikátu inkriminované kořenové autority do svého systému, čímž dojde k dosažení plné funkcionality příslušných aplikací a veškeré ovládání pak bude jednoduché a transparentní.

Záloha certifikátů a klíčů

V tomto i předchozím článku jsme si na různých příkladech ukázali, jak užitečné mohou být v praxi moderní šifrovací postupy a použití certifikátů. Jistě vám neušla jedna velmi důležitá skutečnost: funkcionalita celé struktury stojí a padá s tím, že máte k dispozici svůj klíčový pár, tedy dvojici veřejný a privátní klíč, a navíc musíte být schopni zajistit v případě privátního klíče jeho maximální utajení.

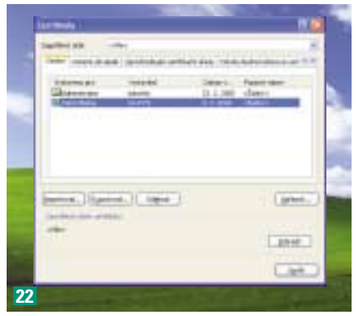
Stejně jako vše ostatní na pevném disku vašeho počítače, i certifikáty a klíčové páry uložené v útrobách operačního systému mohou snadno podlehnout zničení. Zhroutí-li se vám aplikace, nainstalujete ji znovu, ovšem přijdete-li o privátní klíč, není cesty zpět.

V zásadě nejjednodušší metodou pro zálohování certifikátů, případně i s privátním klíčem, je export z úložiště v operačním systému na nějaké přenosné médium, jež následně uchováváte na přiměřeně dobře utajeném místě. Tato procedura dovoluje v podstatě vyrobit záložní kopie certifikátů i s klíči, a to opakovaně v neomezeném počtu. Než k této proceduře přistoupíte, ještě jednom si připomeňme, že následná ochrana záložního média je absolutní nutností. Je tomu tak mimo jiné i proto, že po provedení exportu ztrácí certifikát (včetně klíče) jakousi ochrannou vazbu na účet

v operačním systému Windows: dokud byl v nitru systému, nebylo možno s ním disponovat bez platného přihlášení, ovšem z ukradené diskety jej může kdokoliv naimportovat do svého, jinak zcela cizího účtu, a použít jej k nejtěžšímu útoku formou podvržení vaší identity.

Obr. 22: Export certifikátu z osobního úložiště můžete provádět na více místech, například prostřednictvím MS Internet Exploreru, kde přejděte v menu *Nástroje/Možnosti Internetu* na kartu *Obsah* a stiskněte tlačítko *Certifikáty*. Z tohoto nám již důvěrně známého místa lze označit žádoucí položku a stiskem tlačítka *Exportovat* zahájit samotné zazálohování.

Obr. 23: Pokud se rozhodnete provádět zálohu včetně privátního klíče, jež vám dovolí jako jediná v případě pádu systému či hardwaru obnovit přístup k zašifrovaným datům, musíte ve druhé obrazovce proběhnuvšího Průvodce použít volbu *„Ano, exportovat soukromý klíč"*.


22

Obr. 24: Následující dialog dovoluje nastavit podrobnější parametry exportu. Volba *„Zahrnout všechny certifikáty…"* je výhodná z toho důvodu, že spolu s vaším certifikátem budou zálohovány i nadřízené položky, případně až k certifikátu důvěryhodné kořenové autority. Následná obnova při poškození systému bude o to snazší, že si nebudete moci dodatečně ostatní certifikáty shánět.

Rozhodně také neváhejte s použitím prostřední volby, jež dovolí exportovaný soubor ještě dodatečně ochránit heslem. Třetí, spodní možnost, je užitečná v případě, že jste se rozhodli certifikát exportovat s tím, že na daném počítači dočasně či trvale nebude používán. Jde o situace, jako je plánovaná reinstalace Windows či záměna „železa" za nové, takže citlivý privátní klíč bude po exportu odstraněn z útrob systému.

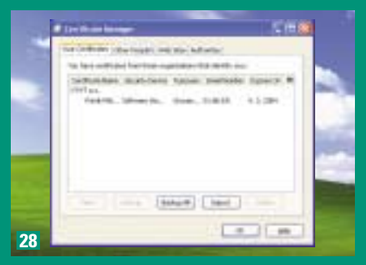
Obr. 25: V dalším dialogu již zadáte ochranné heslo k souboru (pozor, jeho ztrátu nelze napravit!) a následně cestu, kam bude balíček po exportu uložen. Výsledkem akce je soubor jako každý jiný, a proto při nakládání s ním nezapomeňte na zásady důsledné ochrany, o nichž jsme mluvili.

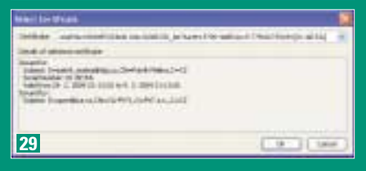
V případě, že opravdu dojde k poruše systému či jiné nemilé kalamitě a budete nuceni certifikát ze zálohy obnovit, postup není o nic složitější. Protože Windows formát souboru rozpoznají již podle asociované přípony, stačí „dvojklik" k tomu, aby byl spuštěn průvodce importem, tedy zave-

Když nepoužívám Outlook Express

Přestože náš příklad s ochranou elektronické pošty byl prováděn na komunikačních programech společnosti Microsoft, nikde není řečeno, že byste si nemohli stejnou ochranu nasadit do jiného nástroje. Pro doplňující ukázku jsme zvolili volně dostupný klient Mozilla Thunderbird, jenž je součástí jinak dobře známého internetového balíku.


27


28


29

Obr. 27: Jediný zásadní rozdíl oproti produktům Microsoftu je zde v tom, že aplikace nabízí vlastní úložiště certifikátů a nevyužívá prostor operačního systému. Nic to však nemění na konkrétních postupech, neboť všechny související operace jsou totožné. Správu zabezpečení pomocí certifikátů najdete v tomto programu v menu *Tools/ Account Settings* a dále pod položkou *Security*. V dialogu, jenž je poměrně podobný oknům v Outlook Expresu, máte možnost přiřadit certifikát zvlášť pro šifrování a zvlášť pro podpis.

Obr. 28: Nezapomeňte však nejdříve naimportovat svůj certifikát, jenž bude k těmto operacím sloužit. Provedete to v příslušném dialogu po stisku tlačítka *Manage Certificates*, kde při zobrazení karty *Your Certificates* zvolte tlačítko *Import* a vyberte soubor, v němž jsou potřebný klíčový pár a certifikát uloženy.

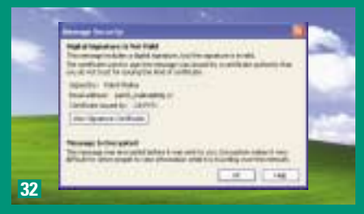
Obr. 29: Po úspěšném importu lze již po návratu do dialogu *Security* pomocí tlačítek *Select* přiřadit certifikát pro šifrování i podpis. Všimněte si, že dialogy aplikace jsou zpracovány velmi hezky a mají velmi vysokou informační hodnotu, takže můžete samotný obsah certifikátu důsledně kontrolovat.

Obr. 30: Použití podpisů a šifry u jednotlivých zpráv je poté opět poměrně jednoduché. Pokud píšete nový e-mail, pomocí voleb pod tlačítkem *Security* můžete specifikovat, zdali použijete podpis, šifru, či oboje zároveň.

Obr. 31: Rovněž práce s přijatou chráněnou poštou je poměrně jednoduchá a intuitivní. E-mail je po otevření v pravé části okna opatřen výraznými ikonami, které uživateli signalizují stav šifrování a podpisu.

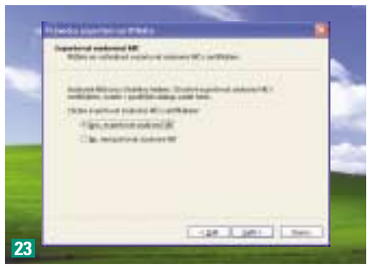

30

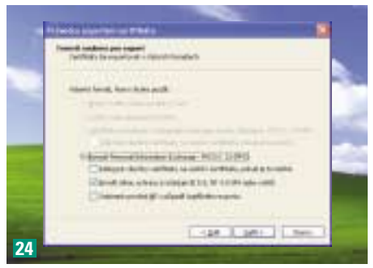

31

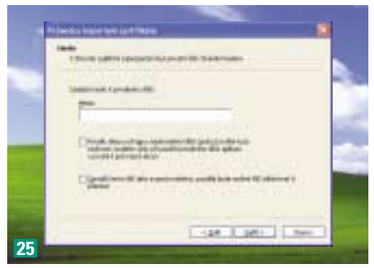

32

Obr. 32: Pokud došlo k porušení zprávy a podpis již není platný či nastala jiná nesrovnalost, např. že e-mail byl podepsán certifikátem od autority, jíž nedůvěřujete, aplikace vám tuto skutečnost dá výrazně najevo (ikona zlomené tužky) a poklepáním si zobrazíte detaily, jež důvod potíží objasní.

Z uvedených příkladů je patrné, že poštovní klient Thunderbird z balíku Mozilla je naprosto plnohodnotně vybaven pro práci s certifikáty a chráněnou elektronickou poštou, a nic vám v tomto ohledu nebrání v jeho nasazení.







dením certifikátu do systému. Před jeho započetím nezapomeňte na skutečnost, že přenést certifikát do osobního úložiště lze provést pouze pro účet, do něhož jste aktuálně přihlášeni. Po spuštění zaváděcí procedury budete v jednom z dialogů požádání o zadání ochranného hesla (opravdu to nepodceňujte!) a zároveň máte na téže obrazovce možnost nastavit dva veledůležité parametry. Silná ochrana privátního klíče spočívá v tom, že operační systém po vás bude při každém jeho použití vyžadovat dodatečné potvrzení, což je sice méně pohodlné, ale mnohem bezpečnější. Volba druhá je zaměřena na vaše budoucí záměry s certifikátem a privátním klíčem: chystáte-li se někdy znovu ze systému, kam klíč nyní zavádíte, provádět export, musíte tuto volbu zatrhnout. Pokud na to zapomenete, klíč bude po importu v systému uvězněn a už nikdy jej nedostanete ven!

Obr. 26: V následujícím kroku se operační systém ptá, zdali může úložiště certifikátu vybrat sám. Protože se Windows běžně trefují do správného cíle, není potřeba v normálních situacích položku měnit. Nezbývá, než operaci dokončit a počkat si na potvrzovací okno.

Popsaná metodika je pochopitelně určena nejen k zálohování certifikátů a klíčů, ale rovněž k jejich univerzálnímu přenosu mezi počítači a operačními systémy. Formát certifikátu spolu s privátním klíčem, jejž obdržíte při exportu, je definován univerzální normou (označovanou jako PKCS 12), a proto takto uložený soubor lze dále univerzálně využívat.

Závěrem

V našem dvoudílném miniseriálu jste mohli narazit na nejčastější použití principů moderního šifrování dat a navazování důvěryhodnosti v kybernetickém světě. Ačkoliv tato problematika je poměrně široká, při pečlivém čtení a experimentování jste si mohli osahat jedny z nejběžnějších operací, jež vám zároveň mohou přinést bezprostřední užitek, především v oblasti zabezpečení osobní komunikace a zvýšení důvěryhodnosti obchodování na internetu. Dobré pochopení základů vás však bude spolehlivě provázet i při nasazení dalších, pokročilejších aplikací geniálního principu asymetrické kryptografie, jenž zásadně ovlivnil elektronický svět. 4 0188/FEL ❑